



## **Guía del usuario de Cisco Router and Security Device Manager**

2.4.1

### **Sede central para América**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
EE.UU.  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Número de pedido del cliente:  
Número de parte de texto: OL-9963-04

LAS ESPECIFICACIONES Y LA INFORMACIÓN RELATIVA A LOS PRODUCTOS DE ESTE MANUAL ESTÁN SUJETAS A CAMBIOS SIN PREVIO AVISO. TODAS LAS DECLARACIONES, INFORMACIONES Y RECOMENDACIONES INCLUIDAS EN ESTE MANUAL SE CONSIDERAN PRECISAS. SIN EMBARGO, LAS MISMAS SE PRESENTAN SIN GARANTÍA DE NINGÚN TIPO, EXPLÍCITA O IMPLÍCITA. LA APLICACIÓN DE CUALQUIER PRODUCTO ES RESPONSABILIDAD TOTAL DE LOS USUARIOS.

LA LICENCIA DE SOFTWARE Y LA GARANTÍA LIMITADA DEL PRODUCTO QUE LA ACOMPAÑA SE ESTABLECEN EN EL PAQUETE DE INFORMACIÓN SUMINISTRADO CON EL PRODUCTO Y SE INCORPORAN EN ESTE DOCUMENTO MEDIANTE ESTA REFERENCIA. SI NO ENCUENTRA LA LICENCIA DE SOFTWARE O LA GARANTÍA LIMITADA, PÓNGASE EN CONTACTO CON EL REPRESENTANTE DE CISCO PARA OBTENER UNA COPIA.

La implantación de Cisco de la compresión de encabezados TCP es una adaptación de un programa desarrollado por la Universidad de California, Berkeley (UCB) como parte de la versión de dominio publico de la UCB del sistema operativo UNIX. Todos los derechos reservados. Copyright © 1981, Regents of the University of California.

A PESAR DE CUALQUIER OTRA GARANTÍA ESPECIFICADA EN ESTE DOCUMENTO, TODOS LOS ARCHIVOS DE DOCUMENTO Y SOFTWARE DE ESTOS PROVEEDORES SE PROPORCIONAN "TAL CUAL" CON TODOS LOS ERRORES. CISCO Y LOS PROVEEDORES MENCIONADOS ANTERIORMENTE RENUNCIAN A TODA GARANTÍA, EXPLÍCITA O IMPLÍCITA, INCLUIDAS, SIN LIMITACIONES, LAS DE COMERCIABILIDAD, CAPACIDAD PARA UN PROPÓSITO EN PARTICULAR Y NO INFRACCIÓN O LAS QUE PUEDAN SURGIR DEL TRATO, USO O PRÁCTICA COMERCIAL.

EN NINGÚN CASO, CISCO NI SUS PROVEEDORES SERÁN RESPONSABLES DE NINGÚN DAÑO INDIRECTO, ESPECIAL, CONSECUENTE O FORTUITO, INCLUYENDO, SIN LIMITACIONES, GANANCIAS PERDIDAS O DATOS PERDIDOS O DAÑADOS, QUE PUEDAN SURGIR DEL USO O INCAPACIDAD DE USO DE ESTE MANUAL, INCLUSO EN CASO DE QUE CISCO O SUS PROVEEDORES HAYAN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

CCVP, el logo de Cisco y el logo de Cisco Square Bridge son marcas comerciales de Cisco Systems, Inc.; Changing the Way We Work, Live, Play y Learn es una marca de servicio de Cisco Systems, Inc.; y Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIIP, CCNA, CCNP, CCSP, Cisco, el logo de Cisco Certified Internetwork Expert, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, el logo de Cisco Systems, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, IQ Expertise, el logo de IQ, IQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, y TransPath son marcas comerciales de Cisco Systems, Inc. y/o de sus filiales en los Estados Unidos y otros países específicos.

El resto de marcas comerciales mencionadas en este documento o sitio Web pertenecen a sus respectivos propietarios. El uso de la palabra socio no implica una relación de sociedad entre Cisco y otra compañía. (0612R)

Ninguna dirección de Protocolo de Internet (IP) utilizada en este documento es real. Todo ejemplo, resultado de visualización de comandos y figura incluido en el documento se muestran sólo con fines ilustrativos. El uso de cualquier dirección IP en contenido ilustrativo es mera coincidencia.

*Guía del usuario de Cisco Router and Security Device Manager 2.4*

© 2007 Cisco Systems, Inc. Todos los derechos reservados.



# CONTENIDO

## **Página de inicio 1**

## **Asistente para LAN 1**

Configuración de Ethernet 3

Asistente para LAN: Seleccionar una interfaz 3

Asistente para LAN: Dirección IP/máscara de subred 3

Asistente para LAN: Activar Servidor DHCP 4

Asistente para LAN: Conjuntos de direcciones DHCP 4

Opciones de DHCP 5

Asistente para LAN: Modo VLAN 6

Asistente para LAN: Puerto del switch 6

Puente IRB 7

Configuración BVI 8

Conjunto DHCP para BVI 8

IRB para Ethernet 9

Configuración de Ethernet Nivel 3 9

Configuración 802.1Q 9

Configuración del enlace o enrutamiento 10

Módulo de configuración del dispositivo del switch 10

Configurar interfaz de Ethernet de gigabits 10

Resumen 11

Cómo... 11

¿Cómo se configura una ruta estática? 11

¿Cómo se visualiza la actividad en la interfaz LAN? 12

¿Cómo se activa o desactiva una interfaz? 13

¿Cómo se visualizan los comandos de IOS que se envían al router? 14

¿Cómo inicio la Aplicación inalámbrica de Cisco SDM? 14

**Autenticación 802.1x 1**

Asistente para LAN: Autenticación 802.1x (puertos de switch) 2

Opciones avanzadas 3

Asistente para LAN: Servidores RADIUS para autenticación 802.1x 5

Editar autenticación 802.1x (puertos de switch) 7

Asistente para LAN: Autenticación 802.1x (VLAN o Ethernet) 8

Listas de excepciones de 802.1x 10

Autenticación 802.1x en interfaces de capa 3 11

Editar la autenticación 802.1x 13

¿Cómo... 14

¿Cómo configuro autenticación 802.1x en más de un puerto Ethernet? 14

**Asistentes para crear conexiones 1**

Crear conexión 1

Ventana de bienvenida de la interfaz del asistente para WAN 3

Ventana de bienvenida de la interfaz del asistente para ISDN (RDSI) 3

Ventana de bienvenida del módem analógico 3

Ventana de bienvenida de la conexión de reserva auxiliar 3

Seleccionar la interfaz 4

Encapsulación: PPPoE 4

Dirección IP: ATM o Ethernet con PPPoE/PPPoA 5

Dirección IP: ATM con enrutamiento RFC 1483 6

Dirección IP: Ethernet sin PPPoE	7
Dirección IP: serie con Protocolo punto a punto	7
Dirección IP: serie con HDLC o Frame Relay	8
Dirección IP: ISDN (RDSI) BRI o módem analógico	9
Autenticación	10
Tipo de switch y SPID	11
Cadena de marcación	12
Configuración de la conexión de reserva	13
Configuración de la conexión de reserva: Direcciones IP de la interfaz principal y del próximo salto (next hop)	13
Configuración de la conexión de reserva: Nombre de host o dirección IP objeto del seguimiento	14
Opciones avanzadas	14
Encapsulación	15
PVC	17
Configuración de LMI y DLCI	19
Configuración del reloj	20
Eliminar conexión	22
Resumen	24
Pruebas y resolución de problemas de la conectividad	25
Cómo...	29
¿Cómo se visualizan los comandos de IOS que se envían al router?	29
¿Cómo se configura una interfaz WAN no admitida?	29
¿Cómo se activa o desactiva una interfaz?	30
¿Cómo se visualiza la actividad en la interfaz WAN?	30
¿Cómo se configura NAT en una interfaz WAN?	31
¿Cómo se configura NAT en una interfaz no admitida?	32
¿Cómo se configura un protocolo de enrutamiento dinámico?	32

¿Cómo se configura el enrutamiento de marcación a petición para la interfaz asíncrona o ISDN? 33

¿Cómo se edita una Configuración de interfaz de radio? 34

## **Editar interfaz/conexión 1**

Conexión: Ethernet para IRB 6

Conexión: Ethernet para enrutamiento 7

Métodos existentes de DNS dinámico 8

Agregar Método de DNS dinámico 9

Inalámbrica 10

Asociación 10

NAT 13

Editar puerto del switch 13

Servicio de aplicación 15

General 16

Seleccionar el tipo de configuración Ethernet 18

Conexión: VLAN 19

Lista de subinterfases 20

Agregar/Editar una interfaz BVI 20

Agregar o editar una interfaz de retrobucle 21

Conexión: Interfaz de plantilla virtual 21

Conexión: LAN Ethernet 22

Conexión: WAN Ethernet 23

Ethernet Properties (Propiedades de Ethernet) 25

Conexión: Ethernet sin encapsulación 27

Conexión: ADSL 28

Conexión: ADSL sobre ISDN (RDSI) 31

Conexión: G.SHDSL 34

Configurar controlador DSL	38
Agregar una conexión G.SHDSL	40
Conexión: Interfaz de serie, encapsulación Frame Relay	43
Conexión: Interfaz de serie, encapsulación PPP	46
Conexión: Interfaz de serie, encapsulación HDLC	48
Agregar o editar un túnel GRE	49
Conexión: ISDN (RDSI) BRI	51
Conexión: Módem analógico	54
Conexión: (Reserva AUX.)	56
Autenticación	59
Información de SPID	60
Opciones de marcación	61
Configuración de la copia de seguridad	63
<b>Crear un firewall</b>	<b>1</b>
Asistente de configuración para firewall básico	4
Configuración de la interfaz de firewall básico	4
Configuración del firewall para acceso remoto	5
Asistente de configuración para firewall avanzado	5
Configuración de la interfaz de firewall avanzado	5
Configuración del servicio DMZ de firewall avanzado	6
Configuración de servicio DMZ	7
Configuración de seguridad de la aplicación	8
Configuración del servidor del nombre del dominio	9
Configuración del servidor de filtro URL	9
Seleccionar la zona de interfaz	10
Zonas internas de ZPF	10
Resumen	10
Alerta de SDM: Acceso a SDM	12

Cómo... 14

- ¿Cómo se visualiza la actividad en el firewall? 14
- ¿Cómo se configura un firewall en una interfaz no compatible? 16
- ¿Cómo se configura un firewall después de configurar una VPN? 17
- ¿Cómo se puede permitir que pase determinado tráfico por una interfaz DMZ? 17
- ¿Cómo se modifica un firewall existente para permitir el tráfico procedente de una nueva red o host? 18
- ¿Cómo se configura NAT en una interfaz no admitida? 19
- ¿Cómo se configura el paso de NAT (NAT Passthrough) para un firewall? 19
- ¿Cómo se permite que el tráfico llegue al concentrador Easy VPN a través del firewall? 20
- ¿Cómo se asocia una regla a una interfaz? 21
- ¿Cómo se anula la asociación de una regla de acceso con una interfaz? 22
- ¿Cómo se elimina una regla que esté asociada a una interfaz? 23
- ¿Cómo se crea una regla de acceso para una lista Java? 23
- ¿Cómo se permite que tráfico determinado entre en la red si no se dispone de una red DMZ? 24

**Política de firewall 1**

- Editar política de firewall/Lista de control de acceso 1
- Seleccionar un flujo de tráfico 3
- Examinar el diagrama de tráfico y seleccionar una dirección de tráfico 5
- Realizar cambios a las reglas de acceso 7
- Realizar cambios a las reglas de inspección 11
- Agregar entrada de aplicación *nombre\_aplicación* 13
- Agregar entrada de aplicación RPC 14
- Agregar entrada de aplicación de fragmento 15
- Agregar o editar entrada de aplicación HTTP 16
- Bloqueo del subprograma Java 17
- Advertencia de Cisco SDM: Regla de inspección 18
- Advertencia de Cisco SDM: Firewall 18



Editar política de firewall	19
Agregar una nueva regla	22
Agregar tráfico	23
Inspección de aplicación	25
Filtro URL	25
Calidad de servicio (QoS)	25
Parámetro de inspección	25
Seleccionar tráfico	26
Eliminar regla	26
<b>Seguridad de la Aplicación</b>	<b>1</b>
Ventanas de Seguridad de la Aplicación	2
Ninguna Política de Seguridad de la Aplicación	3
Correo electrónico	4
Mensajería Instantánea	6
Aplicaciones Par-a-Par	7
Filtrado de URL	7
HTTP	8
Opciones del encabezado	10
Opciones del contenido	11
Aplicaciones y Protocolos	13
Tiempos de inactividad y umbrales para mapas de parámetros de inspección y CBAC	15
Asociar Política con una Interfaz	18
Editar la Regla de Inspección	18
Controles Permitir, Bloquear y Alerta	20

**VPN sitio a sitio 1**

Guía de diseño de VPN	1
Crear VPN sitio a sitio	1
Asistente para VPN sitio a sitio	4
Ver valores por defecto	6
Información acerca de la conexión VPN	6
Propuestas IKE	8
Conjunto de transformación	11
Tráfico para proteger	13
Resumen de la configuración	15
Configuración de spoke	15
Túnel GRE seguro (GRE sobre IPSec)	16
Información acerca del túnel GRE	17
Información de autenticación VPN	18
Información acerca del túnel GRE de reserva	19
Información de enrutamiento	20
Información sobre el enrutamiento estático	22
Seleccionar el protocolo de enrutamiento	24
Resumen de la configuración	24
Editar VPN sitio a sitio	25
Agregar nueva conexión	28
Agregar mapa criptográfico	28
Asistente para mapas criptográficos: Bienvenido	29
Asistente para mapas criptográficos: Resumen de la configuración	30
Eliminar conexión	30
Ping	31
Generar el reflejo...	31
Advertencia de Cisco SDM: Reglas NAT con ACL	32

Cómo...	33
¿Cómo se crea una VPN para más de un sitio?	33
Después de configurar una VPN, ¿cómo se configura la VPN en el router del par?	35
¿Cómo se edita un túnel VPN existente?	37
¿Cómo se puede confirmar que mi VPN funciona?	37
¿Cómo se configura un par de reserva para mi VPN?	38
¿Cómo se acomodan varios dispositivos con diferentes niveles de admisión de VPN?	39
¿Cómo se configura una VPN en una interfaz no compatible?	40
¿Cómo se configura una VPN después de configurar un firewall?	40
¿Cómo se configura el paso de NAT (NAT Passthrough) para una VPN?	40

## Easy VPN remoto 1

Creación de Easy VPN remoto	1
Configurar un cliente de Easy VPN remoto	1
Información del servidor	2
Autenticación	3
Interfaces y configuración de conexiones	5
Resumen de la configuración	6
Editar Easy VPN remoto	7
Agregar o Editar Easy VPN remoto	13
Agregar o Editar Easy VPN remoto: Configuración de Easy VPN	16
Agregar o Editar Easy VPN remoto: Información de autenticación	18
Especificar credenciales para SSH	21
Ventana Conexión a XAuth	21
Agregar o Editar Easy VPN remoto: Configuración general	21
Opciones de la Extensión de la Red	23
Agregar o Editar Easy VPN remoto: Información de autenticación	24
Agregar o Editar Easy VPN remoto: Interfaces y conexiones	26

Cómo... 28

¿Cómo se edita una conexión Easy VPN existente? 28

¿Cómo configuro una conexión de respaldo para una conexión de la Easy VPN? 28

## **Servidor Easy VPN 1**

Crear un servidor Easy VPN 1

Bienvenido al asistente para servidores Easy VPN 2

Interfaz y Autenticación 2

Búsqueda de Política de grupos y Autorización de grupos 3

Autenticación de usuario (XAuth) 4

Cuentas de usuario para XAuth 5

Agregar servidor RADIUS 6

Autorización de grupo: Políticas de grupos de usuarios 6

Información General del Grupo 7

Configuración de DNS y WINS 9

División de la arquitectura de túneles 10

Configuraciones del Cliente 12

Elija las Configuraciones del Proxy del Explorador 15

Agregar o Editar Configuraciones del Proxy del Explorador 16

Autenticación de usuario (XAuth) 17

Actualización del Cliente 18

Agregar o Editar Entrada de Actualización del Cliente 19

Resumen 21

Configuraciones del Proxy del Explorador 21

Agregar o Editar el Servidor de la Easy VPN 23

Agregar o editar conexión de servidor Easy VPN 24

Restringir Acceso 25

Configuración de políticas de grupo 26

**Conjuntos IP 29**

Agregar o editar conjunto local IP 30

Agregar intervalo de direcciones IP 30

**Enhanced Easy VPN 1**

Interfaz y Autenticación 1

Servidores RADIUS 2

Políticas de Grupo de usuarios y Autorización de grupos 4

Agregar o Editar servidor Easy VPN: Ficha General 5

Agregar o Editar servidor Easy VPN: Ficha IKE 5

Agregar o Editar servidor Easy VPN: Ficha IPsec 7

Crear interfaz de túnel virtual 8

**DMVPN 1**

Red privada virtual multipunto dinámica (DMVPN) 1

Asistente para hubs de red privada virtual multipunto dinámica 2

Tipo de hub 3

Configurar la clave previamente compartida 3

Configuración de la interfaz de túnel GRE de hub 4

Configuración avanzada para la interfaz de túnel 5

Hub principal 7

Seleccionar el protocolo de enrutamiento 7

Información de enrutamiento 8

Asistente para spokes de privada virtual multipunto dinámica 10

Topología de red DMVPN 10

Especificar la información del hub 11

Configuración de la interfaz de túnel GRE de spoke 11

Advertencia de Cisco SDM: DMVPN Dependency (Dependencia DMVPN) 13

- Editar VPN multipunto dinámica (DMVPN) 13
  - Panel General 15
  - Panel NHRP 17
    - Configuración del mapa NHRP 18
  - Panel Enrutamiento 19
- ¿Cómo se configura una red DMVPN manualmente? 21

**Configuración VPN global 1**

- Configuración VPN global 1
  - Configuración VPN global: IKE 3
  - Configuración VPN global: IPSec 4
  - Configuración del cifrado de la clave VPN 5

**Seguridad IP 1**

- Políticas IPSec 1
  - Agregar una política IPSec/Editar la política IPSec 4
  - Agregar o editar el mapa criptográfico: General 5
  - Agregar o editar el mapa criptográfico: Información del par 7
  - Agregar o editar el mapa criptográfico: Conjuntos de transformación 7
  - Agregar o editar el mapa criptográfico: Tráfico de protección 10
- Conjuntos de mapas criptográficos dinámicos 12
  - Agregar un conjunto de mapas criptográficos dinámicos/Editar el conjunto de mapas criptográficos dinámicos 12
  - Asociar mapas criptográficos a esta política IPSec 13
- Perfiles IPSec 13
  - Agregar o editar un perfil IPSec 14
  - Agregar un perfil IPSec/Editar el perfil IPSec y Agregar mapa criptográfico dinámico 16
- Conjunto de transformación 17
  - Agregar/Editar conjunto de transformación 20
- Reglas IPSec 23

**Intercambio de claves por Internet 1**

Intercambio de claves por Internet (IKE) 1

Políticas IKE 2

Agregar o editar una política IKE 4

Claves previamente compartidas de IKE 6

Agregar una nueva clave previamente compartida/Editar la clave  
previamente compartida 8

Perfiles IKE 9

Agregar o editar un perfil IKE 10

**Infraestructura de clave pública 1**

Asistentes para certificados 1

Bienvenido al Asistente para SCEP 3

Información acerca de la Autoridad certificadora (CA) 3

Opciones avanzadas 4

Atributos del nombre de asunto del certificado 5

Otros atributos de asunto 6

Claves RSA 7

Resumen 8

Certificado de servidor de la CA 9

Estado de suscripción 9

Bienvenido al Asistente para cortar y pegar 10

Tarea de suscripción 10

Solicitud de suscripción 11

Continuar con la suscripción sin terminar 11

Importar el certificado de la CA 12

Importar el o los certificados de router 12

- Certificados digitales 13
  - Información acerca del punto de confianza 15
  - Detalles del certificado 16
  - Comprobar revocación 16
  - Comprobar revocación de CRL únicamente 17
- Ventana Claves RSA 17
  - Generar par de claves RSA 18
  - Credenciales del token USB 20
- Tokens USB 20
  - Agregar o Editar un token USB 21
- Abrir Firewall 23
  - Abrir detalles del firewall 24

**Servidor de la autoridad certificadora 1**

- Crear servidor de la CA 1
  - Tareas previas para configuraciones de PKI 2
  - Asistente para el servidor de la CA: Bienvenido 3
  - Asistente para el servidor de la CA: Información acerca de la Autoridad certificadora 4
    - Opciones avanzadas 5
  - Asistente para el servidor de la CA: Claves RSA 7
  - Abrir Firewall 8
  - Asistente para el servidor de la CA: Resumen 9
- Administrar servidor de la CA 10
  - Servidor de la CA de reserva 12
- Administrar servidor de la CA: Restaurar ventana 12
  - Restaurar servidor de la CA 12
    - Editar configuración del servidor de la CA: Ficha General 13
    - Editar configuración del servidor de la CA: Ficha Avanzado 13
- Administrar servidor de la CA: Servidor de la CA no configurado 14



Administrar certificados	14
Solicitudes pendientes	14
Certificados revocados	16
Revocar certificado	17
<b>VPN con SSL de Cisco IOS</b>	<b>1</b>
Enlaces de VPN con SSL de Cisco IOS en Cisco.com	2
Crear SSL VPN	3
Certificado con firma automática permanente	5
Bienvenido	6
Gateways SSL VPN	6
Autenticación del Usuario	7
Configurar sitios Web de la intranet	9
Agregar o editar URL	9
Personalizar el portal SSL VPN	10
Configuración de paso por SSL VPN	10
Política de usuarios	11
Detalles de la política de grupo de SSL VPN: Policyname	11
Seleccionar el grupo de usuarios de SSL VPN	12
Seleccionar funciones avanzadas	12
Cliente ligero (mapeo de puertos)	13
Agregar o editar un servidor	13
Más detalles acerca de los servidores de mapeo de puertos	14
Túnel completo	15
Buscar el paquete de instalación de Cisco SDM	17
Activar Cisco Secure Desktop	19
Sistema de archivos de Internet común	20
Activar Citrix sin cliente	21
Resumen	21
Editar SSL VPN	21

Contexto de SSL VPN	23
Designar interfaces como internas o externas	25
Seleccionar un gateway	25
Contexto: Políticas de grupo	25
Más detalles acerca de las políticas de grupo	26
Política de grupo: Ficha General	27
Política de grupo: Ficha Sin clientes	27
Política de grupo: Ficha Cliente ligero	28
Política de grupo: Ficha Cliente VPN con SSL (túnel completo)	29
Opciones avanzadas de túnel	30
Más detalles acerca de la división de la arquitectura de túneles	33
Servidores DNS y WINS	34
Contexto: Configuración HTML	34
Seleccionar color	35
Contexto: Listas de servidores de nombres NetBIOS	36
Agregar o editar una lista de servidores de nombres NetBIOS	36
Agregar o editar un servidor NBNS	36
Contexto: Listas de mapeo de puertos	37
Agregar o editar una lista de mapeo de puertos	37
Contexto: Listas de direcciones URL	37
Agregar o editar una lista de direcciones URL	38
Contexto: Cisco Secure Desktop	38
Gateways SSL VPN	39
Agregar o editar un gateway SSL VPN	40
Paquetes	41
Instalar paquete	42
Contextos, gateways y políticas VPN con SSL de Cisco IOS	42

Cómo... 49

¿Cómo puedo confirmar que VPN con SSL de Cisco IOS funciona? 49

¿Cómo se configura una VPN con SSL de Cisco IOS después de configurar un firewall? 50

¿Cómo puedo asociar una instancia de VRF con un contexto de VPN con SSL de Cisco IOS? 50

## **Resolución de problemas de VPN 1**

Resolución de problemas de VPN 1

Resolución de problemas de VPN: Especificar el cliente Easy VPN 4

Resolución de problemas de VPN: Generar tráfico 4

Resolución de problemas de VPN: Generar tráfico GRE 6

Advertencia de Cisco SDM: SDM activará depuraciones del router 7

## **Auditoría de seguridad 1**

Página de bienvenida 4

Página de selección de la interfaz 5

Página Tarjeta de informes 5

Página Repararlo 6

Desactivar el servicio Finger 7

Desactivar el servicio PAD 8

Desactivar el servicio de pequeños servidores TCP 8

Desactivar el servicio de pequeños servidores UDP 9

Desactivar el servicio del servidor IP bootp 10

Desactivar el servicio IP ident 10

Desactivar CDP 11

Desactivar la ruta de origen IP 11

Activar el servicio de cifrado de contraseñas 12

Activar los paquetes "keep-alive" de TCP para sesiones telnet entrantes 12

Activar los paquetes "keep-alive" de TCP para sesiones telnet salientes 13

Activar números de secuencia y marcadores de hora en depuraciones	13
Activar IP CEF	14
Desactivar Gratuitous ARP de IP	14
Definir la longitud mínima de la contraseña a menos de 6 caracteres	15
Definir la proporción de fallos de autenticación a menos de 3 intentos	15
Definir la hora TCP Synwait	16
Definir anuncio	16
Activar registro	17
Definir activación de la contraseña secreta	18
Desactivar SNMP	18
Definir el intervalo del Programador	19
Definir asignación del Programador	19
Definir usuarios	20
Activar configuración Telnet	20
Activar cambio a NetFlow	21
Desactivar redireccionamiento IP	21
Desactivar ARP Proxy IP	22
Desactivar difusión dirigida IP	22
Desactivar servicio MOP	23
Desactivar IP de destino inalcanzable	23
Desactivar respuesta de máscara IP	24
Desactivar IP de destino inalcanzable en interfaz NULA	24
Activar RPF unidifusión en todas las interfaces externas	25
Activar firewall en todas las interfaces externas	26
Definir la clase de acceso en el servicio de servidor HTTP	26
Definir la clase de acceso en líneas VTY	27
Activar SSH para acceder al router	27
Activar AAA	28
Pantalla Resumen de la configuración	28
Cisco SDM y AutoSecure de Cisco IOS	28

Configuraciones de seguridad que Cisco SDM puede deshacer	31
Cómo deshacer las correcciones de la Auditoría de seguridad	32
Pantalla Agregar/Editar una cuenta Telnet/SSH	32
Configurar cuentas de usuario para Telnet/SSH	33
Página Enable Secret and Banner (Activar contraseña secreta y anuncio)	34
Página Registro	35

## **Enrutamiento** 1

Agregar ruta estática de IP/Editar la ruta estática de IP	4
Agregar/Editar una ruta RIP	5
Agregar o editar una ruta OSPF	6
Agregar o editar una ruta EIGRP	7

## **Traducción de direcciones de red** 1

Asistentes de traducción de direcciones de la red	1
Asistente de NAT básica: Bienvenido	2
Asistente de NAT básica: Conexión	2
Resumen	3
Asistente de NAT avanzada: Bienvenido	3
Asistente de NAT avanzada: Conexión	4
Agregar dirección IP	4
Asistente de NAT avanzada: Redes	4
Agregar redes	5
Asistente de NAT avanzada: Direcciones IP públicas del servidor	6
Agregar o editar Regla de traducción de direcciones	6
Asistente de NAT avanzada: Conflicto ACL	8
Detalles	8
Reglas de traducción de direcciones de la red	8
Designar interfaces NAT	13
Configuración del límite de tiempo para la traducción	13

Editar mapa de ruta	15
Editar entrada del mapa de ruta	16
Conjuntos de direcciones	17
Agregar/Editar conjunto de direcciones	18
Agregar o editar regla de traducción de direcciones estáticas: De interna a externa	19
Agregar o editar regla de traducción de direcciones estáticas: De externa a interna	22
Agregar o editar regla de traducción de direcciones dinámicas: De interna a externa	25
Agregar o editar regla de traducción de direcciones dinámicas: De externa a interna	28
Cómo . . .	30
¿Cómo configuro la Traducción de direcciones de externa a interna?	31
¿Cómo configuro NAT con una LAN y múltiples WAN?	31

## **Cisco IOS IPS 1**

Crear IPS	2
Crear IPS: Bienvenido	3
Crear IPS: Seleccionar interfaces	3
Crear IPS: Ubicación SDF	3
Crear IPS: Archivo de firma	4
Crear IPS: Ubicación y categoría del archivo de configuración	6
Agregar o editar una ubicación de configuración	6
Selección de directorio	7
Archivo de firma	7
Crear IPS: Resumen	8
Crear IPS: Resumen	9
Editar IPS	10
Editar IPS: Políticas IPS	11
Activar o editar IPS en una interfaz	14

Editar IPS: Configuraciones globales	15
Editar configuración global	17
Agregar o editar una ubicación de firma	19
Editar IPS: Mensajes SDEE	20
Texto de los mensajes SDEE	21
Editar IPS: Configuraciones globales	23
Editar configuración global	24
Editar requisitos previos de IPS	26
Agregar clave pública	27
Editar IPS: Actualización automática	27
Editar IPS: Configuración SEAP	29
Editar IPS: Configuración SEAP: Índice de valor de destino	29
Agregar Índice de valor de destino	31
Editar IPS: Configuración SEAP: Anulaciones de acción de evento	31
Agregar o editar una anulación de acción de evento	33
Editar IPS: Configuración SEAP: Filtros de acción de evento	34
Agregar o editar un filtro de acción de evento	36
Editar IPS: Firmas	39
Editar IPS: Firmas	45
Editar firma	50
Selección de archivos	53
Asignar acciones	54
Importar firmas	55
Agregar, editar o duplicar firma	57
Cisco Security Center	59
Archivos de definición de firmas entregados con IPS	59
Panel de seguridad	61
Migración IPS	64
Asistente para migración: Bienvenido	64

Asistente para migración: Seleccione el archivo de firma de copia de seguridad de IOS IPS 64

    Archivo de firma 65

Java Heap Size 65

## **Gestión del módulo de red 1**

Gestión del módulo de red IDS 1

    Dirección IP de la interfaz del sensor IDS 3

    Determinación de la dirección IP 4

    Lista de verificación de la configuración del módulo de red IDS 5

    Configuración de supervisión de la interfaz del módulo de red IDS 7

Inicio de sesión del módulo de red 7

Función No disponible 7

Selección de interfaz del módulo de switch 7

## **Calidad de servicio (QoS) 1**

Crear política de QoS 1

Asistente para QoS 2

    Selección de Interfaz 2

Generación de la política de QoS 3

Resumen de la configuración de QoS 3

Editar política de QoS 5

    Asociar o anular asociación de la política de QoS 8

    Agregar o editar una clase de QoS 8

        Editar valores DSCP de coincidencia 10

        Editar valores de protocolo de coincidencia 10

        Agregar protocolos personalizados 11

        Editar ACL de coincidencia 11

    Editar valores DSCP de coincidencia 11



## **Control de Admisión a la Red 1**

Ficha Crear NAC 2

Otras Tareas en una Implementación del NAC 3

Bienvenido 4

Servidores de Políticas del NAC 5

Selección de Interfaz 7

Lista de excepción de NAC 8

Agregar o Editar una Entrada de la Lista de Excepción 9

Elegir una Política de Excepción 9

Agregar Política de Excepción 10

Política de Hosts sin Agentes 11

Configurar el NAC para el Acceso Remoto 12

Modificar el firewall 12

Ventana Detalles 13

Resumen de la configuración 13

Ficha Editar NAC 14

Componentes del NAC 15

Ventana Lista de Excepción 16

Ventana Políticas de Excepción 16

Límites de tiempo del NAC 17

Configurar la Política del NAC 18

Cómo... 20

¿Cómo Configuro un Servidor de Política del NAC? 20

¿Cómo Instalo y Configuro un Agente de gestión de estado en un Host? 20

## **Propiedades del router 1**

Propiedades del dispositivo 1

Fecha y hora: Propiedades del reloj 3

Propiedades de fecha y hora 3

NTP 5

Agregar/Editar detalles del servidor NTP 6

SNTP	7
Agregar detalles del servidor NTP	8
Registro	9
SNMP	10
Netflow	11
Usuarios de Netflow	12
Acceso a router	13
Cuentas de usuario: Configurar cuentas de usuario para el acceso al router	13
Agregar/Editar un nombre de usuario	14
Contraseña de la vista	16
Configuración VTY	17
Editar líneas vty	18
Configurar políticas de acceso a la gestión	19
Agregar/Editar una política de gestión	21
Mensajes de error de acceso a la gestión	23
SSH	25
Configuración DHCP	26
Conjuntos DHCP	26
Agregar o Editar conjunto DHCP	27
Asociaciones DHCP	28
Agregar o Editar la Asociación DHCP	30
Propiedades de DNS	31
Métodos DNS dinámicos	31
Agregar o Editar un método DNS dinámico	32

**Editor ACL 1**

Procedimientos útiles para las reglas de acceso y firewalls 3

Ventanas de reglas 4

Agregar/Editar una regla 8

Asociar con una interfaz 11

Agregar una entrada de regla estándar 12

Agregar una entrada de regla ampliada 14

Seleccionar una regla 19

**Asignación puerto a aplicación 1**

Asignaciones puerto a aplicación 1

Agregar o editar entrada de asignación de puerto 3

**Firewall de política basado en zonas 1**

Ventana de zona 2

Agregar o editar una zona 3

Reglas generales de la política basada en zonas 4

Pares de zonas 5

Agregar o editar un par de zonas 6

Agregar una zona 6

Seleccionar una zona 7

**Authentication, Authorization and Accounting (AAA) 1**

Ventana principal de AAA 2

Grupos y servidores AAA 3

Ventana Servidores AAA 3

Agregar o editar un servidor TACACS+ 4

Agregar o editar un servidor RADIUS 5

Editar configuración global 6

Ventana Grupos de servidores AAA 7

Agregar o editar grupo de servidores AAA 8

- Políticas de Autenticación y Autorización 8
  - Ventanas de Autenticación y Autorización 9
  - Autenticación de NAC 10
  - Autenticación de 802.1x 11
  - Agregar o Editar una lista de métodos para autenticar o autorizar 12

**Provisionamiento del router 1**

- Secure Device Provisioning 1
- Provisionamiento del router desde el USB 2
- Provisionamiento del router desde USB (cargar archivo) 2
- Sugerencias para la resolución de problemas SDP 3

**Lenguaje de política de clasificación común de Cisco 1**

- Mapa de política 1
  - Ventanas de mapa de política 2
    - Agregar o editar un mapa de política de QoS 3
    - Agregar un mapa de política de inspección 4
  - Mapa de política de capa 7 4
  - Inspección de aplicación 5
  - Configurar inspección profunda de paquetes 5
- Mapas de clase 6
  - Asociar mapa de clase 7
    - Opciones avanzadas del mapa de clase 7
  - Mapa de clase de QoS 8
    - Agregar o editar un mapa de clase de QoS 9
    - Agregar o editar un mapa de clase de QoS 9
    - Seleccionar un mapa de clase 9
  - Inspección profunda 9

Ventanas Mapa de clase y Grupos de servicio de aplicación	9
Agregar o editar un mapa de clase de inspección	12
Asociar mapa de parámetro	13
Agregar un mapa de clase de inspección HTTP	13
Encabezado de solicitud HTTP	14
Campos de encabezado de solicitud HTTP	15
Cuerpo de solicitud HTTP	16
Argumentos de encabezado de solicitud HTTP	16
Método HTTP	17
Uso incorrecto del puerto de solicitud	17
URI de solicitud	17
Encabezado de respuesta	18
Campos de encabezado de respuesta	18
Cuerpo de respuesta HTTP	19
Línea de estado de respuesta HTTP	20
Criterios de encabezado de solicitud/respuesta	21
Campos de encabezado de solicitud/respuesta HTTP	21
Cuerpo de solicitud/respuesta	22
Infracción del protocolo de solicitud/respuesta	23
Agregar o editar un mapa de clase IMAP	23
Agregar o editar un mapa de clase SMTP	24
Agregar o editar un mapa de clase SUNRPC	24
Agregar o editar un mapa de clase de mensajería instantánea	24
Agregar o editar un mapa de clase punto a punto	24
Agregar regla P2P	26
Agregar o editar un mapa de clase de POP3	26
Mapas de parámetros	26
Ventanas de mapa de parámetros	27
Agregar o editar un mapa de parámetro para información de protocolo	27
Agregar o editar una entrada del servidor	28

- Agregar o editar expresión regular 28
- Agregar un patrón 29
- Generar expresión regular 30
- Metacaracteres de expresión regular 33

**Filtrado de URL 1**

- Ventana de filtrado de URL 2
  - Editar configuración global 2
  - Configuración general para el filtrado de URL 4
  - Lista de URL local 6
    - Agregar o editar URL local 7
    - Importar lista de URL 8
  - Servidores de filtro de URL 8
    - Agregar o editar el servidor de filtro de URL 9
  - Preferencia del filtrado de URL 10

**Gestión de configuración 1**

- Edición manual del archivo de configuración 1
- Editor de configuración 2
- Restablecer los valores por defecto de fábrica 3
- Esta función no se admite 6

**Información adicional acerca de... 1**

- Direcciones IP y máscaras de subred 1
  - Campos de host y red 3
- Configuraciones de interfaz disponibles 4
- Conjuntos de direcciones DHCP 5
- Significados de las palabras clave "permit" y "deny" 6
- Servicios y puertos 7

Información adicional acerca de NAT	14
Escenarios de traducción de direcciones estáticas	14
Escenarios de traducción de direcciones dinámicas	17
Motivos por los cuales Cisco SDM no puede modificar una regla NAT	19
Información adicional acerca de VPN	20
Recursos de Cisco.com	20
Información adicional acerca de conexiones VPN y políticas IPSec	21
Información adicional acerca de IKE	23
Información adicional acerca de las políticas IKE	24
Combinaciones de transformación permitidas	25
Motivos por los cuales una configuración de interfaz o subinterfaz de serie puede ser de sólo lectura	27
Motivos por los cuales una configuración de interfaz o subinterfaz ATM puede ser de sólo lectura	28
Motivos por los cuales una configuración de interfaz Ethernet puede ser de sólo lectura	29
Motivos por los cuales una configuración de interfaz ISDN (RDSI) BRI puede ser de sólo lectura	29
Motivos por los cuales una configuración de interfaz de módem analógico puede ser de sólo lectura	30
Escenario de utilización de políticas de firewall	32
Recomendaciones para la configuración de DMVPN	32
Informes técnicos sobre Cisco SDM	33
<b>Pasos iniciales</b>	<b>1</b>
¿Qué novedades trae esta versión?	2
Versiones de Cisco IOS admitidas	3

- Visualizar la información del router 1**
  - Aspectos generales 2
  - Estado de la interfaz 6
  - Estado de firewall 10
  - Estado del firewall de política basado en zonas 11
  - Estado de la red VPN 13
    - Túneles IPSec 13
    - Túneles DMVPN 15
    - Servidor Easy VPN 16
    - IKE SA 18
    - Componentes de SSL VPN 19
      - Contexto de SSL VPN 20
      - Sesiones de usuario 21
      - Truncado de URL 22
      - Mapeo de puertos 22
      - CIFS 22
      - Túnel completo 22
      - Lista de usuarios 23
  - Estado del tráfico 25
    - Usuarios más activos de Netflow 25
      - Protocolos más activos 25
      - Usuarios más activos 26
    - Calidad de servicio (QoS) 27
    - Tráfico de aplicaciones/protocolos 29
  - Estado de la red NAC 30
  - Registro 31
    - Syslog 32
    - Registro de firewall 34
    - Registro de Seguridad de la aplicación 37
    - Registro de mensajes SDEE 38



Estado de la red IPS	39
Estadísticas de firmas de IPS	41
Estadísticas de alertas de IPS	42
Estado de la autenticación 802.1x	43

### **Comandos del menú Archivo 1**

Guardar configuración en ejecución en el PC	1
Enviar configuración al router	1
Escribir en la configuración de inicio	2
Restablecer los valores por defecto de fábrica	2
Gestión de archivos	3
Cambiar nombre	6
Nueva carpeta	6
Guardar SDF a PC	6
Salir	6
No se ha podido realizar la compresión de flash	7

### **Comandos del menú Editar 1**

Preferencias	1
--------------	---

### **Comandos del menú Ver 1**

Inicio	1
Configurar	1
Supervisar	1
Configuración en ejecución	2
Mostrar comandos	2
Reglas de Cisco SDM por defecto	3
Actualizar	4

**Comandos del menú Herramientas 1**

Ping 1

Telnet 1

Auditoría de seguridad 1

Configuración de PIN del token USB 2

Aplicación inalámbrica 3

Actualizar Cisco SDM 3

Inicio de sesión en CCO 5

**Comandos del menú Ayuda 1**

Temas de Ayuda 1

Cisco SDM en CCO 1

Matriz de hardware/software 1

Acerca de este router... 2

Acerca de Cisco SDM 2



# CAPÍTULO 1

## Página de inicio

---

La página de inicio proporciona información básica acerca del hardware, el software y la configuración del router. Esta página contiene las secciones siguientes:

### Nombre de host

El nombre configurado del router.

### Acerca de su router

Muestra información básica sobre el hardware y el software del router y contiene los campos siguientes:

Hardware		Software	
<b>Tipo de modelo</b>	Muestra el número de modelo del router.	<b>Versión de IOS</b>	La versión del software Cisco IOS vigente en el router.
<b>Disponible / Memoria total</b>	RAM disponible / RAM total	<b>Versión de Cisco SDM</b>	La versión del software Cisco Router and Security Device Manager (Cisco SDM) vigente en el router.
<b>Capacidad de flash total</b>	Flash + Webflash (si es aplicable)		
<b>Disponibilidad de funciones</b>	Las funciones disponibles en la imagen de Cisco IOS que el router utiliza aparecen marcadas. Las funciones que Cisco SDM comprueba son: IP, Firewall, VPN, IPS y NAC.		

**Más...**

El enlace **Más...** muestra una ventana emergente que proporciona detalles de hardware y software adicionales.

- Detalles de hardware: además de la información presentada en la sección Acerca de su router, esta muestra ficha la siguiente información:
  - Si el router arranca desde el archivo Flash o desde la configuración.
  - Si el router tiene aceleradores; por ejemplo, aceleradores VPN.
  - Una diagrama de configuración de hardware incluyendo la memoria flash y los dispositivos instalados tales como flash USB y tokens USB.
- Detalles de software: además de la información presentada en la sección Acerca de su router, esta ficha muestra la siguiente información:
  - Los grupos de funciones incluidos en la imagen del IOS.
  - La versión de Cisco SDM en ejecución.

**Aspectos generales de configuración**

Esta sección de la página de inicio resume los parámetros de configuración que se han definido.

**Nota**


---

Si en la página de inicio no encuentra información sobre las funciones que se describen en este tema de ayuda, la imagen de Cisco IOS no admite la función. Por ejemplo, si el router está ejecutando una imagen de Cisco IOS que no admite funciones de seguridad, las secciones Política de firewall, VPN y Prevención de intrusiones no aparecerán en la página de inicio.

---

**Ver configuración vigente**

Haga clic en este botón para mostrar la configuración actual del router.

<b>Interfaces y conexiones</b>	<b>Activas (n):</b> el número de conexiones LAN y WAN que están activas.	<b>Inactivas (n):</b> el número de conexiones LAN y WAN que están inactivas.	<b>Punta de flecha doble:</b> haga clic aquí para mostrar u ocultar los detalles.
<b>LAN totales admitidas</b>	El número total de interfaces LAN que se encuentran en el router.	WAN totales admitidas	El número de interfaces WAN admitidas por Cisco SDM que se encuentran en el router.
<b>Interfaz de LAN configurada</b>	El número de interfaces LAN admitidas que se encuentran configuradas en el router.	Conexiones WAN totales	El número total de conexiones WAN admitidas por Cisco SDM que se encuentran en el router.
<b>Servidor DHCP</b>	Configurado/ No configurado		
<b>Grupo DHCP (vista detallada)</b>	Si se configura un grupo, la dirección inicial y la dirección final del grupo DHCP.  Si se han configurado varios grupos, la lista de los nombres de los grupos configurados.	<b>Nº de clientes DHCP (vista detallada)</b>	Número actual de clientes que ceden direcciones.
<b>Interfaz</b>	<b>Tipo</b>	<b>IP/Máscara</b>	<b>Descripción</b>
Nombre de la interfaz configurada	Tipo de interfaz	Dirección IP y máscara de subred	Descripción de la interfaz

<b>Políticas de firewall</b>	<b>Activo/inactivo</b>	<b>Fiable (n)</b>	<b>No fiable (n)</b>	<b>DMZ (n)</b>
	Activo: un firewall está en servicio. Inactivo: no hay ningún firewall en servicio.	El número de interfaces fiables (internas).	El número de interfaces no fiables (externas).	El número de interfaces DMZ.
<b>Interfaz</b>	<b>Icono de firewall</b>	<b>NAT</b>	<b>Regla de inspección</b>	<b>Regla de acceso</b>
El nombre de la interfaz a la que se ha aplicado el firewall	Si la interfaz se ha designado como interfaz interna o externa.	El nombre o número de la regla NAT que se ha aplicado a esta interfaz.	Los nombres o números de las reglas de inspección entrantes y salientes.	Los nombres o números de las reglas de acceso entrantes y salientes.

<b>VPN</b>	<b>Activas (n):</b> el número de conexiones VPN activas.		
<b>IPSec (sitio a sitio)</b>	El número de conexiones VPN sitio a sitio que se han configurado.	<b>GRE sobre IPSec</b>	El número de conexiones GRE sobre IPSec que se han configurado.
<b>Conexión a Xauth necesaria</b>	El número de conexiones Easy VPN que esperan un inicio de sesión de autenticación ampliada (Xauth). <i>Véase la nota.</i>	<b>Easy VPN remoto</b>	El número de conexiones del tipo Easy VPN remoto que se han configurado.
<b>Nº de clientes DMVPN</b>	Si el router está configurado como hub DMVPN, el número de clientes DMVPN.	<b>Nº de clientes VPN activos</b>	Si este router funciona como servidor Easy VPN, el número de clientes Easy VPN con conexiones activas.

<b>VPN</b>	<b>Activas (n):</b> el número de conexiones VPN activas.		
<b>Interfaz</b>	<b>Tipo</b>	<b>Política IPSec</b>	<b>Descripción</b>
El nombre de una interfaz con una conexión VPN configurada	El tipo de conexión VPN configurada en la interfaz.	El nombre de la política IPSec asociada a la conexión VPN.	Breve descripción de la conexión.



**Nota**

- Algunos concentradores o servidores VPN autentican a los clientes mediante la autenticación ampliada ([Xauth](#)). Aquí se muestra el número de túneles VPN que esperan un inicio de sesión de autenticación ampliada (Xauth). Si un túnel Easy VPN espera un inicio de sesión con ese tipo de autenticación, se muestra un panel de mensajes independiente con el botón Conexión. Al hacer clic en **Conexión** se permite al usuario especificar las credenciales para el túnel.
- Si se ha configurado Xauth para un túnel, éste no empezará a funcionar hasta que se haya proporcionado la conexión y la contraseña. No existe ningún límite de tiempo tras el cual se detenga la espera; esta información se esperará de forma indefinida.

<b>Políticas NAC</b>	<b>Activo o Inactivo</b>
<b>Columna Interfaz</b>	<b>Columna de Política NAC</b>
El nombre de la interfaz a la que se le aplica la política. Por ejemplo, FastEthernet 0, o Ethernet 0/0.	El nombre de la política NAC.

<b>Enrutamiento</b>		<b>Prevención de intrusiones</b>	
<b>Nº de rutas estáticas</b>	El número total de rutas estáticas configuradas en el router.	<b>Firmas activas</b>	El número de firmas activas que utiliza el router. Éstas pueden estar incorporadas, o cargarse desde una ubicación remota.
<b>Protocolos de enrutamiento dinámico</b>	Muestra una lista de todos los protocolos de enrutamiento dinámico que están configurados en el router.	<b>Nº de interfaces con IPS activada</b>	El número de interfaces del router con IPS activado.
		<b>Versión SDF</b>	La versión de los archivos SDF de este router.
		<b>Panel de seguridad</b>	Un enlace al Panel de seguridad de IPS en el que se pueden visualizar e implementar las diez firmas principales.





## CAPÍTULO 2

# Asistente para LAN

---

El Asistente para [LAN](#) de Cisco Router and Security Device Manager (Cisco SDM) le guía por el proceso de configuración de una interfaz LAN. La pantalla proporciona una lista de las interfaces LAN del router. Puede seleccionar cualquiera de las interfaces que se indican en la ventana y hacer clic en **Configurar** para convertir la interfaz en una LAN y configurarla.

En esta ventana se proporciona una lista de las interfaces del router que se han designado como interfaces internas en la configuración de inicio, así como una lista de las interfaces Ethernet y de los puertos de switch que aún no se han configurado como interfaces WAN. La lista incluye las interfaces que ya se han configurado.

Al configurar una interfaz como LAN, Cisco SDM inserta el texto de descripción \$ETH-LAN\$ en el archivo de configuración, para que en el futuro pueda reconocerla como una interfaz LAN.

### Interfaz

El nombre de la interfaz.

### Configurar

Haga clic en este botón para configurar una interfaz seleccionada. Si la interfaz nunca se ha configurado, Cisco SDM le guiará por el Asistente para LAN para ayudarlo a configurarla. Si la interfaz se ha configurado mediante Cisco SDM, Cisco SDM muestra una ventana de edición que permite cambiar los ajustes de configuración.

Si la interfaz LAN ha recibido una configuración no compatible con Cisco SDM, es posible que el botón Configurar esté desactivado. Para obtener una lista de este tipo de configuraciones, consulte [Motivos por los cuales una configuración de interfaz Ethernet puede ser de sólo lectura](#).

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Configurar o editar una interfaz o puerto de switch LAN.	Seleccione la interfaz o puerto de switch LAN de la lista y haga clic en <b>Configurar</b> . Si la interfaz no se ha configurado o si ha seleccionado un puerto de switch, Cisco SDM, le guiará por el Asistente para LAN que se puede utilizar para configurar la interfaz. Si la interfaz ya se ha configurado y no se trata de un puerto de switch, al hacer clic en <b>Configurar</b> , aparecerá una ventana de edición que permite cambiar la configuración de la LAN.
Volver a configurar la dirección IP, la máscara o las propiedades de DHCP de una interfaz que ya se ha configurado.	Seleccione una interfaz que disponga de una dirección IP y haga clic en <b>Configurar</b> .
Realizar configuraciones específicas relacionadas con la LAN para elementos como, por ejemplo, los servidores DHCP o los ajustes de unidad de transmisión máxima (MTU).	En la barra de categorías de Cisco SDM, haga clic en <b>Interfaces y conexiones</b> , seleccione la ficha <b>Editar interfaz/conexión</b> y cambie la configuración.
Ver cómo realizar tareas de configuración relacionadas.	<p>Consulte uno de los procedimientos siguientes:</p> <ul style="list-style-type: none"> <li>• <a href="#">¿Cómo se configura una ruta estática?</a></li> <li>• <a href="#">¿Cómo se visualiza la actividad en la interfaz LAN?</a></li> <li>• <a href="#">¿Cómo se activa o desactiva una interfaz?</a></li> <li>• <a href="#">¿Cómo se visualizan los comandos de IOS que se envían al router?</a></li> <li>• <a href="#">¿Cómo inicio la Aplicación inalámbrica de Cisco SDM?</a></li> </ul>

Puede volver a esta pantalla siempre que sea necesario para configurar interfaces LAN adicionales.

# Configuración de Ethernet

El asistente le guía por la configuración de una interfaz Ethernet en la LAN. Usted debe proporcionar la información siguiente:

- Una dirección IP y máscara de subred para la interfaz Ethernet
- Un conjunto de direcciones DHCP en el caso de utilizar DHCP en esta interfaz
- Las direcciones de los servidores DNS y WINS de la WAN
- Un nombre de dominio

## Asistente para LAN: Seleccionar una interfaz

En esta ventana puede seleccionar la interfaz en la que desea configurar una conexión LAN. La misma incluye una lista de las interfaces compatibles con las configuraciones LAN Ethernet.

## Asistente para LAN: Dirección IP/máscara de subred

Esta ventana permite configurar una dirección IP y máscara de subred para la interfaz Ethernet que se elija en la ventana anterior.

### Dirección IP

Especifique la [Dirección IP](#) de la interfaz en formato de decimales con puntos. El administrador de redes debe determinar las direcciones IP de las interfaces LAN. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

### Máscara de subred

Especifique la [máscara de subred](#). Obtenga este valor del administrador de redes. La máscara de subred permite que el router determine qué porción de la dirección IP se utilizará para definir la parte de red y de host de la dirección.

De manera alternativa, seleccione el número de [bits de red](#). Este valor se utiliza para calcular la máscara de subred. El administrador de redes le puede proporcionar el número de bits de red que debe especificar.

## Asistente para LAN: Activar Servidor DHCP

Esta pantalla permite activar un servidor [DHCP](#) en el router. Un servidor DHCP asigna automáticamente a los dispositivos de la LAN direcciones IP que se pueden volver a utilizar. Cuando un dispositivo se activa en la red, el servidor DHCP le concede una [Dirección IP](#). Cuando el dispositivo abandona la red, la dirección IP se devuelve al conjunto para que la pueda utilizar otro dispositivo.

**Para activar un servidor DHCP en el router:**

Haga clic en **Sí**.

## Asistente para LAN: Conjuntos de direcciones DHCP

Esta pantalla permite configurar el conjunto de direcciones IP de DHCP. Las direcciones IP que el servidor [DHCP](#) asigna se obtienen de un conjunto común que se ha configurado mediante la especificación de las direcciones IP inicial y final del intervalo.

Para obtener más información, consulte [Conjuntos de direcciones DHCP](#).



### Nota

---

Si en el router se han configurado conjuntos de direcciones discontinuos, los campos de dirección IP inicial e IP final serán de sólo lectura.

---

### IP inicial

Especifique el inicio del intervalo de direcciones IP que debe utilizar el servidor DHCP al asignar direcciones a los dispositivos de la LAN. Se trata de la dirección IP con el número más bajo del intervalo.

### IP final

Especifique la [Dirección IP](#) con el número más alto del intervalo de direcciones IP.

### Campos Servidor DNS y Servidor WINS

Si en esta ventana aparecen los campos Servidor DNS y Servidor WINS, puede hacer clic en [Opciones de DHCP](#) para obtener información acerca de ellos.

# Opciones de DHCP

Utilice esta ventana para establecer las opciones de DHCP que se enviarán a los hosts de la LAN que solicitan direcciones IP del router. No se trata de opciones que se definen para el router que está configurando, sino de parámetros que se enviarán a los hosts solicitantes de la LAN. Si desea establecer estas propiedades para el router, haga clic en **Tareas adicionales** de la barra de categorías de Cisco SDM, seleccione **DHCP** y configure estos ajustes en la ventana Conjuntos DHCP.

## Servidor DNS 1

El servidor DNS normalmente es un servidor que asigna un nombre de dispositivo conocido con su dirección IP. Si la red dispone de un servidor DNS configurado, especifique aquí la dirección IP del mismo.

## Servidor DNS 2

Si la red dispone de un servidor DNS adicional, en este campo puede especificar la dirección IP de éste.

## Nombre de dominio

El servidor DHCP que está configurando en este router proporcionará servicios a otros dispositivos dentro de este dominio. Especifique el nombre del dominio.

## Servidor WINS 1

Es posible que algunos clientes requieran el **WINS** (Windows Internet Naming Service) para conectarse a dispositivos en Internet. Si la red dispone de un servidor WINS, en este campo especifique la dirección IP del mismo.

## Servidor WINS 2

Si la red dispone de un servidor WINS adicional, en este campo especifique la dirección IP de dicho servidor.

## Asistente para LAN: Modo VLAN

Esta pantalla permite determinar el tipo de información de LAN virtual que se transmitirá a través del puerto de switch. Los puertos de switch pueden designarse en modo de acceso, en cuyo caso reenviarán solamente los datos destinados a la LAN virtual a la que están asignados, o bien en modo de enlace troncal, en cuyo caso reenviarán los datos destinados para todas las LAN virtuales, incluida la LAN virtual a la que están asignados.

Si este puerto de switch se conecta a un dispositivo de cliente como, por ejemplo, un PC o teléfono IP único, o si este dispositivo se conecta a un puerto en un dispositivo de red como, por ejemplo, otro switch, que es un puerto de modo de acceso, seleccione **Dispositivo de cliente**.

Si este puerto de switch se conecta a un puerto en un dispositivo de red como, por ejemplo, otro switch, que está en modo de enlace, seleccione **Dispositivo de red**.

## Asistente para LAN: Puerto del switch

Esta pantalla permite asignar un número de LAN virtual existente al puerto de switch o crear una nueva interfaz de LAN virtual que debe asignarse al puerto de switch de LAN virtual.

### LAN virtual existente

Si desea asignar el puerto de switch a una LAN virtual definida como, por ejemplo, la LAN virtual por defecto (LAN virtual 1), especifique el número de ID de LAN virtual en el campo Identificador (LAN virtual) de la red.

### Nueva LAN virtual

Si desea crear una nueva interfaz de LAN virtual a la que se asignará el puerto de switch, especifique el nuevo número de ID de LAN virtual en el campo Nueva LAN virtual y, a continuación, especifique la dirección IP y la máscara de subred de la nueva interfaz lógica de LAN virtual en los campos correspondientes.

**Incluya esta VLAN en un puente IRB que formará un puente con la red inalámbrica. (Utilice una aplicación inalámbrica para completar).**

Si marca esta casilla, el puerto del switch formará parte de un bridge con la red inalámbrica. La otra parte del bridge debe configurarse utilizando la Aplicación inalámbrica. La dirección IP y los campos para la dirección IP y la máscara de subred bajo la Nueva LAN virtual están desactivados cuando esta casilla está seleccionada.

Después de completar esta configuración LAN, haga lo siguiente para iniciar la Aplicación inalámbrica y completar la configuración de la interfaz inalámbrica.

- 
- Paso 1** Seleccione **Aplicación inalámbrica** del menú Herramientas de Cisco SDM. La Aplicación inalámbrica se abre en otra ventana del explorador.
- Paso 2** En la Aplicación inalámbrica, haga clic en **Seguridad rápida inalámbrica**, y luego haga clic en **Bridge** para proporcionar información para completar la configuración de la interfaz inalámbrica.
- 

## Puente IRB

Si está configurando una VLAN para que sea parte de un bridge IRB, el bridge debe ser un miembro del grupo bridge.

Para crear un nuevo grupo bridge del que esta interfaz será parte, haga clic en **Crear un nuevo grupo bridge** y especifique un valor en el rango de 1 a 255.

Para que esta LAN virtual sea miembro de un grupo bridge existente, haga clic en **Únase a un grupo bridge existente** y seleccione un grupo bridge.



### Nota

Cuando haya completado la configuración de la interfaz inalámbrica en la Aplicación inalámbrica, debe utilizar el mismo número de grupo bridge especificado en esta pantalla.

---

# Configuración BVI

Asigne una dirección IP y una máscara de subred a la interfaz BVI. Si seleccionó un grupo bridge existente en la pantalla anterior, la dirección IP y la máscara de subred aparecerán en la pantalla. Puede modificar los valores o dejarlos como están.

## Dirección IP

Especifique la [Dirección IP](#) de la interfaz en formato de decimales con puntos. El administrador de redes debe determinar las direcciones IP de las interfaces LAN. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

## Máscara de red

Especifique la [máscara de subred](#). Obtenga este valor del administrador de redes. La máscara de subred permite que el router determine qué porción de la dirección IP se utilizará para definir la parte de red y de host de la dirección.

## Net Bits (Bits de red)

De manera alternativa, seleccione el número de [bits de red](#). Este valor se utiliza para calcular la máscara de subred. El administrador de redes le puede proporcionar el número de bits de red que debe especificar.

# Conjunto DHCP para BVI

Al configurar el router como servidor DHCP, puede crear un conjunto de direcciones IP que pueden ser utilizadas por los clientes de la red. Cuando un cliente se desconecta de la red, la dirección que estaba utilizando es devuelta al conjunto para uso de otro host.



## Configuración del servidor DHCP

Haga clic en la casilla si desea que el router funcione como servidor DHCP. Luego, especifique las direcciones IP inicial y final en el conjunto. Asegúrese de especificar la dirección IP que se encuentren en la misma subred que la dirección IP que le dio a la interfaz. Por ejemplo, si le dio a la interfaz la dirección IP 10.10.22.1, con la máscara de subred 255.255.255.0, tiene más de 250 direcciones disponibles para el conjunto, y debe especificar la **Dirección IP inicial** 10.10.22.2 y la **Dirección IP final** 10.10.22.253.

## IRB para Ethernet

Si su router tiene una interfaz inalámbrica, puede utilizar Enrutamiento y establecimiento de bridge integrado para hacer que esta interfaz forme parte de un bridge a una LAN inalámbrica y permitir que el tráfico destinado para la red inalámbrica sea enrutado por esta interfaz. Haga clic en **Sí** si desea configurar esta interfaz de Nivel 3 para Enrutamiento o establecimiento de bridge integrado.

Si no desea que esta interfaz sea utilizada como bridge a la interfaz inalámbrica, haga clic en **No**. Todavía podrá configurarla como una interfaz regular del router.

## Configuración de Ethernet Nivel 3

Cisco SDM admite la configuración de Ethernet Nivel 3 en los routers con módulos de switch 3750 instalados. Usted puede crear configuraciones de VLAN y designar las interfaces de Ethernet del router como servidores DHCP.

## Configuración 802.1Q

Puede configurar una VLAN que no use el protocolo de encapsulación 802.1Q usado para conexiones de enlace. Suministre un número de identificación de la VLAN, y marque la opción **VLAN nativa** si no desea que la VLAN use el etiquetado 802.1Q.

Si usted desea usar el etiquetado 802.1Q, deje el cuadro VLAN nativa sin marcar.

## Configuración del enlace o enrutamiento

Usted puede configurar interfaces de Ethernet Nivel 3 para el enlace 802.1Q o para enrutamiento básico. Si usted configura la interfaz para el enlace 802.1Q, podrá configurar VLANs en la interfaz, y podrá configurar una VLAN nativa que no use el protocolo de encapsulación 802.1q. Si usted configura la interfaz para enrutamiento, no podrá configurar las subinterfaces o VLANs adicionales en la interfaz.

## Módulo de configuración del dispositivo del switch

Si usted está configurando una interfaz de Ethernet de Gigabits para enrutamiento, podrá suministrar información sobre el módulo del switch en esta ventana. No se requiere que proporcione esta información.

Usted podrá suministrar una dirección IP y una máscara de subred para el módulo del switch, y las credenciales de inicio de sesión requeridas para ingresar a la interfaz del módulo del switch.

Marque la casilla al final de la pantalla si desea entrar al módulo del switch después de suministrar información en este asistente y entregar la configuración al router.

## Configurar interfaz de Ethernet de gigabits

Proporcione información de la dirección IP y la máscara de subred para las interfaces Gigabit Ethernet en esta ventana. Para obtener más información sobre las direcciones IP y las máscaras de subred, consulte [Asistente para LAN: Dirección IP/máscara de subred](#).

### Dirección IP de la interfaz física

Suministre la dirección IP y la máscara de subred para la interfaz de Ethernet de Gigabits física en estos campos.

## Dirección IP de la subinterfaz de la VLAN

Suministre la dirección IP y la máscara de subred para la subinterfaz de la VLAN que desee crear en la interfaz física. Estos campos aparecen si usted está configurando esta interfaz para el enrutamiento. Estos campos no aparecen si usted está configurando esta interfaz para el enrutamiento y bridge integrado (IRB, Integrated Routing and Bridging).

## Resumen

En esta ventana se proporciona un resumen de los cambios en la configuración que ha realizado para la interfaz seleccionada.

### Para guardar esta configuración en la configuración en ejecución del router y salir de este asistente:

Haga clic en **Finalizar**. Cisco SDM guarda los cambios de configuración en la configuración en ejecución del router. Aunque los cambios se aplican inmediatamente, los mismos se perderán si se apaga el router.

Si ha marcado la opción **Obtener una vista previa de los comandos antes de enviarlos al router** de la ventana Preferencias del usuario, aparecerá la ventana Enviar. Esta ventana permite ver los comandos CLI que se envían al router.

## Cómo...

En esta sección se incluyen procedimientos para las tareas que el asistente no le ayuda a llevar a cabo.

## ¿Cómo se configura una ruta estática?

Para configurar una [ruta estática](#):

- 
- Paso 1** En la barra de categorías, haga clic en **Enrutamiento**.
  - Paso 2** En el grupo Enrutamiento estático, haga clic en **Agregar...**  
Aparecerá el cuadro de diálogo Agregar ruta estática de IP.

- Paso 3** En el campo Prefijo, especifique la dirección IP de la red de destino de la ruta estática.
- Paso 4** En el campo Máscara de prefijo, especifique la máscara de subred de la red de destino.
- Paso 5** Si desea que esta ruta estática sea la ruta por defecto, marque la casilla de verificación **Convierta esta ruta en la ruta por defecto**.
- Paso 6** En el grupo Envío, seleccione si se debe identificar una interfaz de router o la dirección IP del router de destino como el método para enviar datos y, a continuación, seleccione la interfaz del router de envío o especifique la dirección IP del router de destino.
- Paso 7** De manera opcional, en el campo Distance Metric (Distancia métrica), especifique la distancia métrica que debe almacenarse en la tabla de enrutamiento.
- Paso 8** Si desea configurar esta ruta estática como la ruta permanente, lo que significa que no se eliminará incluso si se desactiva la interfaz o si el router no se puede comunicar con el router siguiente, marque la casilla de verificación **Ruta permanente**.
- Paso 9** Haga clic en **Aceptar**.
- 

## ¿Como se visualiza la actividad en la interfaz LAN?

La actividad de una interfaz LAN puede visualizarse mediante el modo Supervisión en Cisco SDM. El mencionado modo puede mostrar estadísticas sobre la interfaz LAN, incluido el número de paquetes y bytes que la interfaz ha enviado o recibido y el número de errores en dichos procesos. Para ver las estadísticas sobre una interfaz LAN:

- 
- Paso 1** En la barra de herramientas, haga clic en **Supervisar**.
- Paso 2** En el panel izquierdo, haga clic en **Estado de la interfaz**.
- Paso 3** En el campo Seleccione una interfaz, elija la interfaz LAN cuyas estadísticas desee visualizar.

- Paso 4** Para seleccionar el elemento o elementos de datos que desee visualizar, marque las casillas de verificación correspondientes. Puede ver un máximo de cuatro estadísticas a la vez.
- Paso 5** Para ver las estadísticas de todos los elementos de datos seleccionados, haga clic en **Iniciar Supervisión**.

Aparecerá la ventana Detalles de la interfaz que muestra todas las estadísticas seleccionadas. Por defecto, la ventana muestra los datos en tiempo real, de modo que sondea el router cada 10 segundos. Si la interfaz está activa y se transmiten datos sobre ella, deberá observar un aumento en el número de paquetes y bytes que se transfieren a través de la misma.

---

## ¿Cómo se activa o desactiva una interfaz?

Una interfaz puede desactivarse sin quitar su configuración. También es posible reactivar una interfaz desactivada.

- 
- Paso 1** En la barra de categorías, haga clic en **Interfaces y conexiones**.
- Paso 2** Haga clic en la ficha **Editar interfaz/conexión**.
- Paso 3** Seleccione la interfaz que desee desactivar o activar.
- Paso 4** Si la interfaz está activada, aparecerá el botón Desactivar debajo de la lista de interfaces. Haga clic en dicho botón para activar la interfaz. Si la interfaz está desactivada, aparecerá el botón Activar debajo de la lista de interfaces. Haga clic en dicho botón para activar la interfaz.
-

## ¿Cómo se visualizan los comandos de IOS que se envían al router?

Si está finalizando un asistente para configurar una función, puede ver los comandos de Cisco IOS que se envían al router haciendo clic en **Finalizar**.

- 
- Paso 1** En el menú Editar de Cisco SDM, seleccione **Preferencias**.
  - Paso 2** Marque la casilla **Obtener una vista previa de los comandos antes de enviarlos al router**.
  - Paso 3** Haga clic en **Aceptar**.
- 

La próxima vez que utilice un asistente para configurar el router y haga clic en **Finalizar** en la ventana Resumen, aparecerá la ventana Enviar. En esta ventana puede ver los comandos que está enviando a la configuración del router. Cuando haya terminado de revisar los comandos, haga clic en **Enviar**.

Si está editando una configuración, la ventana Enviar aparece al hacer clic en **Aceptar** en la ventana del cuadro de diálogo. Esta ventana permite ver los comandos de Cisco IOS que se envían al router.

## ¿Cómo inicio la Aplicación inalámbrica de Cisco SDM?

Utilice el siguiente procedimiento para iniciar la aplicación inalámbrica de Cisco SDM.

- 
- Paso 1** Vaya al menú Herramientas de Cisco SDM y seleccione **Aplicación inalámbrica**. **La Aplicación inalámbrica se inicia en otra ventana del explorador**.
  - Paso 2** En el panel izquierdo, haga clic en el título de la pantalla de configuración en la que desea trabajar. Para obtener ayuda para cualquier pantalla, haga clic en el icono de ayuda en la esquina superior derecha. Este icono es un libro abierto con un signo de pregunta.
-



## CAPÍTULO 3

# Autenticación 802.1x

---

La autenticación 802.1x permite que un router remoto de Cisco IOS conecte usuarios VPN autenticados a una red segura mediante un túnel VPN que está constantemente activado. El router de Cisco IOS autenticará los usuarios mediante un servidor RADIUS en la red segura.

La autenticación 802.1x se aplica a puertos de switch o puertos Ethernet (enrutados), pero no a ambos tipos de interfaces. Si la autenticación 802.1x se aplica a un puerto Ethernet, los usuarios no autenticados se pueden enrutar a Internet afuera del túnel VPN.

La autenticación 802.1x se configura en las interfaces utilizando el asistente para LAN. Sin embargo, antes de que pueda activar 802.1x en alguna interfaz, debe activar AAA en el router de Cisco IOS. Si intenta usar el asistente para LAN antes de activar AAA, aparece una ventana que le solicita su confirmación para activar AAA. Si elige activar AAA, las pantallas de configuración de 802.1x aparecen como parte del asistente para LAN. Si elige *no* activar AAA, las pantallas de configuración de 802.1x *no* aparecen.

# Asistente para LAN: Autenticación 802.1x (puertos de switch)

Esta ventana le permite activar la autenticación 802.1x en el o los puertos de switch que seleccionó para configuración, utilizando el asistente para LAN.

## Activar autenticación 802.1x

Marque **Activar autenticación 802.1x** para activar la autenticación 802.1x en el puerto de switch.

## Modo host

Elija **Único** o **Múltiple**. El modo único permite el acceso de sólo un cliente autenticado. El modo múltiple permite el acceso de varios clientes después de la autenticación de un cliente.



### Nota

---

Los puertos en los routers Cisco 85x y Cisco 87x se pueden definir sólo en modo host múltiple. El modo único está desactivado para estos routers.

---

## VLAN de invitado

Marque **VLAN de invitado** para activar una red VLAN para clientes que no tienen soporte 802.1x. Si activa esta opción, elija una red VLAN desde la lista desplegable de VLAN.

## Fallos de autenticación de VLAN

Marque **Fallos de autenticación de VLAN** para activar una red VLAN para clientes que no tienen autorización 802.1x. Si activa esta opción, elija una red VLAN desde la lista desplegable de VLAN.



## Reautenticación periódica

Marque **Reautenticación periódica** para imponer la reautenticación de los clientes 802.1x en un intervalo regular. Elija configurar el intervalo localmente o permitir que el servidor RADIUS defina el intervalo. Si elige configurar el intervalo de reautenticación localmente, especifique un valor entre 1 y 65535 segundos. El valor por defecto es 3600 segundos.

## Opciones avanzadas

Haga clic en **Opciones avanzadas** para abrir una ventana con parámetros de autenticación 802.1x adicionales.

## Opciones avanzadas

Esta ventana le permite cambiar los valores por defecto para varios parámetros de autenticación 802.1x.

### Límite de tiempo de servidor RADIUS

Especifique el tiempo, en segundos, que el router Cisco IOS espera antes de alcanzar el límite de tiempo de su conexión al servidor RADIUS. Los valores deben estar entre 1 y 65535 segundos. El valor por defecto es 30 segundos.

### Límite de tiempo de respuesta del suppliant

Especifique el tiempo, en segundos, que el router Cisco IOS espera una respuesta de un cliente 802.1x antes de alcanzar el límite de tiempo de su conexión a ese cliente. Los valores deben estar entre 1 y 65535 segundos. El valor por defecto es 30 segundos.

### Límite de tiempo de reintentos del suppliant

Especifique el tiempo, en segundos, que el router Cisco IOS reintenta un cliente 802.1x antes de alcanzar el límite de tiempo de su conexión a ese cliente. Los valores deben estar entre 1 y 65535 segundos. El valor por defecto es 30 segundos.

### Período tranquilo

Especifique el tiempo, en segundos, que el router Cisco IOS espera entre la conexión inicial a un cliente y el envío de una solicitud de inicio de sesión. Los valores deben estar entre 1 y 65535 segundos. El valor por defecto es 60 segundos.

### Período límite de velocidad

Los valores deben estar entre 1 y 65535 segundos. Sin embargo, el valor por defecto es 0 segundos, lo que desactiva el **Período límite de velocidad**.

### Máximo de intentos de reautenticación

Especifique el número máximo de veces que el router Cisco IOS intenta reautenticar un cliente 802.1x. Los valores deben estar entre 1 y 10. El valor por defecto es 2.

### Máximo de reintentos

Especifique el número máximo de solicitudes de inicio de sesión que se pueden enviar al cliente. Los valores deben estar entre 1 y 10. El valor por defecto es 2.

### Restablecer valores por defecto

Haga clic en **Restablecer valores por defecto** para restablecer todas las opciones avanzadas a sus valores por defecto.

# Asistente para LAN: Servidores RADIUS para autenticación 802.1x

La información de autenticación 802.1x se configura y guarda en una base de datos de políticas que reside en servidores RADIUS que ejecutan Cisco Secure ACS, versión 3.3. El router debe validar las credenciales de los clientes 802.1x comunicándose con un servidor RADIUS. Utilice esta ventana para proporcionar la información que el router necesita para contactarse con uno o más servidores RADIUS. Cada servidor RADIUS que usted especifique deberá tener el software de ACS Seguro de Cisco versión 3.3, instalado y configurado.



## Nota

Todas las interfaces del router Cisco IOS activadas con autorización 802.1x utilizarán los servidores RADIUS configurados en esta ventana. Cuando configure una nueva interfaz, verá nuevamente esta pantalla. Sin embargo, no se deben realizar adiciones o cambios a la información del servidor RADIUS.

## Seleccionar el origen de cliente RADIUS

Configurar el origen RADIUS le permite especificar la dirección IP del origen que se enviará en paquetes RADIUS con destino al servidor RADIUS. Si necesita más información sobre una interfaz, escoja la interfaz y haga clic en el botón **Detalles**.

La dirección IP del origen en los paquetes RADIUS enviados desde el router debe configurarse como la dirección IP del NAD en la versión 3.3 o superior de Cisco ACS.

Si selecciona **El router elige el origen**, la dirección IP del origen en los paquetes RADIUS será la dirección de la interfaz a través de la cual los paquetes RADIUS saldrán del router.

Si elige una interfaz, la dirección IP del origen en los paquetes RADIUS será la dirección de la interfaz que usted escoja como el origen de cliente RADIUS.



## Nota

El software Cisco IOS permite que una interfaz de origen RADIUS única se configure en el router. Si el router ya tiene configurado un origen RADIUS y usted elige un origen diferente, la dirección IP del origen colocada en los paquetes enviados al servidor RADIUS cambia a la dirección IP del nuevo origen, y es probable que no coincida con la dirección IP del NAD configurada en Cisco ACS.

## Detalles

Si necesita una visión rápida de la información sobre una interfaz antes de seleccionarla, haga clic en **Detalles**. La pantalla le mostrará la dirección IP y la máscara de subred, las reglas de acceso y las reglas de inspección aplicadas a la interfaz, la política de IPSec y la política de QoS aplicadas, y si hay una configuración de Easy VPN en la interfaz.

## Columnas de Servidor IP, Límite de tiempo y Parámetros

Columnas de Servidor IP, Límite de tiempo y parámetros contienen la información que el router usa para comunicarse con un servidor RADIUS. Si no hay información del servidor RADIUS relacionada con la interfaz elegida, estas columnas quedarán en blanco.

## Casilla de verificación Usar para 802.1x

Marque esta casilla si desea utilizar el servidor RADIUS que aparece en la lista para 802.1x. El servidor debe tener configurada la información de autorización de 802.1x requerida si 802.1x se utiliza correctamente.

## Agregar, editar y enviar un ping

Para suministrar información a un servidor RADIUS, haga clic en el botón **Agregar** e introduzca la información en la pantalla mostrada. Elija una fila y haga clic en **Editar** para modificar la información para un servidor RADIUS. Escoja una fila y haga clic en **Ping** para probar la conexión entre el router y el servidor RADIUS.



### Nota

Cuando se esté efectuando una prueba de ping, introduzca la dirección IP de la interfaz del origen RADIUS en el campo de origen en el diálogo de ping. Si usted elige **El router elige el origen**, no necesitará proporcionar ningún valor en el campo de origen del diálogo de ping.

Los botones **Editar** y **Ping** se desactivan cuando no hay ninguna información del servidor RADIUS disponible para la interfaz elegida.

# Editar autenticación 802.1x (puertos de switch)

Esta ventana le permite activar y configurar parámetros de autenticación 802.1x.

Si el mensaje “802.1x no se puede configurar para un puerto que funciona en modo de enlace.” aparece en lugar de los parámetros de autenticación 802.1x, el switch no puede tener activada la autenticación 802.1x.

Si los parámetros de autenticación 802.1x aparecen pero están desactivados, entonces una de las siguientes afirmaciones es verdadera:

- AAA no se ha activado.

Para activar AAA, vaya a **Configurar > Tareas adicionales > AAA**.

- AAA se activó, pero no se ha configurado una política de autenticación 802.1x.

Para configurar una política de autenticación 802.1x, vaya a **Configurar > Tareas adicionales > AAA > Políticas de autenticación > 802.1x**.

## Activar autenticación 802.1x

Marque **Activar autenticación 802.1x** para activar la autenticación 802.1x en este puerto de switch.

## Modo host

Elija **Único** o **Múltiple**. El modo único permite el acceso de sólo un cliente autenticado. El modo múltiple permite el acceso de varios clientes después de la autenticación de un cliente.



### Nota

---

Los puertos en los routers Cisco 87x se pueden definir sólo en modo host múltiple. El modo único está desactivado para estos routers.

---

## VLAN de invitado

Marque **VLAN de invitado** para activar una red VLAN para clientes que no tienen soporte 802.1x. Si activa esta opción, elija una red VLAN desde la lista desplegable de VLAN.

## Fallos de autenticación de VLAN

Marque **Fallos de autenticación de VLAN** para activar una red VLAN para clientes que no tienen autorización 802.1x. Si activa esta opción, elija una red VLAN desde la lista desplegable de VLAN.

## Reautenticación periódica

Marque **Reautenticación periódica** para imponer la reautenticación de los clientes 802.1x en un intervalo regular. Elija configurar el intervalo localmente o permitir que el servidor RADIUS defina el intervalo. Si elige configurar el intervalo de reautenticación localmente, especifique un valor entre 1 y 65535 segundos. El valor por defecto es 3600 segundos.

## Opciones avanzadas

Haga clic en **Opciones avanzadas** para abrir una ventana con parámetros de autenticación 802.1x adicionales.

# Asistente para LAN: Autenticación 802.1x (VLAN o Ethernet)

Esta ventana le permite activar la autenticación 802.1x en el puerto Ethernet que seleccionó para configuración, utilizando el asistente para LAN. Para routers Cisco 87x, esta ventana está disponible para configurar una VLAN con autenticación 802.1x.



### Nota

---

Antes de configurar 802.1x en la VLAN, asegúrese de que 802.1x *no* esté configurado en ningún puerto de switch de VLAN. Asegúrese también de que la VLAN esté configurada para DHCP.

---

## Utilizar autenticación 802.1x para separar tráfico fiable y no fiable en la interfaz

Marque **Utilizar autenticación 802.1x para separar el tráfico fiable y no fiable en la interfaz** para activar autenticación 802.1x.

## Conjunto de direcciones IP de DHCP para clientes 802.1x que no son fiables

Para activar una conexión a Internet para clientes que no tienen autenticación 802.1x, a cada cliente no fiable se le debe asignar una dirección IP única. Estas direcciones IP pueden venir de un conjunto de direcciones IP nuevo o existente, pero los conjuntos usados no se pueden superponer con las direcciones IP de alguna de las interfaces existentes del router Cisco IOS.



### Nota

El conjunto de direcciones IP se puede superponer con la dirección IP utilizada para una interfaz de retrobucle. Sin embargo, se le solicitará que confirme dicha superposición antes de que se permita.

Elija **Crear un conjunto nuevo** para configurar un nuevo conjunto de direcciones IP para emitir direcciones IP a clientes que no son fiables. Los campos siguientes pueden estar completos con información ingresada anteriormente, pero usted puede cambiarlos o llenarlos:

<b>Red</b>	Especifique la dirección de red IP desde la cual se deriva el conjunto de direcciones IP.
<b>Máscara de subred</b>	Especifique la máscara de subred para definir la red y las partes de host de la dirección IP especificada en el campo <b>Red</b> .
<b>Servidor DNS 1</b>	El servidor DNS es un servidor que asigna un nombre de dispositivo conocido a su dirección IP. Si se configura un servidor DNS para su red, especifique la dirección IP para ese servidor.
<b>Servidor DNS 2</b>	Si hay un servidor DNS adicional en la red, especifique la dirección IP para ese servidor.

**Servidor WINS 1**

Algunos clientes pueden necesitar Windows Internet Naming Service (WINS) para conectarse a dispositivos de Internet. Si hay un servidor WINS en la red, especifique la dirección IP para ese servidor.

**Servidor WINS 2**

Si hay un servidor WINS adicional en la red, especifique la dirección IP para ese servidor.

Si hay un conjunto de direcciones IP existente que desea usar para emitir direcciones IP a clientes que no son fiables, elija **Seleccionar un conjunto existente**. Elija el conjunto existente desde el menú desplegable. Para ver más información acerca de un conjunto existente, haga clic en **Detalles**.

**Listas de excepciones**

Haga clic en **Listas de excepciones** para crear o editar una lista de excepciones. Una lista de excepciones exime de autenticación 802.1x a determinados clientes mientras les permite usar el túnel VPN.

**Eximir a los teléfonos Cisco IP de autenticación 802.1x**

Marque **Eximir los teléfonos Cisco IP de autenticación 802.1x** para eximir a los teléfonos Cisco IP de autenticación 802.1x mientras les permite usar el túnel VPN.

**Listas de excepciones de 802.1x**

Una lista de excepciones exime de autenticación 802.1x a determinados clientes mientras les permite usar el túnel VPN. Los clientes eximidos se identifican por sus direcciones MAC.

**Agregar**

Haga clic en **Agregar** para abrir una ventana donde pueda agregar la dirección MAC de un cliente. La dirección MAC debe estar en el formato que coincida con uno de estos ejemplos:

- 0030.6eb1.37e4
- 00-30-6e-b1-37-e4



Cisco SDM rechaza direcciones MAC que tienen formato incorrecto, excepto direcciones MAC más cortas que los ejemplos dados. Las direcciones MAC más cortas se rellenarán con un “0” (cero) por cada dígito que falte.

**Nota**

---

La función 802.1x de Cisco SDM no admite la opción CLI que asocia políticas con direcciones MAC, y no se incluirá en las direcciones MAC de la lista de excepciones que tienen una política asociada con ellas.

---

**Eliminar**

Haga clic en **Eliminar** para eliminar un cliente seleccionado de la lista de excepciones.

## Autenticación 802.1x en interfaces de capa 3

Esta ventana le permite configurar autenticación 802.1x en una [Interfaz de capa 3](#). Enumera puertos Ethernet e interfaces VLAN que se han configurado o que se pueden configurar con autenticación 802.1x, le permite seleccionar una interfaz de plantilla virtual para clientes no fiables y crea una lista de excepciones para que los clientes omitan la autenticación 802.1x.

**Nota**

---

Si las políticas se han definido utilizando la CLI, aparecerán como información de sólo lectura en esta ventana. En este caso, sólo se permite activar o desactivar 802.1x en esta ventana.

---

**Tareas previas**

Si aparece una tarea previa en la ventana, ésta debe finalizarse antes de que la autenticación 802.1x se pueda configurar. Se muestra un mensaje que explica la tarea previa, junto con un enlace a la ventana donde se puede finalizar la tarea.

**Activar globalmente la autenticación 802.1x**

Marque **Activar globalmente la autenticación 802.1x** para activar la autenticación 802.1x en todos los puertos Ethernet.

## Tabla de interfaces

La tabla de interfaces tiene las siguientes columnas:

**Interfaz:** muestra el nombre de la interfaz Ethernet o VLAN.

**Autenticación 802.1x:** indica si la autenticación 802.1x está activada para el puerto Ethernet.

## Editar

Haga clic en **Editar** para abrir una ventana con parámetros de autenticación 802.1x editables. Los parámetros son los ajustes de autenticación 802.1x para la interfaz elegida en la tabla de interfaces.

## Política de usuarios no fiables

Elija una interfaz de plantilla virtual desde la lista desplegable. La interfaz de plantilla virtual elegida representa la política que se aplica a clientes que no tienen autenticación 802.1x.

Para ver más información acerca de la interfaz de plantilla virtual elegida, haga clic en el botón **Detalles**.

## Lista de excepciones

Para obtener más información acerca de la lista de excepciones, consulte [Listas de excepciones de 802.1x](#).

## Eximir a los teléfonos Cisco IP de autenticación 802.1x

Marque **Eximir los teléfonos Cisco IP de autenticación 802.1x** para eximir a los teléfonos Cisco IP de autenticación 802.1x mientras les permite usar el túnel VPN.

## Aplicar cambios

Haga clic en **Aplicar cambios** para que los cambios realizados se apliquen.

## Descartar cambios

Haga clic en **Descartar cambios** para borrar los cambios realizados que no se aplicaron.

## Editar la autenticación 802.1x

Esta ventana le permite activar y cambiar los valores por defecto para varios parámetros de autenticación 802.1x.

### Activar la autenticación 802.1x

Marque **Activar la autenticación 802.1x** para activar la autenticación 802.1x en el puerto Ethernet.

### Reautenticación periódica

Marque **Reautenticación periódica** para imponer la reautenticación de los clientes de 802.1x en un intervalo regular. Elija configurar el intervalo localmente o permitir que el servidor RADIUS defina el intervalo. Si elige configurar el intervalo de reautenticación localmente, especifique un valor entre 1 y 65535 segundos. El valor por defecto es 3600 segundos.

### Opciones avanzadas

Haga clic en [Opciones avanzadas](#) para ver descripciones de los campos en el cuadro Opciones avanzadas.

## ¿Cómo...

Esta sección contiene procedimientos para tareas que el asistente no le ayuda a finalizar.

### ¿Cómo configuro autenticación 802.1x en más de un puerto Ethernet?

Una vez que configure la autenticación 802.1x en una interfaz, el asistente para LAN ya no mostrará ninguna opción 802.1x para puertos Ethernet, porque Cisco SDM utiliza la configuración 802.1x de manera global.

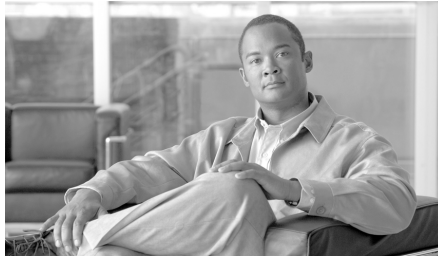
**Nota**

---

Para configurar switches, el asistente para LAN continuará mostrando las opciones 802.1x.

---

Si desea editar la configuración de autenticación 802.1x en un puerto Ethernet, vaya a **Configurar > Tareas adicionales > 802.1x**.



# CAPÍTULO 4

## Asistentes para crear conexiones

---

Los asistentes para crear conexiones permiten configurar conexiones LAN y WAN para todas las interfaces compatibles con Cisco SDM.

### Crear conexión

Esta ventana permite crear nuevas conexiones LAN y WAN.



**Nota**

---

Cisco SDM no puede utilizarse para crear conexiones WAN para los routers Cisco de la serie 7000.

---

### Crear nueva conexión

Escoja un tipo de conexión para configurar en las interfaces físicas disponibles en su router. Sólo están disponibles las interfaces que no han sido configuradas. Cuando usted hace clic en el botón de opción para un tipo de conexión, un diagrama del escenario del caso aparecerá para ilustrar ese tipo de conexión. Si todas las interfaces han sido configuradas, no se mostrará esta área de la ventana.

Si el router tiene interfaces de modo de transferencia asíncrona (ATM) o serie, es posible configurar varias conexiones a partir de una misma interfaz debido a que Cisco Router and Security Device Manager II (Cisco SDM) configura subinterfaces para cada interfaz de dicho tipo.

El botón de opción Otros (no admitido por Cisco SDM) aparece si existe alguna interfaz lógica o física no admitida o si existe una interfaz admitida a la que se ha asignado una configuración no admitida. Cuando hace clic en el botón de opción Otros (no admitido por Cisco SDM), el botón Crear nueva conexión se desactivará.

Si el router tiene interfaces de radio, pero usted no ve un botón de opción **Inalámbrico**, no ha ingresado al sistema como administrador de Cisco SDM. Si tiene que usar la aplicación inalámbrica, vaya al menú Herramientas de Cisco SDM y elija **Aplicación inalámbrica**.

**¿Qué desea hacer?**

<b>Si desea:</b>	<b>Haga lo siguiente:</b>
Saber cómo ejecutar configuraciones para las que este asistente no proporciona ninguna ayuda.	Consulte uno de los procedimientos siguientes: <ul style="list-style-type: none"> <li>• <a href="#">¿Cómo se visualizan los comandos de IOS que se envían al router?</a></li> <li>• <a href="#">¿Cómo se configura una interfaz WAN no admitida?</a></li> <li>• <a href="#">¿Cómo se activa o desactiva una interfaz?</a></li> <li>• <a href="#">¿Cómo se visualiza la actividad en la interfaz WAN?</a></li> <li>• <a href="#">¿Cómo se configura NAT en una interfaz WAN?</a></li> <li>• <a href="#">¿Cómo se configura una ruta estática?</a></li> <li>• <a href="#">¿Cómo se configura un protocolo de enrutamiento dinámico?</a></li> <li>• <a href="#">¿Cómo se configura el enrutamiento de marcación a petición para la interfaz asíncrona o ISDN?</a></li> </ul>
Configurar una interfaz no admitida por Cisco SDM.	Vea la guía de configuración de software para el router para usar el CLI para configurar la interfaz.

## Ventana de bienvenida de la interfaz del asistente para WAN

Esta ventana incluye una lista de los tipos de conexiones que se pueden configurar para esta interfaz mediante Cisco SDM. Si requiere configurar otro tipo de conexión para esta interfaz, puede hacerlo mediante el CLI.

## Ventana de bienvenida de la interfaz del asistente para ISDN (RDSI)

PPP es el único tipo de codificación admitido en un ISDN (RDSI) BRI por Cisco SDM.

## Ventana de bienvenida del módem analógico

PPP es el único tipo de codificación que Cisco SDM admite sobre una conexión por módem analógico.

## Ventana de bienvenida de la conexión de reserva auxiliar

La opción de configurar el puerto AUXILIAR como sólo una conexión de acceso telefónico aparece para los routers Cisco 831 y 837.

El botón de opción Auxiliar de acceso telefónico está desactivado si existen cualquiera de las condiciones siguientes:

- Existe más de una ruta por defecto.
- Una ruta por defecto existe y está configurada con una interfaz aparte de la interfaz WAN primaria.

La opción Auxiliar de acceso telefónico no se muestra si existen cualquiera de las condiciones siguientes:

- El router no está usando una imagen de Cisco IOS que soporte la función Auxiliar de acceso telefónico.
- La interfaz WAN primaria no está configurada.
- La interfaz asíncrona ya está configurada.
- La interfaz asíncrona no es configurable por Cisco SDM debido a la presencia de comandos de Cisco IOS no admitidos en la configuración existente.

## Seleccionar la interfaz

Esta ventana aparece si hay más de una interfaz del tipo que usted seleccionó en la ventana Crear conexión. Seleccione la interfaz que desee utilizar para esta conexión.

Si está configurando una interfaz Ethernet, Cisco SDM inserta el texto de descripción \$ETH-WAN\$ en el archivo de configuración de modo que, en el futuro, reconocerá la interfaz como una interfaz WAN.

## Encapsulación: PPPoE

Esta ventana permite activar la encapsulación del protocolo punto a punto sobre Ethernet (PPPoE), lo cual será necesario si el proveedor de servicios o el administrador de redes requiere routers remotos para establecer comunicación mediante PPPoE.

PPPoE es un protocolo que utilizan muchos proveedores de servicios de línea de suscriptor digital asimétrico (ADSL). Pregunte a su proveedor de servicios si su conexión utiliza PPPoE.

Si elige la encapsulación PPPoE, Cisco SDM agrega de forma automática una interfaz de marcación a la configuración y la mostrará en la ventana Resumen.



## Activar encapsulación PPPoE

Si el proveedor de servicios requiere que el router utilice PPPoE, marque esta casilla para activar la encapsulación PPPoE. De lo contrario, desmárquela. Esta casilla de verificación no estará disponible si el router ejecuta una versión de Cisco IOS que no admite la encapsulación PPPoE.

# Dirección IP: ATM o Ethernet con PPPoE/PPPoA

Elija el método que utilizará la interfaz WAN para obtener una dirección IP.

## Dirección IP estática

Si selecciona **Dirección IP estática**, indique la dirección IP y la máscara de subred o los bits de la red en los campos proporcionados.

## Dinámica (cliente DHCP)

Si selecciona **Dinámica**, el router aceptará una dirección IP de un servidor DHCP remoto. Especifique el nombre del servidor DHCP que asignará las direcciones.

## IP no numerado

Seleccione **IP no numerado** cuando desee que la interfaz comparta una dirección IP que ya se ha asignado a otra interfaz. Luego escoja la interfaz cuya dirección IP desea usar para la interfaz que está configurando.

## IP simple (IP negociado)

Seleccione **IP simple (IP negociado)** cuando el router obtendrá una dirección IP a través de la negociación de direcciones PPP/IPCP.

## DNS dinámico

Escoja un DNS dinámico si desea actualizar sus servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN. Haga clic en el botón **DNS dinámico** para configurar el DNS dinámico.

# Dirección IP: ATM con enrutamiento RFC 1483

Elija el método que utilizará la interfaz WAN para obtener una dirección IP.

## Dirección IP estática

Si selecciona **Dirección IP estática**, indique la dirección IP y la máscara de subred o los bits de la red en los campos proporcionados. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

## Dinámica (cliente DHCP)

Si selecciona esta opción, el router aceptará una dirección IP de un servidor DHCP remoto. Especifique el nombre del servidor DHCP que asignará las direcciones.

## IP no numerado

Haga clic en **IP no numerado** cuando desee que la interfaz comparta una dirección IP que ya se ha asignado a otra interfaz. Luego escoja la interfaz cuya dirección IP desea usar para la interfaz que está configurando.

## DNS dinámico

Escoja **DNS dinámico** si desea actualizar sus servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN. Haga clic en el botón **DNS dinámico** para configurar el DNS dinámico.

# Dirección IP: Ethernet sin PPPoE

Elija el método que utilizará la interfaz WAN para obtener una dirección IP.

## Dirección IP estática

Si selecciona **Dirección IP estática**, indique la dirección IP y la máscara de subred o los bits de la red en los campos proporcionados. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

## Dinámica (cliente DHCP)

Si selecciona esta opción, el router aceptará una dirección IP de un servidor DHCP remoto. Especifique el nombre del servidor DHCP que asignará las direcciones.

## DNS dinámico

Escoja DNS dinámico si desea actualizar sus servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN. Haga clic en el botón **DNS dinámico** para configurar el DNS dinámico.

# Dirección IP: serie con Protocolo punto a punto

Elija el método que utilizará la interfaz punto a punto para obtener una dirección IP.

## Dirección IP estática

Si selecciona **Dirección IP estática**, indique la dirección IP y la máscara de subred o los bits de la red en los campos proporcionados. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

## IP no numerado

Seleccione **IP no numerado** cuando desee que la interfaz comparta una dirección IP que ya se ha asignado a otra interfaz. Luego escoja la interfaz cuya dirección IP desea usar para la interfaz que está configurando.

## IP simple (IP negociado)

Seleccione **IP simple (IP negociado)** si el router obtendrá una dirección IP a través de la negociación de direcciones PPP/IPCP.

## DNS dinámico

Escoja DNS dinámico si desea actualizar sus servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN. Haga clic en el botón **DNS dinámico** para configurar el DNS dinámico.

# Dirección IP: serie con HDLC o Frame Relay

Elija el método que utilizará la interfaz WAN para obtener una dirección IP. Si se utiliza encapsulación Frame Relay, Cisco SDM crea una subinterfaz a la que Cisco SDM asigna la dirección IP.

## Dirección IP estática

Si selecciona **Dirección IP estática**, indique la dirección IP y la máscara de subred o los bits de la red en los campos proporcionados. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

## IP no numerado

Seleccione **IP no numerado** cuando desee que la interfaz comparta una dirección IP que ya se ha asignado a otra interfaz. Luego escoja la interfaz cuya dirección IP desea usar para la interfaz que está configurando.

## DNS dinámico

Escoja DNS dinámico si desea actualizar sus servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN. Haga clic en el botón **DNS dinámico** para configurar el DNS dinámico.

# Dirección IP: ISDN (RDSI) BRI o módem analógico

Elija el método que utilizará la interfaz ISDN (RDSI) BRI o módem analógico para obtener una dirección IP.

## Dirección IP estática

Si selecciona **Dirección IP estática**, indique la dirección IP y la máscara de subred o los bits de la red en los campos proporcionados. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

## IP no numerado

Seleccione **IP no numerado** cuando desee que la interfaz comparta una dirección IP que ya se ha asignado a otra interfaz. A continuación, seleccione la interfaz que tiene la dirección IP que desea que utilice la interfaz que está configurando.

## IP simple (IP negociado)

Seleccione **IP negociado** si la interfaz va a obtener una dirección IP del ISP a través de la negociación de direcciones PPP/PCP siempre que se establezca una conexión.

## DNS dinámico

Escoja DNS dinámico si desea actualizar sus servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN. Haga clic en el botón **DNS dinámico** para configurar el DNS dinámico.

# Autenticación

Esta página se muestra si usted está habilitado o está configurando lo siguiente:

- [PPP](#) para una conexión serie
- [PPPoE](#) o encapsulación PPPoA para una conexión ATM
- [PPPoE](#) o encapsulación PPPoA para una conexión Ethernet
- Una conexión RDSI Básico o de módem analógico

Es posible que el proveedor de servicios o administrador de redes utilice una contraseña Protocolo de autenticación por desafío mutuo ([CHAP](#)) o Protocolo de autenticación de contraseña ([PAP](#)) para garantizar la seguridad de la conexión entre dos dispositivos. Esta contraseña garantiza la seguridad para el acceso entrante y saliente.

## Tipo de autenticación

Marque la casilla para especificar el tipo de autenticación que utiliza el proveedor de servicios. Si desconoce el tipo que utiliza, puede marcar ambas casillas: el router intentará ambos tipos de autenticación (uno de ellos funcionará).

La autenticación CHAP es más segura que la autenticación PAP.

## Nombre de usuario

El nombre del usuario se le da a usted por su proveedor de servicios de Internet o su administrador de redes y se usa como el nombre del usuario para autenticación CHAP o PAP.

## Contraseña

Especifique la contraseña exactamente tal como se la ha proporcionado por el proveedor de servicios. Las contraseñas distinguen entre mayúsculas y minúsculas. Por ejemplo, la contraseña cisco no es igual a Cisco.

## Confirmar contraseña

Vuelva a especificar la misma contraseña que ha especificado en el cuadro anterior.

# Tipo de switch y SPID

Las conexiones de RDSI Básico requieren la identificación del tipo de switch de RDSI, y en algunos casos, la identificación de los canales B usan números de identificación del perfil del servicio (SPID, service profile ID). Esta información se la proporcionará el proveedor de servicios.

## Tipo de switch ISDN (RDSI)

Seleccione el tipo de switch ISDN (RDSI). Para obtener el tipo de switch de la conexión, póngase en contacto con el proveedor de servicios ISDN (RDSI).

Cisco SDM admite los tipos de switch BRI siguientes:

- Para América del Norte:
  - basic-5ess: switch 5ESS de velocidad básica de Lucent (AT&T)
  - basic-dms100: switch de velocidad básica DMS-100 de Northern Telecom
  - basic-ni: switches ISDN (RDSI) de National
- Para Australia, Europa y Reino Unido:
  - basic-1tr6: switch ISDN (RDSI) 1TR6 para Alemania
  - basic-net3: NET3 ISDN (RDSI) BRI para los tipos de switch de Noruega NET3, Australia NET3 y Nueva Zelanda NET3; tipos de switch conformes con ETSI para el sistema de señalización Euro-ISDN E-DSS1
  - vn3: switches ISDN (RDSI) BRI para Francia
- Para Japón:
  - ntt: switches ISDN (RDSI) NTT para Japón
- Para voz o sistemas de PBX:
  - basic-qsig: switches PINX (PBX) con señalización QSIG según Q.931

## Dispongo de algunos SPID

Marque esta casilla si su proveedor de servicios requiere SPID.

Algunos proveedores de servicios utilizan los SPID para definir los servicios a los que están abonados un dispositivo ISDN (RDSI) que accede al proveedor de servicios ISDN (RDSI). El proveedor de servicios asigna al dispositivo ISDN (RDSI) uno o varios SPID cuando el usuario se abona al servicio. Si utiliza un proveedor de servicios que requiere SPID, el dispositivo ISDN (RDSI) no podrá realizar ni recibir llamadas hasta enviar al proveedor de servicios un SPID válido y asignado en el momento en que el dispositivo accede al switch para inicializar la conexión.

Actualmente, sólo los tipos de switch DMS-100 y NI requieren SPID. El tipo de switch AT&T 5ESS puede admitir un SPID, pero se recomienda que establezca el servicio ISDN (RDSI) sin SPID. Además, los SPID sólo tienen significado en la interfaz ISDN (RDSI) de acceso local. Los routers remotos nunca reciben el SPID.

Normalmente, un SPID es un número de teléfono de 7 dígitos con algunos números opcionales. No obstante, es posible que los proveedores de servicios utilicen esquemas de numeración diferentes. Para el tipo de switch DMS-100, se asignan dos SPID; uno para cada canal B.

### SPID1

Especifique el SPID para el primer canal B BRI que le proporciona el ISP.

### SPID2

Especifique el SPID para el segundo canal B BRI que le proporciona el ISP.

## Cadena de marcación

Especifique el número de teléfono del extremo remoto de la conexión de ISDN (RDSI) BRI o de módem analógico. Este es el número de teléfono que marcará la interfaz de ISDN (RDSI) BRI o de módem analógico siempre que se establezca una conexión. La cadena de marcación se la proporciona el proveedor de servicios.



# Configuración de la conexión de reserva

Las interfaces ISDN (RDSI) BRI y de módem analógico pueden configurarse para que funcionen como interfaces de reserva para otras interfaces principales. En este caso, una conexión ISDN (RDSI) o de módem analógico sólo se establecerá si se produce un error en la interfaz principal. Si se produce un error en la interfaz principal y en la conexión, la interfaz ISDN (RDSI) o de módem analógico realizará inmediatamente una marcación externa e intentará establecer una conexión para evitar la pérdida de los servicios de red.

Seleccione si desea que esta conexión ISDN (RDSI) BRI o de módem analógico funcione como una conexión de respaldo.

Tenga en cuenta los requisitos siguientes:

- La interfaz primaria debe configurarse para la VPN de sitio a sitio.
- La imagen de Cisco IOS en su router debe soportar la función de Mejora del Eco de SAA ICMP.

## Configuración de la conexión de reserva: Direcciones IP de la interfaz principal y del próximo salto (next hop)

Para que la conexión de ISDN (RDSI) BRI o módem analógico funcione como conexión de respaldo, se debe asociar con otra interfaz en el router, que funcionará de conexión principal. La conexión ISDN (RDSI) BRI o de módem analógico sólo se establecerá si se produce un error en la conexión de la interfaz principal.

### Interfaz principal

Seleccione la interfaz del router que mantendrá la conexión principal.

### Dirección IP de próximo salto (next hop) principal

Este campo es opcional. Especifique la dirección IP a la que se conectará la interfaz principal cuando esté activa, conocida como la *dirección IP de próximo salto (next hop)*.

### Dirección IP de próximo salto (next hop) de reserva

Este campo es opcional. Especifique la dirección IP a la que se conectará la interfaz de respaldo cuando esté activa, conocida como la *dirección IP de próximo salto*.

## Configuración de la conexión de reserva: Nombre de host o dirección IP objeto del seguimiento

Esta pantalla permite identificar un host específico con el que debe mantenerse la conectividad. El router realizará un seguimiento de la conectividad con dicho host y, si el router detecta que la interfaz principal ha perdido conectividad con el host especificado, se iniciará la conexión de reserva a través de la interfaz ISDN (RDSI) BRI o de módem analógico.

### Dirección IP objeto del seguimiento

Especifique el nombre de host o la dirección IP del host de destino para el que se realizará un seguimiento de la conectividad. Especifique un destino con el que no se contacte con frecuencia como sitio para realizar el seguimiento.

## Opciones avanzadas

Existen dos opciones avanzadas disponibles en función de la configuración del router: Ruta estática por defecto y traducción de direcciones de puerto (PAT). Si la opción Ruta estática no aparece en la ventana, significa que ya se ha configurado alguna ruta estática en el router. Si la opción PAT no aparece en la ventana, significa que ya se ha configurado PAT en una interfaz.

### Ruta estática por defecto

Marque esta casilla si desea configurar una ruta estática a la interfaz externa a la que se enrutará el tráfico saliente. Si una ruta estática ya ha sido configurada en este router, esta casilla no aparecerá.

### Dirección de próximo salto

Si el proveedor de servicios le ha proporcionado una dirección IP de próximo salto para usar, especifíquela en este campo. Si deja el campo en blanco, Cisco SDM utilizará la interfaz WAN que está configurando como interfaz de próximo salto.

### Traducción de direcciones de puerto

Si los dispositivos de la LAN disponen de direcciones privadas, puede permitir que compartan una misma dirección IP pública. Puede asegurar que el tráfico llega a su destino correspondiente mediante el uso de PAT, que representa a los hosts en una LAN con una sola dirección IP y utiliza distintos números de puerto para distinguir entre los hosts. Si ya se ha configurado PAT en una interfaz, la opción PAT no aparecerá.

### Interfaz interna que se traducirá

Elija la interfaz interna conectada a la red cuyas direcciones IP de host desea que se traduzcan.

## Encapsulación

En esta ventana, seleccione el tipo de encapsulación que utilizará el enlace WAN. Pregunte al administrador de redes o al proveedor de servicios qué tipo de encapsulación se utiliza para este enlace. El tipo de interfaz determina los tipos de encapsulación disponibles.

### Detección automática

Haga clic en **Detección automática** para que Cisco SDM detecte el tipo de encapsulación. Si Cisco SDM lo consigue, suministrará de forma automática el tipo de encapsulación y los demás parámetros de configuración que detecte.



#### Nota

---

Cisco SDM admite la detección automática en los routers SB106, SB107, Cisco 836 y Cisco 837. Sin embargo, si usted está configurando un router Cisco 837 y el router está ejecutando la Versión 12.3(8)T o 12.3(8.3)T de Cisco, no se soporta la función de detección automática.

---

## Encapsulaciones disponibles

Las encapsulaciones disponibles si dispone de una interfaz ADSL, G.SHDSL o ADSL sobre ISDN (RDSI) aparecen en la tabla siguiente.

Encapsulación	Descripción
PPPoE	<p>Proporciona el protocolo punto a punto sobre la encapsulación de Ethernet. Esta opción está disponible si selecciona una interfaz Ethernet o una interfaz ATM. Si configura PPPoE sobre una interfaz ATM, se crearán una subinterfaz ATM y una interfaz de marcación.</p> <p>El botón de opción PPPoE estará desactivado si el router ejecuta una versión de Cisco IOS que no admite la encapsulación de PPPoE.</p>
PPPoA	<p>Protocolo punto a punto en ATM. Esta opción está disponible si selecciona una interfaz ATM. Si configura PPPoA sobre una interfaz ATM, se crearán una subinterfaz ATM y una interfaz de marcación.</p> <p>El botón de opción PPPoA estará desactivado si el router ejecuta una versión de Cisco IOS que no admite la encapsulación de PPPoA.</p>
enrutamiento RFC 1483 con AAL5-MUX	<p>Esta opción está disponible si selecciona una interfaz ATM. Si configura una conexión RFC1483, se creará una subinterfaz ATM. Esta subinterfaz estará visible en la ventana Resumen.</p>
Enrutamiento RFC1483 con AAL5-SNAP	<p>Esta opción está disponible si selecciona una interfaz ATM. Si configura una conexión RFC1483, se creará una subinterfaz ATM. Esta subinterfaz estará visible en la ventana Resumen.</p>

Las encapsulaciones disponibles si dispone de una interfaz de serie aparecen en la tabla siguiente.

Encapsulación	Descripción
<p><b>Frame Relay</b></p>	<p>Proporciona encapsulación Frame Relay. Esta opción está disponible si selecciona una interfaz de serie. Si crea una conexión Frame Relay se creará una subinterfaz de serie. Esta subinterfaz estará visible en la ventana Resumen.</p> <p><b>Nota</b> Si se ha agregado una conexión serie Frame Relay a una interfaz, la encapsulación Frame Relay sólo se activará en esta ventana cuando se configuren las conexiones serie posteriores en la misma interfaz.</p>
<p><b>Protocolo punto a punto</b></p>	<p>Proporciona encapsulación PPP. Esta opción está disponible si selecciona una interfaz de serie.</p>
<p><b>Control del enlace de datos de alto nivel</b></p>	<p>Proporciona encapsulación HDLC. Esta opción está disponible si selecciona una interfaz de serie.</p>

## PVC

El enrutamiento ATM utiliza un esquema jerárquico de dos niveles, rutas virtuales y canales virtuales, indicados por el identificador de ruta virtual (VPI) y el identificador de canal virtual (VCI), respectivamente. Es posible que una ruta virtual concreta transporte una variedad de distintos canales virtuales correspondientes a conexiones individuales. Cuando se realiza una conmutación basada en el VPI, todas las celdas de dicha ruta virtual concreta se conmutan independientemente del VCI. Un switch ATM puede enrutar de acuerdo con VCI, VPI o ambos VCI y VPI.

**VPI**

Especifique el valor del VPI que obtiene del proveedor de servicios o del administrador del sistema. El identificador de ruta virtual (VPI) se utiliza en la conmutación y el enrutamiento ATM para identificar la ruta que se utiliza para una variedad de conexiones. Especifique el valor VPI que le ha proporcionado el proveedor de servicios.

**VCI**

Especifique el valor del VCI que obtiene del proveedor de servicios o del administrador del sistema. El identificador de circuito virtual (VCI) se utiliza en la conmutación y el enrutamiento ATM para identificar una conexión específica dentro de una ruta que posiblemente comparte con otras conexiones. Especifique el valor VCI que le ha proporcionado el proveedor de servicios.

**Valores por defecto de Cisco IOS**

Los valores que figuran en la tabla siguiente son los valores por defecto de Cisco IOS. Cisco SDM no sobrescribirá estos valores si se han cambiado durante una configuración anterior, pero si el router no se ha configurado anteriormente, los valores que se utilizarán son los siguientes:

<b>Tipo de conexión</b>	<b>Parámetro</b>	<b>Valor</b>
ADSL	<ul style="list-style-type: none"> <li>• Modo operativo</li> </ul>	<ul style="list-style-type: none"> <li>• Auto</li> </ul>
G.SHDSL	<ul style="list-style-type: none"> <li>• Modo operativo</li> <li>• Tasa de línea</li> <li>• Tipo de equipo</li> </ul>	<ul style="list-style-type: none"> <li>• Anexo A (señalización EUA)</li> <li>• Auto</li> <li>• CPE</li> </ul>
ADSL sobre ISDN (RDSI)	<ul style="list-style-type: none"> <li>• Modo operativo</li> </ul>	<ul style="list-style-type: none"> <li>• Auto</li> </ul>

# Configuración de LMI y DLCI

Si está configurando una conexión con encapsulación Frame Relay, debe especificar el protocolo utilizado para supervisar la conexión, denominado Identificador de gestión local (LMI), y proporcionar un identificador exclusivo para esta conexión concreta, denominado Identificador de conexión de enlace de datos (DLCI).

## Tipo de LMI

Consulte con el proveedor de servicios para saber cuáles de los siguientes tipos de LMI debe utilizar.

Tipo de LMI	Descripción
ANSI	Anexo D definido por la norma T1.617 del American National Standards Institute (ANSI).
Cisco	Tipo de LMI definido conjuntamente por Cisco Systems y tres otras empresas.
ITU-T Q.933	ITU-T Q.933 Anexo A.
Detección automática	El valor por defecto. Este parámetro permite al router detectar el tipo de LMI que se está utilizando al comunicarse con el switch y, a continuación, utilizar dicho tipo. Si falla la <b>detección automática</b> , el router utilizará el tipo de LMI de Cisco.

## DLCI

Especifique el DLCI en este campo. Este número debe ser exclusivo entre todos los DLCI que se utilizan en esta interfaz.

## Utilice la encapsulación Frame Relay IETF

Encapsulación Internet Engineering Task Force (IETF). Esta opción se utiliza al establecer conexión con routers que no son de Cisco. Marque esta casilla si se está tratando de conectar a un router que no sea de Cisco en esta interfaz.

# Configuración del reloj

La ventana Configuración del reloj está disponible cuando usted está configurando un enlace T1 o E1. Los ajustes por defecto de reloj Frame Relay aparecen en esta página. No los cambie a menos que sus requisitos sean otros.

## Origen del reloj

Interno especifica que el reloj se genera de forma interna. Línea especifica que el origen del reloj se obtiene de la red. El reloj sincroniza la transmisión de datos. El valor por defecto es **línea**.

## Entramado T1/E1

Este campo configura el enlace **T1** o E1 para la operación con D4 Super Frame (SF) o Extended Superframe (ESF). El valor por defecto es **esf**.

## Código de línea

Este campo configura el router para la operación en la sustitución binaria de 8 ceros (B8ZS b8-zeros substitution) o líneas **T1** de inversión de marca alterna (AMI). La configuración de la b8zs asegura la densidad en una línea T1 o E1 al sustituir las violaciones bipolares intencionales en las posiciones 4 y 7 del bit para una secuencia de bits de ocho ceros. Cuando el router se configura con la configuración de AMI, deberá utilizar la configuración invertida de codificación de datos para garantizar la densidad de la línea T1. El valor por defecto es **b8zs**.

## Codificación de los datos

Haga clic en **invertido** si usted sabe que los datos del usuario están invertidos en este enlace, o si el campo Código de línea se fija en AMI. De lo contrario, deje este ajuste con su valor por defecto, que es **normal**. La inversión de datos se utiliza con protocolos orientados a bits como **HDLC**, **PPP** y Proceso de acceso a enlaces, con balance (**LAPB**) para garantizar la densidad en una línea **T1** con codificación **AMI**. Estos protocolos orientados a bits realizan “inserciones de cero” después de cada cinco bits “uno” en el flujo de datos. Esto tiene el efecto de asegurar al menos un cero en cada ocho bits. Si se invierte el flujo de datos, se garantiza que al menos uno de cada ocho bits es un uno.



Cisco SDM fijará la codificación de datos a invertido si el código de línea es AMI y si no hay intervalos de tiempo configurados para 56 kbps. Si usted no quiere usar una codificación de datos invertida con el código de línea AMI, deberá usar el CLI para configurar todos los intervalos de tiempo a 56 kbps.

### Enlace de datos en instalaciones (FDL)

Este campo configura el comportamiento del router en el enlace de datos en instalaciones (FDL) del Superframe ampliado. Si se configura con **att**, el router implementa AT&T TR 54016. Si se configura con **ansi**, implementa ANSI T1.403. Si elige Ambos, el router implementa las dos opciones, **att** y **ansi**. Si elige Ninguno, el router no toma en cuenta el FDL. El valor por defecto es **ninguno**. **Si el entramado T1 o E1 se fija en sf**, Cisco SDM definirá el FDL en **ninguno** y convertirá este campo en un campo de sólo lectura.

### LBO (Line Build Out)

Este campo se utiliza para configurar el **LBO** (Line Build Out) del enlace **T1**. El LBO disminuye la potencia de transmisión de la señal en -7,5 ó -15 decibelios. No es probable que se requiera en las líneas T1/E1 actuales. El valor por defecto es **ninguno**.

### Solicitud de retrobucle remoto

Este campo especifica si el router entra en el retrobucle si en la línea se recibe un código de retrobucle. Si selecciona **completo**, el router aceptará los retrobucles completos y si se selecciona la **carga útil v54**, el router seleccionará los retrobucles de carga útil.

### Activar la generación/detección de alarmas remotas

Marque esta casilla si desea que el enlace **T1** del router genere alarmas remotas (alarmas amarillas) y detecte alarmas remotas que se envían desde el par del otro extremo del enlace.

Un router transmite la alarma remota cuando detecta una condición de alarma: puede ser una alarma roja (pérdida de señal) o una alarma azul (1s no tramados). De este modo, la unidad de servicios de canal o de datos (CSU/DSU) que la recibe está informada sobre la condición de error presente en la línea.

Este ajuste sólo se debe utilizar cuando el entramado T1/E1 está definido en **esf**.

# Eliminar conexión

Puede eliminar una conexión WAN que aparece en la ventana Editar interfaz/conexión. Esta ventana aparece cuando se está eliminando una configuración de interfaz y cuando la conexión que desea eliminar contiene asociaciones como reglas de acceso que se han aplicado a esta interfaz. Desde esta ventana puede guardar las asociaciones para utilizarlas con otra conexión.

Al eliminar una conexión, la lista Crear nueva conexión se actualiza si dicha eliminación deja disponible un tipo de conexión que hasta entonces no lo estaba.

Puede eliminar automáticamente todas las asociaciones de la conexión o eliminar las asociaciones posteriormente.

## Para ver las asociaciones de la conexión:

Haga clic en **Ver detalles**.

## Para eliminar la conexión y todas sus asociaciones:

Haga clic en **Eliminar automáticamente todas las asociaciones** y, a continuación, en **Aceptar** para que Cisco SDM elimine la conexión y todas sus asociaciones.

## Para eliminar manualmente las asociaciones:

Para eliminar las asociaciones de forma manual, haga clic en **Ver detalles** con el fin de obtener una lista de las asociaciones de esta conexión. Anote las asociaciones, seleccione **Eliminaré las asociaciones más tarde** y, a continuación, haga clic en **Aceptar**. Puede eliminar manualmente las asociaciones de la conexión siguiendo las instrucciones de la lista siguiente.

Las asociaciones posibles y las instrucciones para eliminarlas son:

- Ruta estática por defecto: la interfaz se configura como la interfaz de envío para una ruta estática por defecto. Para eliminar la ruta estática con la que está asociada esta interfaz, haga clic en **Configurar** y, a continuación, en **Enrutamiento**. Haga clic en la ruta estática de la tabla Enrutamiento estático y, a continuación, en **Eliminar**.

- Traducción de direcciones de puerto: la PAT se configura mediante la interfaz en la que se ha creado esta conexión. Para eliminar la asociación PAT, haga clic en **Configurar** y, a continuación, en **NAT**. Seleccione la regla asociada con esta conexión y haga clic en **Eliminar**.
- NAT: la interfaz se ha designado como interfaz interna NAT o externa NAT. Para eliminar la asociación NAT, haga clic en **Configurar** y, a continuación, en **Interfaces y conexiones**. Haga clic en la conexión en la lista de interfaces y, luego, en **Editar**. Haga clic en la ficha **NAT**, luego elija **Ninguno** del menú desplegable NAT.
- ACL: se aplica una ACL a la interfaz en la que se ha creado la conexión. Para eliminar la lista de control de acceso, haga clic en **Configurar** y, a continuación, en **Interfaces y conexiones**. Seleccione la conexión de la lista de interfaces y, a continuación, haga clic en **Editar**. Haga clic en la **ficha Asociación**. Luego, en el grupo Regla de acceso, haga clic en el botón ... que aparece junto a los campos Entrante y Saliente y, a continuación, en **Ninguno**.
- Inspección: se aplica una regla de inspección a la interfaz en la que se ha creado la conexión. Para eliminar la regla de inspección, haga clic en **Configurar** y, a continuación, en **Interfaces y conexiones**. Seleccione la conexión de la lista de interfaces y, a continuación, haga clic en **Editar**. Haga clic en la **ficha Asociación**; a continuación, en el grupo Regla de inspección, en los campos Entrante y Saliente, seleccione **Ninguno**.
- Criptografía: se aplica un mapa criptográfico a la interfaz en la que se ha creado la conexión. Para eliminar el mapa criptográfico, haga clic en **Configurar** y, a continuación, en **Interfaces y conexiones**. Haga clic en la conexión en la lista de interfaces y, luego, en **Editar**. Haga clic en la **ficha Asociación**; luego en el grupo VPN, en el campo Política IPsec, haga clic en **Ninguno**.
- EzVPN: se aplica una Easy VPN a la interfaz en la que se ha creado la conexión. Para eliminar la Easy VPN, haga clic en **Configurar** y, a continuación, en **Interfaces y conexiones**. Haga clic en la conexión en la lista de interfaces y, luego, en **Editar**. Haga clic en la **ficha Asociación**; a continuación, en el grupo VPN, en el campo Easy VPN, haga clic en **Ninguno**.
- VPDN: los comandos VPDN requeridos para una configuración PPPoE están presentes en la configuración del router. Si hay otras conexiones PPPoE configuradas en el router, no elimine los comandos VPDN.
- ip tcp adjust mss: este comando se aplica a una interfaz LAN para ajustar el tamaño máximo de TCP. Si hay otras conexiones PPPoE configuradas en el router, no elimine este comando.

- Conexión de respaldo: cuando existe una conexión de respaldo configurada para la interfaz principal. Para eliminar la asociación de conexión de respaldo, haga clic en **Configurar** y, a continuación, en **Interfaces y conexiones**. Seleccione la interfaz de reserva de la lista de interfaces y, a continuación, haga clic en **Editar**. Haga clic en la ficha **De reserva** y desmarque la casilla de verificación **Activar conexión de respaldo**.
- PAT en la conexión de respaldo: la PAT está configurada en la interfaz de respaldo. Para eliminar la asociación PAT, haga clic en **Configurar** y, a continuación, en **NAT**. Seleccione la regla asociada con esta conexión y haga clic en **Eliminar**.
- Ruta por defecto flotante en la conexión de respaldo: la interfaz de respaldo se configura con una ruta estática por defecto flotante. Para eliminar la ruta estática flotante, haga clic en **Configurar** y, a continuación, en **Enrutamiento**. Seleccione la ruta estática flotante de la tabla Enrutamiento estático y, a continuación, haga clic en **Eliminar**.

## Resumen

En esta pantalla aparece un resumen del enlace WAN que ha configurado. Para revisar esta información y realizar los cambios necesarios, puede hacer clic en el botón Atrás y volver a la pantalla en la que desea efectuar modificaciones.

### Una vez realizada la configuración, pruebe la conectividad

Marque esta casilla de verificación si desea que Cisco SDM realice una prueba de la conexión que ha configurado después de que se descarguen los comandos al router. Cisco SDM realizará una prueba de la conexión y mostrará un informe de los resultados en otra ventana.

### Para guardar esta configuración en la configuración en ejecución del router y salir de este asistente:

Haga clic en **Finalizar**. Cisco SDM guarda los cambios de configuración en la configuración en ejecución del router. Aunque los cambios se aplican inmediatamente, los mismos se perderán si se apaga el router.

Si ha activado la opción **Obtener una vista previa de los comandos antes de enviarlos al router** de la ventana Preferencias de Cisco SDM, aparecerá la ventana Enviar. Esta ventana permite ver los comandos CLI que se envían al router.

# Pruebas y resolución de problemas de la conectividad

Esta ventana permite probar una conexión configurada al efectuar un ping a un host remoto. Si el ping falla, Cisco SDM informa de la causa probable del fallo y recomienda acciones para corregir el problema.

## ¿Qué tipos de conexión se pueden probar?

Cisco SDM permite resolver problemas de las conexiones ADSL, G.SHDSL V1 y G.SHDSL V2 mediante encapsulación PPPoE, AAL5SNAP o AAL5MUX.

Cisco SDM permite resolver los problemas de las conexiones Ethernet con encapsulación PPPoE.

Cisco SDM no puede resolver los problemas de las conexiones de Ethernet no encapsuladas, de serie o conexiones T1 o E1, conexiones analógicas, y conexiones de RDSI. Cisco SDM proporciona una prueba de ping básica para estos tipos de conexión

## ¿Qué es la prueba de ping básica?

Cuando Cisco SDM realiza una prueba de ping básica, lleva a cabo lo siguiente:

1. Verifica el estado de la interfaz para comprobar si está en servicio o fuera de servicio.
2. Verifica la configuración de DNS, independientemente de si se trata de las opciones por defecto de Cisco SDM o de nombres de host especificados por el usuario.
3. Verifica las configuraciones de DHCP e IPCP en la interfaz.
4. Termina la comprobación de la interfaz.
5. Efectúa un ping al destino.

Cisco SDM presenta un informe con los resultados de estas comprobaciones en las columnas Actividad y Estado. Si el ping se finaliza correctamente, la conexión resultará satisfactoria. De lo contrario, si la conexión resulta estar fuera de servicio, se informa de la prueba que ha fallado.

## ¿Cómo realiza Cisco SDM la resolución de problemas?

Cuando Cisco SDM resuelve un problema con una conexión, realiza una verificación más amplia que la prueba de ping básica. Si el router no supera alguna prueba, Cisco SDM realiza verificaciones adicionales para poder informarle de los motivos posibles del fallo. Por ejemplo, si la Capa 2 está fuera de servicio, Cisco SDM intenta determinar los motivos de este estado, informar de ellos y recomendar acciones para resolver el problema. Cisco SDM realiza las tareas siguientes.

1. Verifica el estado de la interfaz. Si el protocolo de la Capa 2 está en servicio, Cisco SDM va al paso 2.

Si el protocolo de la Capa 2 está fuera de servicio, Cisco SDM verifica el estado de ATM PVC para las conexiones XDSL o el estado de PPPoE para las conexiones Ethernet encapsuladas.

- Si se producen fallos en la prueba ATM PVC, Cisco SDM muestra los motivos posibles del fallo además de acciones que se pueden llevar a cabo para corregir el problema.
- Si la conexión PPPoE está fuera de servicio, existe un problema con el cableado y Cisco SDM muestra los motivos y acciones pertinentes.

Una vez realizadas estas verificaciones, finaliza la prueba y Cisco SDM presenta un informe con los resultados y las acciones recomendadas.

2. Verifica la configuración de DNS, independientemente de si se trata de las opciones por defecto de Cisco SDM o de nombres de host especificados por el usuario.

3. Verifica la configuración de DHCP o IPCP y su estado. Si el router dispone de una dirección IP a través de DHCP o de IPCP, Cisco SDM salta al paso 4.

Si el router está configurado para DHCP o IPCP, pero no ha recibido ninguna dirección IP a través de estos métodos, Cisco SDM realiza las verificaciones del paso 1. La prueba finaliza y Cisco SDM presenta un informe con los resultados y las acciones recomendadas.

4. Efectúa un ping al destino. Si la aplicación de ping es correcta, Cisco SDM presenta un informe positivo.

Si el ping produce fallos en una conexión xDSL con encapsulación PPPoE, Cisco SDM verifica los elementos siguientes:

- El estado de ATM PVC
- El estado del túnel PPPoE
- El estado de la autenticación PPP

Una vez realizadas estas verificaciones, Cisco SDM presenta un informe con los motivos de fallo del ping.

Si el ping produce fallos en una red Ethernet con encapsulación PPPoE, Cisco SDM verifica los elementos siguientes:

- El estado del túnel PPPoE
- El estado de la autenticación PPP

Una vez realizadas estas verificaciones, Cisco SDM presenta un informe con los motivos de fallo del ping.

Si el ping falla en una conexión xDSL con encapsulación AAL5SNAP o AAL5MUX, Cisco SDM verifica el estado de ATM PVC y presenta un informe con los motivos de fallo del ping.

## Dirección IP/Nombre de host

Especifique el nombre de servidor al que desea realizar un ping para probar la interfaz WAN.

### **Determinado automáticamente por SDM**

Cisco SDM realiza un ping a su host por defecto para probar la interfaz WAN. Cisco SDM detecta los servidores DNS configurados de forma estática, además de los servidores DNS importados de forma dinámica. Cisco SDM realiza un ping a estos servidores y, si los pings realizados con éxito salen por la interfaz que está de prueba, Cisco SDM informa del éxito de la operación. Si todos los pings presentan fallos, o si no se encuentran pings correctos que salgan por la interfaz que está de prueba, Cisco SDM informa del fallo.

### **Especificado por el usuario**

Especifique la dirección IP del nombre de host deseado para probar la interfaz WAN.

## Resumen

Haga clic en este botón para ver la información resumida de la resolución de problemas.

## Detalles





Haga clic en este botón para ver la información detallada de la resolución de problemas.

## Actividad

En esta columna se muestran las actividades de resolución de problemas.

## Estado

Muestra el estado de cada actividad de resolución de problemas mediante los iconos y textos de alerta siguientes:

-  La conexión está activa.
-  La conexión está inactiva.
-  La prueba se ha superado.
-  La prueba ha fallado.

## Motivo

En este cuadro se proporcionan los posibles motivos del fallo de la conexión de la interfaz WAN.

## Acciones recomendadas

En este cuadro se proporciona una posible acción/solución para corregir el problema.



## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Resolver los problemas de la conexión de la interfaz WAN.	Haga clic en el botón <b>Iniciar</b> . Cuando se esté ejecutando la prueba, la etiqueta del botón <b>Iniciar</b> cambiará a <b>Detener</b> . Tiene la opción de cancelar la resolución de problemas mientras la prueba esté ejecutándose.
Guardar el informe de la prueba.	Haga clic en <b>Guardar informe</b> para guardar el informe de la prueba en formato HTML. Este botón sólo estará activo cuando se esté ejecutando una prueba o cuando ésta haya finalizado.

## Cómo...

En esta sección se incluyen procedimientos para las tareas que el asistente no le ayuda a llevar a cabo.

## ¿Cómo se visualizan los comandos de IOS que se envían al router?

Consulte [¿Cómo se visualizan los comandos de IOS que se envían al router?](#)

## ¿Cómo se configura una interfaz WAN no admitida?

Cisco SDM no admite la configuración de todas las interfaces **WAN** que puede admitir el router. Si Cisco SDM detecta una interfaz no admitida en el router o una interfaz admitida con una configuración no admitida, Cisco SDM mostrará un botón de opción con la etiqueta Otros (no admitido por Cisco SDM). La interfaz no admitida aparece en la ventana Interfaces y conexiones, pero no se puede configurar mediante Cisco SDM.

Para configurar una interfaz no admitida, debe utilizar la interfaz de línea de comandos (**CLI**) del router.

## ¿Cómo se activa o desactiva una interfaz?

Una interfaz puede desactivarse sin quitar su configuración. También es posible reactivar una interfaz desactivada.

- 
- Paso 1** Haga clic en **Configurar** en la barra de herramientas de Cisco SDM.
  - Paso 2** En el panel izquierdo, haga clic en **Interfaces y conexiones**.
  - Paso 3** Haga clic en la interfaz que desee desactivar o activar.
  - Paso 4** Si la interfaz está activada, aparecerá el botón Desactivar debajo de la lista de interfaces. Haga clic en dicho botón para desactivar la interfaz. Si la interfaz está desactivada, aparecerá el botón Activar en su lugar. Haga clic en dicho botón para activar la interfaz.
- 

## ¿Como se visualiza la actividad en la interfaz WAN?

La actividad de una interfaz **WAN** puede visualizarse mediante la función de supervisión en Cisco SDM. Las pantallas de supervisión pueden mostrar estadísticas sobre la interfaz WAN, incluido el número de paquetes y bytes que la interfaz ha enviado o recibido y el número de errores de envío o recepción que se han producido. Para ver las estadísticas sobre una interfaz WAN:

- 
- Paso 1** En la barra de herramientas, haga clic en **Supervisar**.
  - Paso 2** En el panel izquierdo, haga clic en **Estado de la interfaz**.
  - Paso 3** En el campo Seleccione una interfaz, seleccione la interfaz WAN cuyas estadísticas desee visualizar.
  - Paso 4** Para seleccionar el o los elementos de datos que desee visualizar, marque las casillas de verificación correspondientes. Puede ver un máximo de cuatro estadísticas a la vez.
  - Paso 5** Para ver las estadísticas de todos los elementos de datos seleccionados, haga clic en **Ver detalles**.

Aparecerá la ventana Detalles de la interfaz que muestra todas las estadísticas seleccionadas. Por defecto, la ventana muestra los datos en tiempo real, de modo que sondea el router cada 10 segundos. Si la interfaz está activa y se transmiten datos sobre ella, deberá observar un aumento en el número de paquetes y bytes que se transfieren a través de la misma.

---

## ¿Cómo se configura NAT en una interfaz WAN?

- 
- Paso 1** Haga clic en **Configurar** en la barra de herramientas de Cisco SDM.
- Paso 2** Haga clic en **NAT** en el panel izquierdo.
- Paso 3** En la ventana NAT, haga clic en **Designar interfaces NAT**.
- Paso 4** Busque la interfaz para la que desea configurar NAT.
- Paso 5** Seleccione la opción **interna (fiable)** junto a la interfaz para designar la interfaz como interna, o fiable. Una designación interna se utiliza generalmente para designar una interfaz que presta servicio a una LAN cuyos recursos se deben proteger. Seleccione la opción **externa (no fiable)** para designarla como una interfaz externa. Generalmente, las interfaces externas se conectan a una red no fiable. Haga clic en **Aceptar**.
- La interfaz se agrega al grupo de interfaces mediante NAT.
- Paso 6** Revise las Reglas de traducción de direcciones de la red en la ventana NAT. Si necesita agregar, eliminar o modificar una regla, haga clic en el botón pertinente de la ventana NAT para realizar la configuración requerida.
- 

Para obtener más información, haga clic en los enlaces siguientes:

- [Agregar o editar regla de traducción de direcciones estáticas: De interna a externa](#)
- [Agregar o editar regla de traducción de direcciones estáticas: De externa a interna](#)
- [Agregar o editar regla de traducción de direcciones dinámicas: De interna a externa](#)
- [Agregar o editar regla de traducción de direcciones dinámicas: De externa a interna](#)

## ¿Cómo se configura NAT en una interfaz no admitida?

Cisco SDM puede configurar la traducción de direcciones de red (NAT) en un tipo de interfaz no compatible con Cisco SDM. Para poder configurar el firewall, primero es preciso utilizar la CLI del router para configurar la interfaz. La interfaz deberá tener, como mínimo, una dirección IP configurada y deberá estar en funcionamiento. Para verificar que la conexión funcione, verifique que el estado de la interfaz sea activo.

Después de configurar la interfaz no admitida mediante el CLI, puede configurar NAT mediante Cisco SDM. La interfaz no admitida aparecerá como “Otro” en la lista de interfaces del router.

## ¿Cómo se configura un protocolo de enrutamiento dinámico?

Para configurar un protocolo de [enrutamiento dinámico](#):

- 
- Paso 1** En la barra de herramientas, haga clic en **Configurar**.
  - Paso 2** En el panel izquierdo, haga clic en **Enrutamiento**.
  - Paso 3** En el grupo Enrutamiento dinámico, haga clic en el protocolo de enrutamiento dinámico que desee configurar.
  - Paso 4** Haga clic en **Editar**.  
Aparece el cuadro de diálogo Enrutamiento dinámico, el cual muestra la ficha del protocolo de enrutamiento dinámico que ha seleccionado.
  - Paso 5** Utilice los campos del cuadro de diálogo Enrutamiento dinámico para configurar el protocolo de enrutamiento dinámico. Si necesita obtener una explicación de cualquiera de los demás cuadros de diálogo, haga clic en **Ayuda**.
  - Paso 6** Una vez finalizada la configuración del protocolo de enrutamiento dinámico, haga clic en **Aceptar**.
-

## ¿Cómo se configura el enrutamiento de marcación a petición para la interfaz asíncrona o ISDN?

Las conexiones ISDN (RDSI) BRI y asíncrona son conexiones de acceso telefónico, lo que significa que para establecer una conexión, el router debe marcar un número de teléfono configurado previamente. Puesto que el costo de estos tipos de conexiones normalmente se determina por la duración de la conexión, y en el caso de una conexión asíncrona, que la línea telefónica quedará ocupada, resulta recomendable configurar un enrutamiento de marcación a petición (DDR, Dial-on-Demand Routing) para este tipo de conexiones.

Cisco SDM puede ayudarle a configurar DDR de la forma siguiente:

- Permitiendo asociar una regla (o ACL) con la conexión, lo que provoca que el router establezca la conexión únicamente cuando detecta un tráfico de red que usted ha identificado como interesante con la regla asociada.
- Definiendo los límites de tiempo de inactividad, lo que provoca que el router finalice una conexión una vez transcurrido un tiempo especificado sin que haya actividad en la misma.
- Activando PPP multienlace, lo que provoca que una conexión ISDN (RDSI) BRI utilice únicamente uno de los dos canales B, a menos que se exceda el porcentaje de banda ancha especificado en el primer canal B. Este proceso presenta la ventaja de ahorrar costos cuando el tráfico de red es bajo y no se requiere el segundo canal B, aún permitiéndole utilizar la banda ancha de la conexión ISDN (RDSI) BRI en su totalidad siempre que sea necesario.

Para configurar DDR en una conexión ISDN (RDSI) BRI o asíncrona existente:

- 
- Paso 1** Haga clic en **Configurar** en la barra de herramientas de Cisco SDM.
  - Paso 2** En el panel izquierdo, haga clic en **Interfaces y conexiones**.
  - Paso 3** Haga clic en la interfaz ISDN (RDSI) o asíncrona en la que desee configurar DDR.
  - Paso 4** Haga clic en **Editar**.  
Aparecerá la ficha Conexión.
  - Paso 5** Haga clic en **Opciones**.  
Aparecerá el cuadro de diálogo Editar Opciones de marcación.

- Paso 6** Si desea que el router establezca la conexión sólo cuando detecte un tráfico IP concreto, haga clic en el botón de opción **Filtrar tráfico según una lista de control de acceso seleccionada** y especifique un número de regla (ACL) que identifique el tráfico IP que debería obligar al router a realizar la marcación del router o bien, haga clic en el botón ... para examinar la lista de reglas y seleccionar la regla que desee utilizar para identificar el tráfico IP.
- Paso 7** Si desea configurar el router para finalizar una conexión inactiva, es decir, cuando no pasa tráfico por ella, durante un tiempo especificado, en el campo **Límite de tiempo de inactividad**, especifique el número de segundos que la conexión podrá permanecer inactiva antes de que el router finalice la conexión.
- Paso 8** Si está editando una conexión ISDN (RDSI), y desea utilizar el segundo canal B sólo cuando el tráfico en el primero exceda un límite determinado, marque la casilla de verificación **Activar PPP multienlace**. A continuación, en el campo **Umbral de la carga**, especifique un número entre 1 y 255, donde 255 equivale al 100% de banda ancha, que determinará el límite en el primer canal B. Si el tráfico del canal supera este límite, el router se conectará al segundo canal B. Además, en el campo **Dirección de datos**, puede elegir si este límite se debe aplicar al tráfico saliente o al entrante.
- Paso 9** Haga clic en **Aceptar**.
- 

## ¿Cómo se edita una Configuración de interfaz de radio?

Debe utilizar Aplicación inalámbrica para editar una configuración de interfaz de radio existente.

- Paso 1** Haga clic en **Configurar** en la barra de herramientas de Cisco SDM.
- Paso 2** Haga clic en **Interfaces y conexiones** en el marco izquierdo, y luego haga clic en la ficha Editar interfaz/conexión.
- Paso 3** Seleccione la interfaz de radio y haga clic en **Editar**. En la ficha Conexiones, puede cambiar la dirección IP o la información de bridge. Si desea cambiar otros parámetros inalámbricos, haga clic en **Iniciar aplicación inalámbrica**.
-



## CAPÍTULO 5

# Editar interfaz/conexión

---

En esta ventana se muestran las interfaces y las conexiones del router, y se permite agregar, editar y eliminar conexiones, además de activarlas y desactivarlas.

### Agregar

Al seleccionar una interfaz física sin configurar y hacer clic en **Agregar**, el menú dispondrá de opciones para agregar una conexión en dicha interfaz. Haga clic en **Agregar** para crear una nueva interfaz de retrobucle o de túnel. Si la imagen de Cisco IOS en el router admite interfaces de plantilla virtual (**VTI**), el menú contextual incluye una opción para agregar una VTI. Si existen puertos de switch en el router, puede agregar una nueva VLAN.

Si desea volver a configurar una interfaz y sólo se muestran las opciones Retrobucle y Túnel al hacer clic en **Agregar**, seleccione la interfaz en cuestión y haga clic en **Eliminar**. En el menú Agregar, aparecerán todos los tipos de conexiones disponibles para dicho tipo de interfaz. Haga clic en **Configuraciones de interfaz disponibles** para ver las configuraciones disponibles para una determinada interfaz.

### Editar

Al seleccionar una interfaz y hacer clic en **Editar**, aparecerá un cuadro de diálogo. Si la interfaz es compatible, está configurada y no es un puerto de switch, el cuadro de diálogo presentará las siguientes fichas:

- Conexión
- Ficha Asociación
- Ficha NAT

- Servicio de aplicación
- Ficha General

Si la interfaz no es compatible, el cuadro de diálogo *no* presentará la ficha Conexión. Si selecciona un puerto de switch, aparecerá el cuadro de diálogo Editar puerto del switch. Si la interfaz es compatible pero no se ha configurado, el botón Editar estará desactivado.

## Eliminar

Al seleccionar una conexión y hacer clic en **Eliminar**, aparecerá un cuadro de diálogo que muestra las asociaciones de dicha conexión y que le solicita si desea quitar las asociaciones junto con la conexión. Puede eliminar solamente la conexión o la conexión y todas sus asociaciones.

## Resumen

Al hacer clic en el botón Resumen, se ocultan los detalles sobre la conexión, lo que restringe la información para la dirección IP, tipo, ranura, estado y descripción.

## Detalles

Al hacer clic en **Detalles**, aparecerá el área Detalles de la interfaz que se describe a continuación. Dichos detalles se muestran por defecto.

## Activar o desactivar

Cuando la interfaz o la conexión elegida está caída, esto aparecerá como el botón **Activar**. Haga clic en el botón **Activar** para levantar la interfaz o conexión elegida. Cuando la interfaz o conexión elegida está levantada, esto aparecerá como el botón **Desactivar**. Haga clic en el botón **Desactivar** para desactivar administrativamente la interfaz o conexión. Este botón no puede usarse con una interfaz cuya configuración no ha sido enviada al router.

## Probar conexión

Haga clic en este botón para probar la conexión seleccionada. Aparecerá un cuadro de diálogo que permite especificar un host remoto al que se podrá hacer ping a través de esta conexión. A continuación, el cuadro de diálogo muestra un informe indicando si la prueba se ha realizado correctamente o no. Si la prueba no se realiza correctamente, se proporcionará información sobre los posibles motivos, además de los pasos que se deberán llevar a cabo para corregir el problema.



## Lista de interfaces

La lista de interfaces muestra las interfaces físicas y las conexiones lógicas para las que están configuradas.

### Interfaces

En esta columna aparece una lista de las interfaces físicas y lógicas ordenadas por nombre. Si una **interfaz lógica** está configurada para una **interfaz física**, la interfaz lógica aparece bajo la interfaz física.

Si ejecuta Cisco SDM en un router de la familia 7000 de Cisco, podrá crear una conexión solamente en las interfaces Ethernet y Fast Ethernet.

### Dirección IP

Esta columna puede contener los siguientes tipos de direcciones IP:

- La dirección IP configurada de la interfaz.
- Cliente DHCP: la interfaz recibe una dirección IP de un servidor DHCP (Dynamic Host Configuration Protocol).
- IP negociado: la interfaz recibe una dirección IP a través de una negociación con el dispositivo remoto.
- IP no numerado: el router utilizará un conjunto de direcciones IP suministrado por el proveedor de servicios del router y los dispositivos de la LAN.
- No aplicable: no se puede asignar ninguna dirección IP al tipo de interfaz.

### Tipo

La columna Tipo muestra el tipo de interfaz como, por ejemplo, Ethernet, en serie o ATM.

### Ranura

El número de la ranura física del router en la que está instalada la interfaz. Si ejecuta Cisco SDM en un router Cisco 1710, el campo de ranura está vacío.

### Estado

Esta columna muestra si la interfaz está activada o desactivada. Un icono verde con la punta de flecha orientada hacia arriba indica que la interfaz está activada. Por el contrario, si el icono es rojo y presenta una punta de flecha orientada hacia abajo, la interfaz está desactivada.

### Descripción

Esta columna contiene las descripciones que se proporcionan para esta conexión.

## Detalles de la interfaz

En esta área de la ventana se muestra la información de asociación y de conexión (si procede) de la interfaz seleccionada en la lista de interfaces. Entre los detalles de asociación se incluye información como, por ejemplo, las reglas de traducción de direcciones de red (NAT), de acceso y de inspección, las políticas IPsec y las configuraciones de Easy VPN. Entre los detalles de conexión se incluyen la dirección IP, el tipo de encapsulación y las opciones DHCP.

### Nombre de elemento

El nombre del elemento de configuración como, por ejemplo, la dirección IP, máscara de subred o la política IPsec. Los elementos que se incluyen en esta columna dependen del tipo de interfaz seleccionada.

### Valor de elemento

Si un elemento con nombre dispone de un valor configurado, se muestra en esta columna.

## ¿Qué desea hacer?

Para:	Haga lo siguiente:
Agregar una conexión nueva.	Haga clic en <b>Agregar</b> y seleccione la conexión en el menú contextual.
Agregar una nueva interfaz lógica.	Haga clic en <b>Agregar</b> y seleccione Nueva interfaz lógica del menú contextual.
Agregar una nueva interfaz de LAN virtual.	Haga clic en <b>Agregar</b> , seleccione <b>Nueva interfaz lógica</b> del menú contextual y, a continuación, seleccione <b>LAN virtual</b> del submenú.
Editar una interfaz existente.	Resalte la interfaz que desea editar y haga clic en <b>Editar</b> .  <b>Nota</b> Si está editando un túnel GRE, la ficha Conexión no aparecerá si dicho túnel no está configurado para que utilice el modo <b>gre ip</b> .
Restablecer una interfaz física a un estado no configurado.	Seleccione la interfaz física y haga clic en <b>Restablecer</b> .

Para:	Haga lo siguiente:
Eliminar una interfaz lógica.	Seleccione la interfaz que desea eliminar y haga clic en <b>Eliminar</b> .
Ver cómo realizar tareas de configuración relacionadas.	Consulte uno de los procedimientos siguientes: <ul style="list-style-type: none"> <li>• <a href="#">¿Cómo se configura una ruta estática?</a></li> <li>• <a href="#">¿Cómo se visualiza la actividad en la interfaz LAN?</a></li> <li>• <a href="#">¿Cómo se activa o desactiva una interfaz?</a></li> <li>• <a href="#">¿Cómo se visualizan los comandos de IOS que se envían al router?</a></li> <li>• <a href="#">¿Cómo se configura una interfaz WAN no admitida?</a></li> <li>• <a href="#">¿Cómo se visualiza la actividad en la interfaz WAN?</a></li> <li>• <a href="#">¿Cómo se configura NAT en una interfaz WAN?</a></li> <li>• <a href="#">¿Cómo se configura una ruta estática?</a></li> <li>• <a href="#">¿Cómo se configura un protocolo de enrutamiento dinámico?</a></li> </ul>

### ¿Por qué algunas interfaces o conexiones son de sólo lectura?

Existen varias condiciones que impiden que Cisco SDM modifique una interfaz o subinterfaz configurada anteriormente.

- Para conocer los motivos por los cuales una interfaz o subinterfaz serie configurada anteriormente puede aparecer como de sólo lectura en la lista de interfaces, consulte el tema de ayuda [Motivos por los cuales una configuración de interfaz o subinterfaz de serie puede ser de sólo lectura](#).
- Para conocer los motivos por los cuales una interfaz o subinterfaz ATM configurada anteriormente puede aparecer como de sólo lectura en la lista de interfaces, consulte el tema de ayuda [Motivos por los cuales una configuración de interfaz o subinterfaz ATM puede ser de sólo lectura](#).
- Para conocer los motivos por los cuales una interfaz o subinterfaz Ethernet LAN o WAN configurada anteriormente puede aparecer como de sólo lectura en la lista de interfaces, consulte el tema de ayuda [Motivos por los cuales una configuración de interfaz Ethernet puede ser de sólo lectura](#).
- Para conocer los motivos por los cuales una interfaz o subinterfaz ISDN (RDSI) BRI configurada anteriormente puede aparecer como de sólo lectura en la lista de interfaces, consulte el tema de ayuda [Motivos por los cuales una configuración de interfaz ISDN \(RDSI\) BRI puede ser de sólo lectura](#).

# Conexión: Ethernet para IRB

Este cuadro de diálogo contiene los siguientes campos si ha seleccionado **Ethernet para IRB** en la lista Configurar.

## Grupo Bridge actual/BVI asociada

Estos campos de sólo lectura contienen el valor del grupo del bridge actual y el nombre de la Interfaz Virtual del Grupo del Bridge (BVI, Bridge-Group Virtual Interface) actual.

## Cree un Grupo Bridge/Únase a un Grupo Bridge existente

Seleccione si desea hacer que esta interfaz sea miembro de un nuevo Grupo Bridge, o si desea unirse a un Grupo Bridge existente. Si desea crear un nuevo Grupo Bridge, especifique un número entre 1 y 255. Si desea que la interfaz se una a un Grupo Bridge existente, seleccione la interfaz BVI que ya sea miembro de ese grupo.

## Dirección IP

Especifique la dirección IP y la máscara de subred en los campos proporcionados.

## DNS dinámico

Active el DNS dinámico si desea actualizar los servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN.



### Nota

---

Esta función sólo aparece si es admitida por la versión de Cisco IOS en su router.

---

Para escoger un método de DNS dinámico a usar, haga algo de lo siguiente:

- Introduzca el nombre de un método existente de DNS dinámico.

Introduzca el nombre en el campo de Método DNS dinámico exactamente como aparece en la lista en **Configurar > Tareas adicionales > Métodos de DNS dinámico**.

- Escoja un método existente de DNS dinámico de una lista.  
Haga clic en el menú desplegable y escoja un método existente. Se abrirá una ventana con una lista de los métodos existentes de DNS dinámico. Esta opción del menú está disponible sólo si hay métodos existentes de DNS dinámico.
- Cree un nuevo método de DNS dinámico.  
Haga clic en el menú desplegable y elija crear un nuevo método de DNS dinámico.

Para borrar un método asociado de DNS dinámico de la interfaz, elija **Ninguno** del menú desplegable.

## Conexión: Ethernet para enrutamiento

Este cuadro de diálogo contiene los siguientes campos si ha seleccionado **Ethernet para enrutamiento** en la lista Configurar.

### Dirección IP

Especifique una dirección IP y máscara de subred en los campos de Dirección IP. Esta dirección será la dirección IP origen para el tráfico originado desde esta interfaz, y la dirección IP de destino para el tráfico destinado a los hosts conectados a esta interfaz.

### DHCP Relay

Haga clic en este botón para permitir que el router funcione como un DHCP relay. Un dispositivo que funciona como un DHCP reenvía solicitudes DHCP a un servidor DHCP. Cuando un dispositivo requiere una dirección IP asignada dinámicamente, éste envía una solicitud DHCP. Un servidor DHCP responde a esta solicitud con una dirección IP. Puede haber un máximo de un DHCP o un servidor DHCP por subred.



#### Nota

---

Si el router se configuró para que funcione como un DHCP relay y para disponer de más de una dirección IP de servidor remoto DHCP, estos campos están desactivados.

---

#### Dirección IP del servidor DHCP remoto

Especifique la dirección IP del servidor DHCP que proporcionará las direcciones a los dispositivos de la LAN.

## DNS dinámico

Active el DNS dinámico si desea actualizar los servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN.



### Nota

Esta función sólo aparece si es admitida por la versión de Cisco IOS en su router.

Para escoger un método de DNS dinámico a usar, haga algo de lo siguiente:

- Introduzca el nombre de un método existente de DNS dinámico.  
Introduzca el nombre en el campo de Método DNS dinámico exactamente como aparece en la lista en **Configurar > Tareas adicionales > Métodos de DNS dinámico**.
- Escoja un método existente de DNS dinámico de una lista.  
Haga clic en el menú desplegable y escoja un método existente. Se abrirá una ventana con una lista de los métodos existentes de DNS dinámico. Esta opción del menú está disponible sólo si hay métodos existentes de DNS dinámico.
- Cree un nuevo método de DNS dinámico.  
Haga clic en el menú desplegable y elija crear un nuevo método de DNS dinámico.

Para borrar un método asociado de DNS dinámico de la interfaz, elija **Ninguno** del menú desplegable.

## Métodos existentes de DNS dinámico

Esta ventana permite que usted escoja un método de DNS dinámico para relacionarlo con una interfaz WAN.

La lista de los métodos existentes de DNS dinámico muestra cada nombre del método y los parámetros asociados. Elija un método de la lista, y luego haga clic en **Aceptar** para asociarlo a la interfaz WAN.

Para agregar, editar, o eliminar los métodos de DNS dinámico, vaya a **Configurar > Tareas adicionales > Métodos de DNS dinámico**.

## Agregar Método de DNS dinámico

Esta ventana permite que usted agregue un método de DNS dinámico. Escoja el tipo de método, HTTP o IETF, y configúrelo.

### HTTP

HTTP es un método de DNS dinámico que actualiza a un proveedor de servicio de DNS con cambios en la dirección IP de la interfaz asociada.

### Servidor

Si se usa HTTP, elija la dirección de dominio del proveedor de servicio DNS desde el menú desplegable.

### Nombre de usuario

Si se usa HTTP, especifique un nombre de usuario para acceder al proveedor de servicio DNS.

### Contraseña

Si se usa HTTP, especifique una contraseña para acceder al proveedor de servicio DNS.

### IETF

IETF es un método de DNS dinámico que actualiza a un servidor de DNS con los cambios para la dirección IP de la interfaz asociada.

### Servidor de DNS

Si usa IETF, y no hay ningún servidor DNS configurado para el router en **Configurar > Tareas adicionales > DNS**, entonces introduzca la dirección IP del servidor DNS.

## Nombre del Host

Introduzca un nombre de host si no hay uno configurado en **Configurar > Tareas adicionales > Propiedades del router > Editar > Host**, o si desea sobrescribir el nombre del host. Cuando actualice la dirección IP de la interfaz, el método de DNS dinámico enviará el nombre del host junto con la nueva dirección IP de la interfaz.

## Nombre del Dominio

Introduzca un nombre de dominio si no se ha configurado uno en **Configurar > Tareas adicionales > Propiedades del router > Editar > Dominio**, o si desea sobrescribir el nombre de dominio. Cuando actualice la dirección IP de la interfaz, el método de DNS dinámico enviará el nombre de dominio junto con la nueva dirección IP de la interfaz.

# Inalámbrica

Si el router tiene una interfaz inalámbrica, puede iniciar la aplicación inalámbrica desde esta ficha. También puede iniciar la aplicación inalámbrica desde el menú Herramientas si selecciona **Herramientas > Aplicación inalámbrica**.

# Asociación

Utilice esta ventana para ver, crear, editar o eliminar asociaciones entre interfaces y reglas o conexiones VPN.

## Interfaz

El nombre de la interfaz seleccionada en la ventana Interfaces y conexiones.

## Zona

Si esta interfaz es miembro de una [zona de seguridad](#), el nombre de la zona aparece en este campo. Si desea incluir esta interfaz en una zona de seguridad, haga clic en el botón ubicado a la derecha del campo, elija **Seleccionar una zona**, y especifique la zona en el diálogo que aparece. Si necesita crear una zona nueva, seleccione **Crear una zona**, especifique un nombre para la zona en el diálogo que aparece y haga clic en Aceptar. El nombre de la zona creada aparece en el campo zona.



## Regla de acceso

Los nombres o números de las reglas de acceso asociadas con esta interfaz. Dichas reglas permiten o deniegan tráfico que coincide con la dirección IP y los criterios de servicio especificados en la regla.

### Entrante

El nombre o número de una regla de acceso que se aplica al tráfico entrante en esta interfaz. Si desea aplicar una regla, haga clic en el botón ... y seleccione una regla de acceso existente. O bien, puede crear una nueva regla de acceso y seleccionarla.

Cuando una regla se aplica al tráfico entrante de una interfaz, filtra el tráfico antes de que éste haya entrado en el router. Se abandonan todos los paquetes no permitidos por la regla y no volverán a enrutarse a ninguna otra interfaz. Al aplicar una regla a la dirección entrante de una interfaz, no sólo impide su entrada en una red fiable conectada al router, sino que también impide que el router local la enrute hacia cualquier otro lugar.

### Saliente

El nombre o número de una regla de acceso que se aplica al tráfico saliente en esta interfaz. Si desea aplicar una regla, haga clic en el botón ... y seleccione una regla de acceso existente. O bien, puede crear una nueva regla de acceso y seleccionarla.

Cuando una regla se aplica al tráfico saliente de una interfaz, filtra el tráfico después de que éste entre en el router pero antes de que haya salido de la interfaz. Se abandonan todos los paquetes no permitidos por la regla antes de que salgan de la interfaz.

## Regla de inspección

Los nombres de las reglas de inspección asociadas con esta interfaz. Las reglas de inspección crean agujeros temporales en los firewalls de manera que los hosts dentro del firewall que iniciaron sesiones de cierto tipo puedan recibir tráfico de vuelta del mismo tipo.

### Entrante

El nombre o número de una regla de inspección que se aplica al tráfico entrante de esta interfaz. Si desea aplicar una regla entrante, haga clic en el menú desplegable **Entrante** y seleccione una regla.

**Saliente**

El nombre o número de una regla de inspección que se aplica al tráfico saliente de esta interfaz. Si desea aplicar una regla saliente, haga clic en el menú desplegable **Saliente** y seleccione una regla.

**VPN**

Las VPN protegen el tráfico que se puede transmitir a través de líneas que no controla la organización. Es posible utilizar la interfaz seleccionada en una VPN al asociarla con una política IPsec.

**Política IPsec**

La política IPsec configurada y asociada con esta interfaz. Para asociar la interfaz con una política IPsec, seleccione la política de esta lista.

**Nota**


---

Una interfaz se puede asociar con una sola política IPsec.

---

**Nota**


---

Para crear un túnel GRE sobre IPsec, primero debe asociar la política con la interfaz de túnel y, a continuación, asociarla con la interfaz de origen del túnel. Por ejemplo, para asociar una política con el Túnel3 cuya interfaz de origen es Serie0/0, en primer lugar, seleccione Túnel3 en la ventana Interfaces y conexiones, haga clic en **Editar**, asocie la política con la misma y luego haga clic en **Aceptar**. A continuación, seleccione la interfaz Serie0/0 y asóciela la misma política.

---

**EzVPN**

Si la interfaz se utiliza en una conexión Easy VPN, el nombre de la conexión se muestra aquí.

**Nota**


---

Una interfaz no puede utilizarse simultáneamente en una conexión VPN y en una conexión Easy VPN.

---

## Cambios de asociación

Cuando usted cambia las propiedades de asociación de una interfaz, los cambios se reflejan en la parte inferior de la ventana de Editar Interfaz/ Conexión. Por ejemplo, si asocia una política IPsec con la interfaz, su nombre se muestra en la parte inferior de la ventana. Si elimina una asociación, el valor de la columna Valor de elemento cambia a <Ninguno>.

## NAT

Si su intención es utilizar esta interfaz en una configuración NAT, debe designarla como una interfaz interna o externa. Seleccione la dirección de tráfico a la que debe aplicarse NAT. Si la interfaz se conecta a una LAN a la que presta servicio el router, seleccione **Interna**. Si se conecta a Internet o a la WAN de la organización, seleccione **Externa**. Si ha seleccionado una interfaz que no se puede utilizar en una configuración NAT como, por ejemplo, una interfaz lógica, se desactivará este campo y figurará el valor No admitido.

## Editar puerto del switch

En esta ventana se puede editar la información de la LAN virtual para los puertos de switch Ethernet.

### Grupo de modo

Seleccione el tipo de información de la LAN virtual que debe transmitirse a través de este puerto de switch Ethernet. Al seleccionar **Acceso**, el puerto del switch reenviará solamente los datos cuyo destino sea un número de LAN virtual específico. Al seleccionar **Trunking (Enlaces)**, el puerto del switch reenvía datos a todas las LAN virtuales, incluidos los datos propios de la LAN virtual. Solamente seleccione **Trunking (Enlaces)** para “enlazar” los puertos de la LAN virtual que se conectan a otros dispositivos de red como, por ejemplo, otro switch que se conectará a los dispositivos en varias LAN virtuales.

## VLAN

Para asignar el puerto del switch a una LAN virtual, especifique el número de dicha red a la que debe pertenecer el puerto del switch. Si el puerto del switch no tiene asociada ninguna LAN virtual, este campo mostrará el valor VLAN1 por defecto. Para crear una nueva interfaz de LAN virtual que corresponda al ID de LAN virtual, especifique dicho ID aquí y marque la casilla de verificación **Haga la LAN virtual visible en la lista de interfaces**.

### Casilla de verificación Haga la LAN virtual visible en la lista de interfaces

Seleccione esta casilla si desea crear una nueva LAN virtual con el ID de LAN virtual especificado en el campo LAN virtual.

### Socio de la pila

Seleccione el módulo de switch que desea utilizar como el socio de la pila. Cuando un dispositivo contiene varios módulos de switch, éstos deben apilarse antes de los demás socios de la pila.

### Número de Grupo Bridge

Si desea que este puerto de switch forme parte de un bridge a una red inalámbrica, especifique el número de un grupo bridge existente.

### Velocidad

Elija la velocidad para que coincida con la red a la que se conectará el puerto de switch. O bien, seleccione **automático** para que la velocidad se establezca automáticamente en el valor óptimo.

### Dúplex

Seleccione **full** o **half**, o **automática** para que el dúplex se establezca automáticamente para que coincida con la red a la que se conectará el puerto de switch.

Si **Velocidad** está definida en **automática**, **Dúplex** estará desactivado.

## Alimentación de entrada

La lista desplegable **Alimentación de entrada** aparece si el puerto del switch admite una fuente de alimentación de entrada. Elija uno de los valores siguientes:

- **automático**: detecta automáticamente los dispositivos de alimentación de entrada.
- **nunca**: nunca aplica la alimentación de entrada.

# Servicio de aplicación

Esta ventana permite asociar políticas QoS y supervisión de aplicaciones y protocolos a la interfaz seleccionada.

## Calidad de servicio (QoS)

Para asociar una política QoS a la interfaz en la dirección entrante, seleccione una política QoS en el menú desplegable **Entrante**.

Para asociar una política QoS a la interfaz en la dirección saliente, seleccione una política QoS en el menú desplegable **Saliente**.

Las estadísticas de QoS para la interfaz pueden supervisarse yendo a **Supervisar > Estado del tráfico > QoS**.

## Netflow

Para asociar la supervisión de las estadísticas de Netflow a la interfaz en la dirección entrante, seleccione la casilla de verificación **Entrante**.

Para asociar la supervisión de las estadísticas de Netflow a la interfaz en la dirección saliente, seleccione la casilla de verificación **Saliente**.

Las estadísticas de Netflow para la interfaz pueden supervisarse yendo a **Supervisar > Estado de la interfaz**. Los usuarios más activos de la red y los protocolos que generan más tráfico de Netflow pueden supervisarse en **Supervisar > Estado del tráfico > N flujos de tráfico más activos**.

## NBAR

Para asociar el Reconocimiento de aplicaciones basadas en la red (NBAR) a la interfaz, seleccione la casilla de verificación **Protocolo NBAR**.

Las estadísticas de NBAR para la interfaz pueden supervisarse en **Supervisar > Estado del tráfico > Tráfico de aplicaciones/protocolos**.

# General

En esta ventana se muestra la configuración de seguridad general y se permite activarla o desactivarla al marcar o desmarcar la casilla de verificación situada junto al nombre y la descripción. Si ha habilitado la función Auditoría de seguridad para desactivar determinadas propiedades y desea volver a activarlas, puede hacerlo en esta ventana. En esta pantalla se muestran las propiedades siguientes:

## Descripción

En este campo usted podrá introducir una breve descripción de la configuración de la interfaz. Esta descripción es visible en la ventana de Editar Interfaces y Conexiones. Una descripción, tal como “Contabilidad” o “Red 5 de prueba”, puede ayudar a otros usuarios de Cisco SDM a comprender el propósito de la configuración.

## Difusiones dirigidas por IP

Una difusión dirigida por IP es un datagrama que se envía a la dirección de difusión de una subred a la que la máquina que realiza el envío no está conectada directamente. La difusión dirigida se enruta a través de la red como un paquete de unidifusión hasta que alcanza la subred de destino, donde se convierte en una difusión de capa de enlace. Debido a la naturaleza de la arquitectura de direcciones IP, solamente el último router de la cadena (el que se conecta directamente a la subred de destino) puede identificar de manera concluyente una difusión dirigida. Las difusiones dirigidas a veces se utilizan por motivos legítimos, pero este tipo de uso no es común fuera del sector de servicios financieros.

Las difusiones dirigidas por IP se utilizan para los comunes y populares ataques “smurf” de denegación de servicio y también pueden utilizarse en ataques relacionados. En un ataque “smurf”, el atacante envía solicitudes de eco ICMP desde una dirección de origen falsificada a una dirección de difusión dirigida, lo que hace que todos los hosts de la subred de destino envíen respuestas al origen falsificado. Al enviar un flujo continuo de tales solicitudes, el atacante puede crear un flujo de respuesta mucho más grande, que puede inundar completamente al host cuya dirección está siendo falsificada.

Desactivar las difusiones dirigidas por IP excluye a las difusiones dirigidas que de otro modo “revertirían” a nivel de enlace en esa interfaz.

## ARP Proxy IP

La red utiliza ARP para convertir direcciones IP en direcciones MAC. Normalmente, ARP se limita a una sola LAN, pero un router puede funcionar como proxy para las peticiones ARP, lo que hace que las consultas ARP estén disponibles en varios segmentos LAN. Puesto que rompe la barrera de seguridad de la LAN, el ARP proxy sólo debe utilizarse entre dos LAN con el mismo nivel de seguridad, y sólo cuando sea necesario.

## Flujo de caché por ruta IP

Esta opción activa la función Netflow de Cisco IOS. Al usar Netflow, puede determinar la distribución de paquetes, la distribución de protocolos y los flujos actuales de los datos en el router. Esta información es útil para ciertas tareas tales como buscar el origen de un ataque tipo spoof a la dirección IP.



### Nota

---

La opción Flujo de caché por ruta IP activa Netflow en el tráfico entrante y saliente. Para activar Netflow en el tráfico entrante o saliente, use las opciones de Netflow disponibles en la ficha **Servicio de aplicación**.

---

## Redireccionamiento IP

Los mensajes de redireccionamiento de ICMP instruyen a un nodo final a usar un router específico como parte de su ruta a un destino en particular. En una red de IP que funciona apropiadamente, un router envía redireccionamientos solamente a los hosts en sus propias subredes locales, y ningún nodo final enviará nunca un redireccionamiento, y ningún redireccionamiento negará nunca más de un salto de la red. Sin embargo, un atacante podría violar estas reglas. Desactivar los redireccionamientos de ICMP no tiene ningún efecto negativo en la red y puede eliminar los ataques de redireccionamiento.

## Respuesta a la máscara de IP

Los mensajes de respuesta de máscara ICMP se envían cuando un dispositivo de red debe conocer la máscara de subred para una subred determinada en la interred. Dichos mensajes se envían al dispositivo que solicita información mediante los dispositivos que disponen de la información solicitada. Un atacante puede utilizar dichos mensajes para obtener información de asignación de la red.

## IP de destino inalcanzables

Los mensajes de host inalcanzable ICMP se envían si un router recibe un paquete de no difusión que utiliza un protocolo desconocido o si un router recibe un paquete que no puede entregar al destino final porque no conoce ninguna ruta hacia la dirección de destino. Un atacante puede utilizar dichos mensajes para obtener información de asignación de la red.

# Seleccionar el tipo de configuración Ethernet

Esta ventana se muestra cuando usted hace clic en una interfaz en la ventana Interfaces y conexiones, y Cisco SDM no puede determinar si la interfaz está configurada como una interfaz LAN o como una interfaz WAN. Al configurar una interfaz mediante Cisco SDM, se designa como una interfaz interna o externa y Cisco SDM agrega un comentario descriptivo al archivo de configuración en función de dicha designación. Si configura una interfaz mediante la interfaz de línea de comandos (CLI), la configuración no incluirá este comentario descriptivo y Cisco SDM no dispondrá de dicha información.

## Para indicar que la interfaz es una interfaz LAN:

Haga clic en **LAN** y, a continuación, en **Aceptar**. Cisco SDM agrega la línea de comentario \$ETH-LAN\$ a la configuración de la interfaz, y la interfaz aparece en la ventana del asistente para LAN con la designación Interna en la ventana Interfaces y conexiones.

## Para indicar que la interfaz es una interfaz WAN:

Haga clic en **WAN** y, a continuación, en **Aceptar**. Cisco SDM agrega la línea de comentario \$ETH-WAN\$ a la configuración de la interfaz, y la interfaz aparece en la ventana del asistente para WAN con la designación Externa en la ventana Interfaces y conexiones.



# Conexión: VLAN

Esta ventana le permite configurar una interfaz VLAN.

## ID de LAN virtual

Introduzca el número de identificación de la nueva interfaz de VLAN. Si usted está editando una interfaz de VLAN, usted no puede cambiar el identificador de VLAN.

## Casilla de verificación VLAN nativa

Verifique si la VLAN es una VLAN sin troncal.

## Campos de Dirección IP

### Tipo de dirección IP de la interfaz

Indique si esta interfaz de LAN virtual dispondrá de una dirección IP estática o si no tendrá ninguna dirección IP. Este campo es visible cuando se selecciona **Sólo VLAN** en el campo Configurar como.

### Dirección IP

Especifique la dirección IP de la interfaz de LAN virtual.

### Máscara de subred

Especifique la máscara de subred de la interfaz LAN virtual o utilice el campo para indicar el número de bits de subred.

### Relé DHCP

Para obtener más información, haga clic en [DHCP Relay](#).

## Lista de subinterfases

Esta ventana muestra los subinterfases configurados para la interfaz que usted escogió, y le permite agregar, editar, y quitar los subinterfases configurados. Para cada subinterfaz configurada, la ventana muestra la identificación de la Subinterfaz, la identificación de la VLAN, la dirección IP y la máscara, y una descripción, si se introdujo una. Por ejemplo, si el router tuviera la interfaz FastEthernet 1, y están configuradas las Subinterfases FastEthernet1.3 y FastEthernet1.5, esta ventana podría mostrar lo siguiente:

5	56	56.8.1.1/255.255.255.0
3	67	Nro. de puente 77

En este ejemplo, FastEthernet1.5 está configurada para enrutamiento, y FastEthernet1.3 está configurada para [IRB](#).



### Nota

Usted debe escoger la interfaz física en la que los subinterfases están configurados para mostrar esta ventana. Para el ejemplo descrito, tendría que escoger FastEthernet 1 para mostrar esta ventana. Si usted escogió FastEthernet1.3 o FastEthernet1.5 e hizo clic en edición, mostrará el diálogo de edición con la información para esa interfaz.

### Botones Agregar, Editar y Eliminar

Use estos botones para configurar, editar, y eliminar subinterfases de la interfaz física elegida.

## Agregar/Editar una interfaz BVI

En esta ventana puede agregar o editar una Interfaz virtual de grupo bridge (BVI). Si el router tiene una interfaz Dot11Radio, se crea automáticamente una BVI cuando configura el nuevo grupo bridge. Esto se hace para admitir el establecimiento de bridges IRB. Puede cambiar la dirección IP y la máscara de subred en esta ventana.

### Dirección IP/máscara de subred

Especifique la dirección IP y la máscara de subred que desea otorgar a la BVI.

# Agregar o editar una interfaz de retrobucle

Esta ventana permite agregar una interfaz de retrobucle a la interfaz seleccionada.

## Dirección IP

Seleccione si la interfaz de retrobucle debe disponer de una dirección IP estática o si no debe tener ninguna dirección IP.

### Dirección IP estática

Si ha seleccionado **Dirección IP estática**, especifíquela en este campo.

### Máscara de subred

Especifique en este campo la máscara de subred o seleccione el número de bits de subred del campo situado a la derecha. La máscara de subred indica al router cuáles bits de la dirección IP designan la dirección de la red y qué bits designan la dirección del host.

# Conexión: Interfaz de plantilla virtual

Puede agregar o editar una [VTI](#) como parte de una configuración 802.1x o VPN. Cuando edita una VTI, los campos que puede editar aparecen en la ficha Conexión.

## Tipo de interfaz

Seleccione **por defecto** o **túnel**. Si selecciona túnel, también debe seleccionar un modo túnel.

## Dirección IP

Seleccione **No numerado**. La VTI utiliza la dirección IP de la interfaz física seleccionada en el campo No numerado en.

## No numerado en

Este campo aparece cuando selecciona **No numerado** en el campo Dirección IP. Seleccione la interfaz cuya dirección IP desea que use esta VTI.

## Modo túnel

Seleccione **IPSec-IPv4**.

# Conexión: LAN Ethernet

Utilice esta ventana para configurar la **Dirección IP** y las propiedades de **DHCP** de una interfaz **Ethernet** que desee utilizar como una interfaz LAN.

## Dirección IP

Especifique una dirección IP para esta interfaz. El valor de la dirección IP se obtiene del proveedor de servicios o del administrador de redes. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

## Máscara de subred

Especifique la [máscara de subred](#). Obtenga este valor del administrador de redes. La máscara de subred permite que el router determine qué porción de la dirección IP se utilizará para definir la parte de red y subred de la dirección.

## DHCP Relay

Haga clic en este botón para permitir que el router funcione como un DHCP relay. Un dispositivo que funciona como un DHCP reenvía solicitudes DHCP a un servidor DHCP. Cuando un dispositivo requiere una dirección IP asignada dinámicamente, éste envía una solicitud DHCP. Un servidor DHCP responde a esta solicitud con una dirección IP. Puede haber un máximo de un DHCP relay o un servidor DHCP por subred.



### Nota

---

Si el router se configuró para que funcione como un DHCP relay con más de una dirección IP de servidor remoto DHCP, este botón estará desactivado.

---

### Dirección IP del servidor DHCP remoto

Si ha hecho clic en **DHCP Relay**, especifique la dirección IP del servidor DHCP que proporcionará las direcciones a los dispositivos de la LAN.

# Conexión: WAN Ethernet

Esta ventana permite agregar una conexión WAN Ethernet.

## Activar encapsulación PPPoE

Haga clic en esta opción si la conexión debe usar el protocolo Punto A Punto Sobre Encapsulación de Ethernet (PPPoE, Point-to-Point Protocol over Ethernet). El proveedor de servicios puede indicarle si la conexión utiliza PPPoE. Al configurar una conexión PPPoE, se crea una interfaz de marcación automáticamente.

## Dirección IP

Seleccione uno de los siguientes tipos de direcciones IP y especifique la información en los campos que aparecen. Si la conexión Ethernet no utiliza PPPoE, sólo aparecerán las opciones Dirección IP estática y Dirección IP dinámica.

### Dirección IP estática

Si selecciona **Dirección IP estática**, introduzca la dirección IP y la máscara de subred o los bits de la red en los campos proporcionados. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

### Dinámica (cliente DHCP)

Si selecciona **Dinámica**, el router aceptará una dirección IP de un servidor DHCP remoto. Especifique el nombre del servidor DHCP del que se cederán las direcciones.

### IP no numerado

Seleccione **IP no numerado** cuando desee que la interfaz comparta una dirección IP que ya esté asignada a otra interfaz. Luego escoja la interfaz cuya dirección IP de esta interfaz es para compartir.

### IP simple (IP negociado)

Seleccione esta opción si el router debe obtener una dirección IP a través de la negociación de direcciones PPP/IPCP (Point-to-Point Protocol/IP Control Protocol).

## Autenticación

Haga clic en este botón para especificar la información de contraseña de autenticación de [CHAP/PAP](#).

## DNS dinámico

Active el DNS dinámico si desea actualizar los servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN.



### Nota

---

Esta función sólo aparece si es admitida por la versión de Cisco IOS en su router.

---

Para escoger un método de DNS dinámico a usar, haga algo de lo siguiente:

- Introduzca el nombre de un método existente de DNS dinámico.  
Introduzca el nombre en el campo de Método DNS dinámico exactamente como aparece en la lista en **Configurar > Tareas adicionales > Métodos de DNS dinámico**.
- Escoja un método existente de DNS dinámico de una lista.  
Haga clic en el menú desplegable y escoja un método existente. Se abrirá una ventana con una lista de los métodos existentes de DNS dinámico. Esta opción del menú está disponible sólo si hay métodos existentes de DNS dinámico.
- Cree un nuevo método de DNS dinámico.  
Haga clic en el menú desplegable y elija crear un nuevo método de DNS dinámico.

Para borrar un método asociado de DNS dinámico de la interfaz, elija **Ninguno** del menú desplegable.

# Ethernet Properties (Propiedades de Ethernet)

Esta ventana permite configurar las propiedades para un enlace de WAN Ethernet.

## Activar encapsulación PPPoE

Haga clic en **Activar encapsulación PPPoE** si el proveedor de servicios requiere el uso de dicha opción. **PPPoE** especifica el protocolo punto a punto sobre la encapsulación de Ethernet.

## Dirección IP

### Dirección IP estática

Disponible con encapsulación PPPoE y sin encapsulación. Si selecciona **Dirección IP estática**, introduzca la dirección IP y la máscara de subred o los bits de la red en los campos proporcionados. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

### Dinámica (cliente DHCP)

Disponible con encapsulación PPPoE y sin encapsulación. Si selecciona **Dinámica**, el router aceptará una dirección IP de un servidor DHCP remoto. Especifique el nombre del servidor DHCP que asignará las direcciones.

### IP no numerado

Disponible con encapsulación PPPoE. Seleccione **IP no numerado** cuando desee que la interfaz comparta una dirección IP que ya se ha asignado a otra interfaz. Luego escoja la interfaz cuya dirección IP de esta interfaz es para compartir.

### IP simple (IP negociado)

Disponible con encapsulación PPPoE. Seleccione **IP simple (IP negociado)** cuando el router obtendrá una dirección IP a través de la negociación de direcciones PPP/IPCP.

## Autenticación

Haga clic en este botón para especificar la información de contraseña de autenticación de [CHAP/PAP](#).

## DNS dinámico

Active el DNS dinámico si desea actualizar los servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN.

**Nota**

Esta función sólo aparece si es admitida por la versión de Cisco IOS en su router.

Para escoger un método de DNS dinámico a usar, haga algo de lo siguiente:

- Introduzca el nombre de un método existente de DNS dinámico.  
Introduzca el nombre en el campo de Método DNS dinámico exactamente como aparece en la lista en **Configurar > Tareas adicionales > Métodos de DNS dinámico**.
- Escoja un método existente de DNS dinámico de una lista.  
Haga clic en el menú desplegable y escoja un método existente. Se abrirá una ventana con una lista de los métodos existentes de DNS dinámico. Esta opción del menú está disponible sólo si hay métodos existentes de DNS dinámico.
- Cree un nuevo método de DNS dinámico.  
Haga clic en el menú desplegable y elija crear un nuevo método de DNS dinámico.

Para borrar un método asociado de DNS dinámico de la interfaz, elija **Ninguno** del menú desplegable.



# Conexión: Ethernet sin encapsulación

Use esta ventana para configurar una conexión de Ethernet sin encapsulación.

## Dirección IP

Seleccione cómo el router obtendrá una [Dirección IP](#) para este enlace.

- **Dirección IP estática:** si selecciona esta opción, especifique la dirección IP y la máscara de subred o los bits de red en los campos proporcionados. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).
- **Dirección IP dinámica:** si selecciona esta opción, el router aceptará una dirección IP de un servidor DHCP remoto. A continuación, especifique el nombre o la dirección IP del servidor DHCP.

## Nombre del Host

Si el proveedor de servicios inserta un nombre de host para el router en la respuesta DHCP que contiene la dirección IP dinámica, puede especificar dicho nombre en este campo con fines informativos.

## DNS dinámico

Active el DNS dinámico si desea actualizar los servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN.



### Nota

---

Esta función sólo aparece si es admitida por la versión de Cisco IOS en su router.

---

Para escoger un método de DNS dinámico a usar, haga algo de lo siguiente:

- Introduzca el nombre de un método existente de DNS dinámico.  
Introduzca el nombre en el campo de Método DNS dinámico exactamente como aparece en la lista en **Configurar > Tareas adicionales > Métodos de DNS dinámico**.
- Escoja un método existente de DNS dinámico de una lista.  
Haga clic en el menú desplegable y escoja un método existente. Se abrirá una ventana con una lista de los métodos existentes de DNS dinámico. Esta opción del menú está disponible sólo si hay métodos existentes de DNS dinámico.

- Cree un nuevo método de DNS dinámico.

Haga clic en el menú desplegable y elija crear un nuevo método de DNS dinámico.

Para borrar un método asociado de DNS dinámico de la interfaz, elija **Ninguno** del menú desplegable.

## Conexión: ADSL

Esta ventana permite especificar o editar las propiedades de un enlace PPPoE compatible con una conexión ADSL.

### Encapsulación

Seleccione el tipo de encapsulación que se utilizará para este enlace.

- PPPoE especifica el protocolo punto a punto sobre la encapsulación de Ethernet.
- PPPoA especifica la encapsulación del protocolo punto a punto sobre ATM.
- Enrutamiento RFC1483 (AAL5SNAP) especifica que cada PVC puede llevar varios protocolos.
- Enrutamiento RFC1483 (AAL5MUX) especifica que cada PVC puede contener un solo tipo de protocolo.

Si está modificando una conexión, la encapsulación se muestra pero no se puede editar. Si necesita cambiar el tipo de encapsulación, elimine la conexión y vuelva a crearla con el tipo de encapsulación necesario.

Para obtener más información acerca de los tipos de encapsulación, haga clic [Encapsulación](#).

### Identificador de la ruta virtual

El identificador de ruta virtual (VPI) se utiliza en la conmutación y el enrutamiento ATM para identificar la ruta que se utiliza para una variedad de conexiones. Especifique el valor VPI que le ha proporcionado el proveedor de servicios.

Si está modificando una conexión existente, este campo aparece desactivado. Si necesita cambiar este valor, elimine la conexión y vuelva a crearla con el valor necesario.

## Identificador de circuito virtual

El Identificador de Circuito Virtual (VCI, Virtual Circuit Identifier) se usa en la conmutación y enrutamiento de ATM para identificar una conexión en particular dentro de una ruta que su conexión pueda compartir con otras conexiones. Introduzca el valor del VCI dado a usted por su proveedor de servicios.

Si está modificando una conexión existente, este campo aparece desactivado. Si necesita cambiar este valor, elimine la conexión y vuelva a crearla con el valor necesario.

## Dirección IP

Seleccione cómo el router obtendrá una [Dirección IP](#) para este enlace.

- **Dirección IP estática:** si selecciona esta opción, especifique la dirección IP y la máscara de subred o los bits de red en los campos proporcionados. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).
- **Dirección IP dinámica:** si selecciona esta opción, el router aceptará una dirección IP de un servidor DHCP remoto. A continuación, especifique el nombre o la dirección IP del servidor DHCP.
- Seleccione **IP no numerado** cuando desee que la interfaz comparta una dirección IP que ya se ha asignado a otra interfaz. Luego escoja la interfaz cuya dirección IP de esta interfaz es para compartir.
- **IP negociado:** esta interfaz obtendrá una dirección IP mediante la negociación de direcciones PPP/IPCP.

## Nombre de host

Si el proveedor de servicios le ha proporcionado un nombre de host para la opción DHCP 12, especifíquelo aquí.

## Modo operativo

Elija uno de los valores siguientes:

- **Automático:** configura la línea de la Línea de Suscriptor Digital Asimétrica (ADSL, Asymmetric Digital Subscriber Line) después de autonegociar con el Multiplexor de Acceso a la Línea de Suscriptor Digital (DSLAM, Digital Subscriber Access Line Multiplexer) ([DSLAM](#)) ubicada en la oficina central.
- **ansi-dmt:** configura la línea ADSL para prepararla en el modo ANSI T1.413 modo de conflicto 2.

- **itu-dmt**: configura la línea ADSL para prepararla en el modo de ITU G.992.1.
- **adls2**: configura la línea ADSL para que funcione en el modo de ITU G.992.3. Este modo está disponible para/b HWIC-ADSL-B/ST, HWIC-ADSLI-B/ST, HWIC-1ADSL, y los módulos de red de HWIC-1ADSLI ADSL.
- **adsl2+**: configura la línea ADSL para que funcione en el modo de ITU G.992.4. Este modo está disponible para/b HWIC-ADSL-B/ST, HWIC-ADSLI-B/ST, HWIC-1ADSL, y los módulos de red de HWIC-1ADSLI ADSL.
- **splitterless**: configure la línea ADSL para prepararla en el modo G.Lite. Este módulo está disponible para módulos de red ADSL más antiguos tales como el WIC-1ADSL.

## Autenticación

Haga clic en este botón si necesita especificar información de autenticación [CHAP](#) o [PAP](#).

## DNS dinámico

Active el DNS dinámico si desea actualizar los servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN.



### Nota

---

Esta función sólo aparece si es admitida por la versión de Cisco IOS en su router.

---

Para escoger un método de DNS dinámico a usar, haga algo de lo siguiente:

- Introduzca el nombre de un método existente de DNS dinámico.  
Introduzca el nombre en el campo de Método DNS dinámico exactamente como aparece en la lista en **Configurar > Tareas adicionales > Métodos de DNS dinámico**.
- Escoja un método existente de DNS dinámico de una lista.  
Haga clic en el menú desplegable y escoja un método existente. Se abrirá una ventana con una lista de los métodos existentes de DNS dinámico. Esta opción del menú está disponible sólo si hay métodos existentes de DNS dinámico.
- Cree un nuevo método de DNS dinámico.  
Haga clic en el menú desplegable y elija crear un nuevo método de DNS dinámico.

Para borrar un método asociado de DNS dinámico de la interfaz, elija **Ninguno** del menú desplegable.

### Enable Multilink PPP (Activar PPP multienlace)

Marque esta casilla de verificación si desea usar el Protocolo de punto a punto multienlace (Multilink Point-to-Point Protocol, MLP) con esta interfaz. MLP puede mejorar el rendimiento de una red con varias conexiones WAN utilizando la funcionalidad de equilibrado de carga, la fragmentación de paquetes, el ancho de banda a petición y otras funciones.

## Conexión: ADSL sobre ISDN (RDSI)

Agregue o modifique una conexión ADSL sobre ISDN (RDSI) en esta ventana.

### Encapsulación

Seleccione el tipo de encapsulación que se utilizará para este enlace.

- **PPPoE** especifica el protocolo punto a punto sobre la encapsulación de Ethernet.
- **Enrutamiento RFC1483 (AAL5SNAP)** especifica que cada PVC puede contener varios protocolos.
- **Enrutamiento RFC1483 (AAL5MUX)** especifica que cada PVC puede contener un solo tipo de protocolo.

Si está modificando una conexión, la encapsulación se muestra pero no se puede editar. Si necesita cambiar el tipo de encapsulación, elimine la conexión y vuelva a crearla con el tipo de encapsulación necesario.

### Identificador de la ruta virtual

El identificador de ruta virtual (VPI) se utiliza en la conmutación y el enrutamiento ATM para identificar la ruta que se utiliza para una variedad de conexiones. Este valor se obtiene del proveedor de servicios.

Si está modificando una conexión existente, este campo aparece desactivado. Si necesita cambiar este valor, elimine la conexión y vuelva a crearla con el valor necesario.

## Identificador de circuito virtual

El Identificador de Circuito Virtual (VCI, Virtual Circuit Identifier) se usa en la conmutación y enrutamiento de ATM para identificar una conexión en particular dentro de una ruta que su conexión pueda compartir con otras conexiones. Este valor se obtiene del proveedor de servicios.

Si está modificando una conexión existente, este campo aparece desactivado. Si necesita cambiar este valor, elimine la conexión y vuelva a crearla con el valor necesario.

## Dirección IP

Seleccione cómo el router obtendrá una [Dirección IP](#) para este enlace.

- **Dirección IP estática:** si selecciona esta opción, especifique la dirección IP y la máscara de subred o los bits de red en los campos proporcionados. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).
- **Dirección IP dinámica:** si selecciona esta opción, el router aceptará una dirección IP de un servidor DHCP remoto. A continuación, especifique el nombre o la dirección IP del servidor DHCP.
- Seleccione **IP no numerado** cuando desee que la interfaz comparta una dirección IP que ya se ha asignado a otra interfaz. Luego escoja la interfaz cuya dirección IP de esta interfaz es para compartir.
- IP negociado: esta interfaz obtendrá una dirección IP mediante la negociación de direcciones PPP/IPCP.

## Modo operativo

Seleccione el modo que la línea ADSL debe utilizar para la preparación.



### Nota

Si la versión de Cisco IOS que se está ejecutando en el router no admite los cinco modos operativos, se mostrarán solamente las opciones que corresponden a los modos operativos compatibles con dicha versión.

- **annexb:** modo Anexo B estándar de ITU-T G.992.1.
- **annexb-ur2:** modo Anexo B de ITU-T G.992.1.

- **Automático:** configura la línea de la Línea de Suscriptor Digital Asimétrica (ADSL, Asymmetric Digital Subscriber Line) después de autonegociar con el Multiplexor de Acceso a la Línea de Suscriptor Digital (DSLAM, Digital Subscriber Access Line Multiplexer) (**DSLAM**) ubicada en la oficina central.
- **etsi:** modo del ETSI (European Telecommunications Standards Institute).
- **multimodo:** modo elegido por el firmware para la mejor condición operativa en la Línea de Suscriptor Digital (DSL, Digital Subscriber Line). El modo final puede ser tanto modo ETSI como el modo Anexo-B estándar dependiendo de la configuración del DSLAM actual.

## Autenticación

Haga clic en este botón si necesita especificar información de autenticación [CHAP](#) o [PAP](#).

## DNS dinámico

Active el DNS dinámico si desea actualizar los servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN.



### Nota

---

Esta función sólo aparece si es admitida por la versión de Cisco IOS en su router.

---

Para escoger un método de DNS dinámico a usar, haga algo de lo siguiente:

- Introduzca el nombre de un método existente de DNS dinámico.  
Introduzca el nombre en el campo de Método DNS dinámico exactamente como aparece en la lista en **Configurar > Tareas adicionales > Métodos de DNS dinámico**.
- Escoja un método existente de DNS dinámico de una lista.  
Haga clic en el menú desplegable y escoja un método existente. Se abrirá una ventana con una lista de los métodos existentes de DNS dinámico. Esta opción del menú está disponible sólo si hay métodos existentes de DNS dinámico.
- Cree un nuevo método de DNS dinámico.  
Haga clic en el menú desplegable y elija crear un nuevo método de DNS dinámico.

Para borrar un método asociado de DNS dinámico de la interfaz, elija **Ninguno** del menú desplegable.

## Enable Multilink PPP (Activar PPP multienlace)

Marque esta casilla de verificación si desea usar el Protocolo de punto a punto multienlace (Multilink Point-to-Point Protocol, MLP) con esta interfaz. MLP puede mejorar el rendimiento de una red con varias conexiones WAN utilizando la funcionalidad de equilibrado de carga, la fragmentación de paquetes, el ancho de banda a petición y otras funciones.

# Conexión: G.SHDSL

Esta ventana permite crear o modificar una conexión [G.SHDSL](#).



### Nota

Si la conexión que usted está configurando usa un controlador de DSL, los campos de Tipo de Equipo y Modo Operativo no aparecerán en el cuadro de diálogo.

## Encapsulación

Seleccione el tipo de encapsulación que se utilizará para este enlace.

- **PPPoE** especifica el protocolo punto a punto sobre la encapsulación de Ethernet.
- **PPPoA** especifica la encapsulación del protocolo punto a punto sobre ATM.
- **Enrutamiento RFC 1483 (AAL5SNAP)** especifica que cada PVC puede contener varios protocolos.
- **Enrutamiento RFC1483 (AAL5MUX)** especifica que cada PVC puede contener un solo tipo de protocolo.

Si está modificando una conexión, la encapsulación se muestra pero no se puede editar. Si necesita cambiar el tipo de encapsulación, elimine la conexión y vuelva a crearla con el tipo de encapsulación necesario.

Para obtener más información acerca de los tipos de encapsulación, haga clic [Encapsulación](#).



## Identificador de la ruta virtual

El identificador de ruta virtual (VPI) se utiliza en la conmutación y el enrutamiento ATM para identificar la ruta que se utiliza para una variedad de conexiones. Este valor se obtiene del proveedor de servicios.

Si está modificando una conexión existente, este campo aparece desactivado. Si necesita cambiar este valor, elimine la conexión y vuelva a crearla con el valor necesario.

## Identificador de circuito virtual

El Identificador de Circuito Virtual (VCI, Virtual Circuit Identifier) se usa en la conmutación y enrutamiento de ATM para identificar una conexión en particular dentro de una ruta que su conexión pueda compartir con otras conexiones. Este valor se obtiene del proveedor de servicios.

Si está modificando una conexión existente, este campo aparece desactivado. Si necesita cambiar este valor, elimine la conexión y vuelva a crearla con el valor necesario.

## Dirección IP

Seleccione cómo el router obtendrá una dirección IP para este enlace. Los campos que aparecen en esta área cambian en función del tipo de encapsulación seleccionado. El proveedor de servicios o administrador de redes deben proporcionar el método que debe utilizar el router para obtener una dirección IP.

### Dirección IP estática

Si selecciona **Dirección IP estática**, introduzca la dirección que utilizará la interfaz y la máscara de subred o los bits de la red. Esta información se obtiene del proveedor de servicios o del administrador de redes. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

**Dirección IP dinámica**

Si selecciona esta opción, la interfaz obtendrá una dirección IP de un servidor DHCP de la red. Si el servidor DHCP utiliza la opción DHCP 12, éste envía un nombre de host para el router, junto con la dirección IP que debe utilizar. Para determinar el nombre de host enviado, consulte con el proveedor de servicios o administrador de redes.

**IP no numerado**

Seleccione esta opción si desea que la interfaz comparta una dirección IP con una interfaz Ethernet en el router. Si la selecciona, en la lista desplegable debe especificar la interfaz Ethernet cuya dirección desee utilizar.

**Dirección IP de la conexión remota en la oficina central**

Especifique la **Dirección IP** del sistema de gateway al que se conectará este enlace. Esta dirección IP la proporciona el proveedor de servicios o el administrador de redes. El gateway es el sistema al que el router debe conectarse para obtener acceso a Internet o a la WAN de la organización.

**Tipo de equipamiento**

Seleccione uno de los valores siguientes:

**CPE**

Equipo del sitio del cliente. Si el tipo de encapsulación es PPPoE, CPE se selecciona automáticamente y el campo aparece desactivado.

**CO**

Oficina central.

**Modo operativo**

Seleccione uno de los valores siguientes:

**Anexo A (señalización EUA)**

Permite configurar los parámetros operativos regionales para América del Norte.

**Anexo B (señalización Europa)**

Permite configurar los parámetros operativos regionales para Europa.

## Enable Multilink PPP (Activar PPP multienlace)

Marque esta casilla de verificación si desea usar el Protocolo de punto a punto multienlace (Multilink Point-to-Point Protocol, MLP) con esta interfaz. MLP puede mejorar el rendimiento de una red con varias conexiones WAN utilizando la funcionalidad de equilibrado de carga, la fragmentación de paquetes, el ancho de banda a petición y otras funciones.

## Autenticación

Haga clic en este botón si necesita especificar información de autenticación [CHAP](#) o [PAP](#).

## DNS dinámico

Active el DNS dinámico si desea actualizar los servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN.



### Nota

---

Esta función sólo aparece si es admitida por la versión de Cisco IOS en su router.

---

Para escoger un método de DNS dinámico a usar, haga algo de lo siguiente:

- Introduzca el nombre de un método existente de DNS dinámico.  
Introduzca el nombre en el campo de Método DNS dinámico exactamente como aparece en la lista en **Configurar > Tareas adicionales > Métodos de DNS dinámico**.
- Escoja un método existente de DNS dinámico de una lista.  
Haga clic en el menú desplegable y escoja un método existente. Se abrirá una ventana con una lista de los métodos existentes de DNS dinámico. Esta opción del menú está disponible sólo si hay métodos existentes de DNS dinámico.
- Cree un nuevo método de DNS dinámico.  
Haga clic en el menú desplegable y elija crear un nuevo método de DNS dinámico.

Para borrar un método asociado de DNS dinámico de la interfaz, elija **Ninguno** del menú desplegable.

# Configurar controlador DSL

Cisco SDM admite la configuración del WIC-1SHDSL-V2 de Cisco. Este WIC admite una conexión TI, E1 o G.SHDSL sobre una interfaz ATM. Cisco SDM sólo admite una conexión G.SHDSL a través de una interfaz ATM. Esta ventana permite establecer en ATM el modo de controlador en el WIC, lo que activa la conexión. También permite crear o modificar la información acerca del controlador DSL para la conexión G.SHDSL.

## Modo de controlador

Cisco SDM admite solamente el modo ATM, lo que proporciona servicio para una conexión G.SHDSL, en este controlador. Al hacer clic en el botón Aceptar, este campo se establecerá automáticamente en el modo ATM.

## Tipo de equipamiento

Seleccione si la conexión termina en la oficina central (CO) o en el equipo del sitio del cliente (CPE).

## Modo operativo

Seleccione si la conexión DSL debe utilizar la señalización Anexo A (para las conexiones DSL en EE.UU.) o Anexo B (para conexiones DSL en Europa).

## Modo de línea

Seleccione si se trata de una conexión G.SHDSL de 2 ó 4 cables.

## Número de línea

Seleccione el número de interfaz en el que se realizará la conexión.

## Tasa de línea

Seleccione la velocidad de línea DSL para el puerto G.SHDSL. Si ha seleccionado una conexión de 2 cables, puede seleccionar **auto** (autom.), con lo que se configura la interfaz para que realice automáticamente la negociación de la velocidad de línea entre el puerto G.SHDSL y el DSLAM, o la velocidad de línea DSL real. Las velocidades de línea admitidas son 200, 264, 392, 520, 776, 1032, 1160, 1544, 2056 y 2312.

Si ha seleccionado una conexión de 4 cables, debe seleccionar una velocidad de línea fija. Las velocidades de línea admitidas para una conexión de 4 cables son 384, 512, 640, 768, 896, 1024, 1152, 1280, 1408, 1664, 1792, 1920, 2048, 2176, 2304, 2432, 2688, 2816, 2944, 3072, 3200, 3328, 3456, 3584, 3712, 3840, 3968, 4096, 4224, 4352, 4480 y 4608.



### Nota

Si se configuran velocidades de línea DSL diferentes en los extremos opuestos del enlace ascendente DSL, la velocidad de línea real siempre es la velocidad más baja.

## Activar margen del índice de sonido a ruido

La relación señal-ruido proporciona un umbral para el módem DSL con el fin de determinar si debe reducir o aumentar la salida de potencia en función de la cantidad de ruido en la conexión. Si ha establecido la velocidad de línea en “auto” (autom.), puede activar esta función para maximizar la calidad de la conexión DSL. Tenga en cuenta que esta función no puede utilizarse si la velocidad de línea es fija. Para activar La relación señal-ruido, marque esta casilla de verificación y seleccione los márgenes de índice en los campos Vigente y Snext. Para desactivarla, desmarque la casilla.

### Vigente

Seleccione el margen de la relación señal-ruido en decibelios para la conexión vigente. Cuanto más bajo sea el índice, mayor será el ruido que se tolerará en la conexión. Una configuración inferior de decibelios hará que el módem DSL permita una mayor cantidad de ruido en la línea, lo que posiblemente resultará en una conexión de menor calidad pero con un mayor rendimiento. Una configuración superior de decibelios hará que el módem restrinja el ruido, lo que posiblemente resultará en una conexión de mayor calidad pero con un rendimiento inferior.

### Snext

Seleccione el margen de la relación señal-ruido de autoparadiafonía (Snext) en la forma de decibelios.

## Conexiones DSL

Este campo muestra todas las conexiones G.SHDSL configuradas actualmente en este controlador. Para configurar una nueva conexión G.SHDSL, haga clic en **Agregar**. Aparecerá la página [Agregar una conexión G.SHDSL](#) en la que podrá configurar la nueva conexión. Para editar una conexión G.SHDSL existente, seleccione la conexión en este campo y haga clic en **Editar**. Aparecerá también la página [Agregar una conexión G.SHDSL](#) en la que podrá editar la configuración de la conexión. Para eliminar una conexión, selecciónela en este campo y haga clic en **Eliminar**.

# Agregar una conexión G.SHDSL

Esta ventana permite crear o modificar una conexión [G.SHDSL](#).

## Encapsulación

Seleccione el tipo de encapsulación que se utilizará para este enlace.

- **PPPoE** especifica el protocolo punto a punto sobre la encapsulación de Ethernet.
- **PPPoA** especifica la encapsulación del protocolo punto a punto sobre ATM.
- **Enrutamiento RFC 1483 (AAL5SNAP)** especifica que cada PVC puede contener varios protocolos.
- **Enrutamiento RFC1483 (AAL5MUX)** especifica que cada PVC contendrá un solo tipo de protocolo.

Si está modificando una conexión, la encapsulación se muestra pero no se puede editar. Si necesita cambiar el tipo de encapsulación, elimine la conexión y vuelva a crearla con el tipo de encapsulación necesario.

## Identificador de la ruta virtual

El identificador de ruta virtual (VPI) se utiliza en la conmutación y el enrutamiento ATM para identificar la ruta que se utiliza para una variedad de conexiones. Este valor se obtiene del proveedor de servicios.

Si está modificando una conexión existente, este campo aparece desactivado. Si necesita cambiar este valor, elimine la conexión y vuelva a crearla con el valor necesario.

## Identificador de circuito virtual

El identificador de circuito virtual (VCI) se utiliza en la conmutación y el enrutamiento ATM para identificar una conexión específica dentro de una ruta que posiblemente comparte con otras conexiones. Este valor se obtiene del proveedor de servicios.

Si está modificando una conexión existente, este campo aparece desactivado. Si necesita cambiar este valor, elimine la conexión y vuelva a crearla con el valor necesario.

## Dirección IP

Seleccione cómo el router obtendrá una dirección IP para este enlace. Los campos que aparecen en esta área cambian en función del tipo de encapsulación seleccionado. El proveedor de servicios o administrador de redes debe proporcionar el método que debe utilizar el router para obtener una dirección IP.

### Dirección IP estática

Si selecciona esta opción, especifique la dirección que utilizará la interfaz y la máscara de subred o bits de red. Esta información se obtiene del proveedor de servicios o del administrador de redes. Si desea obtener más información, consulte [Direcciones IP y máscaras de subred](#).

### Dirección IP dinámica

Si selecciona esta opción, la interfaz obtendrá una dirección IP de un servidor DHCP de la red. Si el servidor DHCP utiliza la opción DHCP 12, éste envía un nombre de host para el router, junto con la dirección IP que debe utilizar. Para determinar el nombre de host enviado, consulte con el proveedor de servicios o administrador de redes.

### IP no numerado

Seleccione esta opción si desea que la interfaz comparta una dirección IP con una interfaz Ethernet en el router. Si la selecciona, en la lista desplegable debe especificar la interfaz Ethernet cuya dirección desee utilizar.

## Descripción

Introduzca una descripción de esta conexión que sea fácil de reconocer y administrar.

## Enable Multilink PPP (Activar PPP multienlace)

Marque esta casilla de verificación si desea usar el Protocolo punto a punto multienlace (Multilink Point-to-Point Protocol, MLP) con esta interfaz. MLP puede mejorar el rendimiento de una red con varias conexiones WAN utilizando la funcionalidad de equilibrado de carga, la fragmentación de paquetes, el ancho de banda a petición y otras funciones.

## Autenticación

Haga clic en este botón si necesita especificar información de autenticación [CHAP](#) o [PAP](#).

## DNS dinámico

Active el DNS dinámico si desea actualizar los servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN.



### Nota

---

Esta función sólo aparecerá si se admite por la edición de IOS de su servidor de Cisco.

---

Para escoger un método de DNS dinámico a usar, haga algo de lo siguiente:

- Introduzca el nombre de un método existente de DNS dinámico.  
Introduzca el nombre en el campo de **Método DNS dinámico** exactamente como aparece en la lista en Configurar > Tareas adicionales > Métodos de DNS dinámico.
- Escoja un método existente de DNS dinámico de una lista.  
Haga clic en el menú desplegable y escoja un método existente para usar. Se abrirá una ventana con una lista de los métodos existentes de DNS dinámico. Esta opción del menú está disponible sólo si hay métodos existentes de DNS dinámico.
- Cree un nuevo método de DNS dinámico.  
Haga clic en el menú desplegable y elija crear un nuevo método de DNS dinámico.

Para borrar un método asociado de DNS dinámico de la interfaz, elija **Ninguno** del menú desplegable.



# Conexión: Interfaz de serie, encapsulación Frame Relay

Si está configurando una subinterfaz de serie para la encapsulación [Frame Relay](#), complete estos campos. Si va a editar una conexión o a crear una en la ventana Editar interfaz/conexión, se mostrará la encapsulación pero no se podrá editar. Si necesita cambiar el tipo de encapsulación, elimine la conexión y vuelva a crearla con el tipo de encapsulación necesario.

## Encapsulación

[Frame Relay](#) seleccionado.

## Dirección IP

Seleccione **Dirección IP estática** o **IP no numerado**.

### Dirección IP

Si ha seleccionado **Dirección IP estática**, especifique la [Dirección IP](#) para esta interfaz. Este valor se obtiene del proveedor de servicios o del administrador de redes. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

### Máscara de subred

Si ha seleccionado **Dirección IP estática**, especifique la [máscara de subred](#). La máscara de subred indica la parte de la dirección IP que proporciona la dirección de red. Este valor se sincroniza con los bits de la subred. El administrador de red o proveedor de servicios proporcionan el valor de la máscara de subred o los bits de red.

### Bits de subred

Como alternativa, especifique los [bits de red](#) para indicar qué porción de la dirección IP corresponde a la dirección de red.

### IP no numerado

Si selecciona IP no numerado, la interfaz compartirá una dirección IP que ya ha sido asignada a otra interfaz. Escoja la interfaz cuya dirección IP de esta interfaz es para compartir.

## DLCI

Especifique un identificador de conexión de enlace de datos (DLCI) en este campo. Este número debe ser exclusivo entre todos los DLCI que se utilizan en esta interfaz. El DLCI proporciona un identificador Frame Relay exclusivo para esta conexión.

Si está modificando una conexión existente, el campo DLCI aparece desactivado. Si desea cambiar el DLCI, elimine la conexión y vuelva a crearla.

## Tipo de LMI

Consulte con el proveedor de servicios para saber cuáles de los siguientes tipos de interfaz de gestión local (LMI) debe utilizar. El tipo de LMI especifica el protocolo que se utiliza para supervisar la conexión:

### ANSI

Anexo D definido por la norma T1.617 del American National Standards Institute (ANSI).

### Cisco

Tipo de LMI definido conjuntamente por Cisco y otras tres empresas.

### ITU-T Q.933

ITU-T Q.933 Anexo A.

### Detección automática

Por defecto. Esta configuración permite que el router detecte qué tipo de LMI usa el switch y luego usa ese tipo. Si autodetección falla, el router usará el tipo de LMI de Cisco.

## Utilice la encapsulación Frame Relay IETF

Marque esta casilla de verificación para utilizar la encapsulación [IETF](#) (Internet Engineering Task Force). Esta opción se usa para conectarse con routers que no sean de Cisco. Marque esta casilla si se está tratando de conectar a un router que no sea de Cisco en esta interfaz.

## Configuración del reloj

En la mayoría de los casos, no debe cambiarse la configuración por defecto del reloj. Si usted sabe que sus requisitos son diferentes de los valores por defecto, haga clic en este botón y ajuste la configuración del reloj en la ventana mostrada.

El botón de Configuraciones del Reloj sólo aparece si usted está configurando una conexión de serie T1 ó E1.

## DNS dinámico

Active el DNS dinámico si desea actualizar los servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN.



### Nota

---

Esta función sólo aparece si es admitida por la versión de Cisco IOS en su router.

---

Para escoger un método de DNS dinámico a usar, haga algo de lo siguiente:

- Introduzca el nombre de un método existente de DNS dinámico.  
Introduzca el nombre en el campo de Método DNS dinámico exactamente como aparece en la lista en **Configurar > Tareas adicionales > Métodos de DNS dinámico**.
- Escoja un método existente de DNS dinámico de una lista.  
Haga clic en el menú desplegable y escoja un método existente. Se abrirá una ventana con una lista de los métodos existentes de DNS dinámico. Esta opción del menú está disponible sólo si hay métodos existentes de DNS dinámico.
- Cree un nuevo método de DNS dinámico.  
Haga clic en el menú desplegable y elija crear un nuevo método de DNS dinámico.

Para borrar un método asociado de DNS dinámico de la interfaz, elija **Ninguno** del menú desplegable.

# Conexión: Interfaz de serie, encapsulación PPP

Si está configurando una interfaz de serie para la encapsulación de protocolo de punto a punto (PPP), rellene estos campos. Si va a editar una conexión o a crear una en la ventana Editar interfaz/conexión, se mostrará la encapsulación pero no se podrá editar. Si necesita cambiar el tipo de encapsulación, elimine la conexión y vuelva a crearla con el tipo de encapsulación necesario.

## Encapsulación

PPP seleccionado.

## Dirección IP

Seleccione **Dirección IP estática**, **IP no numerado** o **IP negociado**. Si usted elige **IP no numerado**, escoja la interfaz cuya dirección IP de esta interfaz es para compartir. Si usted elige **IP negociado**, el router obtendrá una dirección IP del proveedor de servicios de Internet para esta interfaz. Si selecciona **Especificar una dirección IP**, rellene los campos a continuación.

### Dirección IP

Especifique la [Dirección IP](#) para esta subinterfaz de punto a punto. Este valor se obtiene del proveedor de servicios o del administrador de redes. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

### Máscara de subred

Especifique la [máscara de subred](#). La máscara de subred indica la parte de la dirección IP que proporciona la dirección de red. Este valor se sincroniza con los bits de la red. Obtenga el valor de la máscara de subred o los bits de red del administrador de red o proveedor de servicios.

### Bits de subred

Como alternativa, especifique los [bits de red](#) para indicar los bits de la dirección IP que proporcionan la dirección de red.

## Autenticación

Haga clic en este botón si necesita especificar información de autenticación [CHAP](#) o [PAP](#).

## Configuración del reloj

En la mayoría de los casos, las configuraciones del reloj no deben cambiarse de los valores por defecto. Si usted sabe que sus requisitos son diferentes de los valores por defecto, haga clic en este botón y ajuste la configuración del reloj en la ventana mostrada.

El botón de Configuraciones del Reloj sólo aparece si usted está configurando una conexión de serie T1 ó E1.

## DNS dinámico

Active el DNS dinámico si desea actualizar los servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN.



### Nota

---

Esta función sólo aparece si es admitida por la versión de Cisco IOS en su router.

---

Para escoger un método de DNS dinámico a usar, haga algo de lo siguiente:

- Introduzca el nombre de un método existente de DNS dinámico.  
Introduzca el nombre en el campo de Método DNS dinámico exactamente como aparece en la lista en **Configurar > Tareas adicionales > Métodos de DNS dinámico**.
- Escoja un método existente de DNS dinámico de una lista.  
Haga clic en el menú desplegable y escoja un método existente. Se abrirá una ventana con una lista de los métodos existentes de DNS dinámico. Esta opción del menú está disponible sólo si hay métodos existentes de DNS dinámico.
- Cree un nuevo método de DNS dinámico.  
Haga clic en el menú desplegable y elija crear un nuevo método de DNS dinámico.

Para borrar un método asociado de DNS dinámico de la interfaz, elija **Ninguno** del menú desplegable.

# Conexión: Interfaz de serie, encapsulación HDLC

Si está configurando una interfaz de serie para la encapsulación [HDLC](#), rellene estos campos. Si va a editar una conexión o a crear una en la ventana Editar interfaz/conexión, se mostrará la encapsulación pero no se podrá editar. Si necesita cambiar el tipo de encapsulación, elimine la conexión y vuelva a crearla con el tipo de encapsulación necesario.

## Encapsulación

HDLC seleccionado.

## Dirección IP

Seleccione **Dirección IP estática** o **IP no numerado**. Si usted elige **IP no numerado**, escoja la interfaz cuya dirección IP de esta interfaz es para compartir. Si selecciona **Dirección IP estática**, rellene los campos a continuación.

### Dirección IP

Especifique la [Dirección IP](#) de esta interfaz. Este valor se obtiene del proveedor de servicios o del administrador de redes. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

### Máscara de subred

Especifique la [máscara de subred](#). La máscara de subred indica la parte de la dirección IP que proporciona la dirección de red. Este valor se sincroniza con los bits de la red. Obtenga el valor de la máscara de subred o los bits de red del administrador de red o proveedor de servicios.

### Bits de subred

Como alternativa, seleccione los bits que indican qué porción de la dirección IP proporciona la dirección de red.

## Configuración del reloj

En la mayoría de los casos, no debe cambiarse la configuración por defecto del reloj. Si usted sabe que sus requisitos son diferentes de los valores por defecto, haga clic en este botón y ajuste la configuración del reloj en la ventana mostrada.

El botón de Configuraciones del Reloj sólo aparece si usted está configurando una conexión de serie T1 ó E1.

## DNS dinámico

Active el DNS dinámico si desea actualizar los servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN.



### Nota

Esta función sólo aparece si es admitida por la versión de Cisco IOS en su router.

Para escoger un método de DNS dinámico a usar, haga algo de lo siguiente:

- Introduzca el nombre de un método existente de DNS dinámico.  
Introduzca el nombre en el campo de Método DNS dinámico exactamente como aparece en la lista en **Configurar > Tareas adicionales > Métodos de DNS dinámico**.
- Escoja un método existente de DNS dinámico de una lista.  
Haga clic en el menú desplegable y escoja un método existente. Se abrirá una ventana con una lista de los métodos existentes de DNS dinámico. Esta opción del menú está disponible sólo si hay métodos existentes de DNS dinámico.
- Cree un nuevo método de DNS dinámico.  
Haga clic en el menú desplegable y elija crear un nuevo método de DNS dinámico.

Para borrar un método asociado de DNS dinámico de la interfaz, elija **Ninguno** del menú desplegable.

## Agregar o editar un túnel GRE

Esta ventana permite agregar un túnel **GRE** a una interfaz o editar una interfaz existente. Si el túnel GRE no se ha configurado mediante el modo **gre ip**, la ventana no aparecerá.

### Tunnel Number (Número de túnel)

Especifique un número para este túnel.

## Origen del túnel

Seleccione la interfaz que utilizará el túnel, la cual debe ser alcanzable desde el otro extremo del túnel y, por lo tanto, debe disponer de una [Dirección IP](#) pública que se pueda enrutar.

## Destino del túnel

El destino del túnel es la interfaz del router en el otro extremo del túnel. Seleccione si se desea especificar una dirección IP o nombre de host y, a continuación, indique dicha información. Si ha seleccionado Dirección IP, proporciónela junto con la máscara de subred en formato decimal con puntos, por ejemplo 192.168.20.1 y 255.255.255.0.

Utilice el comando **ping** para comprobar que se pueden alcanzar la dirección y el nombre de host. De lo contrario, el túnel no se creará correctamente.

## Dirección IP del túnel

Especifique la dirección IP del túnel en formato de decimales con puntos, por ejemplo, 192.168.20.1. Si desea obtener más información, consulte el apartado [Direcciones IP y máscaras de subred](#).

## Casilla de verificación GRE Keepalive

Marque esta casilla de verificación si desea que el router envíe paquetes de este tipo. Especifique en segundos el intervalo para el envío de los paquetes “keepalive” y el período de espera entre los reintentos, también en segundos.

## Unidad de transmisión máxima (MTU)

Especifique el tamaño de la unidad de transmisión máxima (MTU). Si desea ajustar el tamaño a un valor inferior para evitar la fragmentación de paquetes, haga clic en **Ajustar MTU para evitar la fragmentación**.

## Ancho de banda

Haga clic para especificar el ancho de banda en kilobytes para este túnel.



# Conexión: ISDN (RDSI) BRI

Si está configurando una conexión ISDN (RDSI) BRI, complete estos campos. Dado que Cisco SDM sólo admite la encapsulación PPP sobre una conexión ISDN (RDSI) BRI, la encapsulación que aparece no se puede editar.

## Encapsulación

PPP seleccionado.

## Tipo de switch ISDN (RDSI)

Seleccione el tipo de switch ISDN (RDSI). Para obtener el tipo de switch de la conexión, póngase en contacto con el proveedor de servicios ISDN (RDSI).

Cisco SDM admite los tipos de switch BRI siguientes:

- Para América del Norte:
  - basic-5ess: switch 5ESS de velocidad básica de Lucent (AT&T)
  - basic-dms100: switch de velocidad básica DMS-100 de Northern Telecom
  - basic-ni: switches ISDN (RDSI) de National
- Para Australia, Europa y Reino Unido:
  - basic-1tr6: switch ISDN (RDSI) 1TR6 para Alemania
  - basic-net3: NET3 ISDN (RDSI) BRI para los tipos de switch de Noruega NET3, Australia NET3 y Nueva Zelanda NET3; tipos de switch conformes con ETSI para el sistema de señalización Euro-ISDN E-DSS1
  - vn3: switches ISDN (RDSI) BRI para Francia
- Para Japón:
  - ntt: switches ISDN (RDSI) NTT para Japón
- Para los sistemas de voz/PBX:
  - basic-qsig: switches PINX (PBX) con señalización QSIG según Q.931 ()

## SPIDS

Haga clic en este botón cuando necesite especificar la información del ID del perfil de servicio (SPID).

Algunos proveedores de servicios utilizan los SPID para definir los servicios abonados por el dispositivo ISDN (RDSI) que accede al proveedor de servicios ISDN (RDSI). El proveedor de servicios asigna al dispositivo ISDN (RDSI) uno o varios SPID cuando el usuario se suscribe al servicio. Si utiliza un proveedor de servicios que requiere SPID, el dispositivo ISDN (RDSI) no podrá realizar ni recibir llamadas hasta que envíe al proveedor de servicios un SPID válido y asignado en el momento de acceder al switch para inicializar la conexión.

Sólo los tipos de switch DMS-100 y NI requieren SPID. El tipo de switch Lucent (AT&T) 5ESS admite un SPID, pero se recomienda que establezca dicho servicio ISDN (RDSI) sin SPID. Además, los SPID sólo tienen significado en la interfaz ISDN (RDSI) de acceso local. Los routers remotos nunca reciben elb/bSPID.

Normalmente, un SPID es un número de teléfono de siete dígitos con algunos números opcionales. No obstante, es posible que los proveedores de servicios utilicen esquemas de numeración diferentes. Para el tipo de switch DMS-100, se asignan dos SPID; uno para cada canal B.

## Número de teléfono remoto

Especifique el número de teléfono del destino de la conexión ISDN (RDSI).

## Opciones

Haga clic en este botón cuando necesite asociar listas de control de acceso con una lista de marcación para identificar tráfico interesante, especificar la configuración del temporizador o activar o desactivar el PPP multienlace.

Al identificar el tráfico interesante, el router realizará una marcación externa y creará una conexión activa solamente cuando detecte este tipo de tráfico.

La configuración del temporizador permite que el router desconecte automáticamente una llamada cuando la línea se encuentre sin actividad durante la cantidad de tiempo especificada.

El PPP multienlace puede configurarse para proporcionar un balance de carga entre los canales B ISDN (RDSI).

## Dirección IP

Seleccione **Dirección IP estática**, **IP no numerado** o **IP negociado**. Si selecciona **Especificar una dirección IP**, rellene los campos a continuación.

### Dirección IP

Especifique la **Dirección IP** para esta subinterfaz de punto a punto. Este valor se obtiene del proveedor de servicios o del administrador de redes. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

### Máscara de subred

Especifique la **máscara de subred**. La máscara de subred indica la parte de la dirección IP que proporciona la dirección de red. Este valor se sincroniza con los bits de la red. Obtenga el valor de la máscara de subred o los bits de red del administrador de red o proveedor de servicios.

### Bits de subred

Como alternativa, especifique los **bits de red** para indicar los bits de la dirección IP que proporcionan la dirección de red.

## Autenticación

Haga clic en este botón si necesita especificar información de autenticación **CHAP** o **PAP**.

## DNS dinámico

Active el DNS dinámico si desea actualizar los servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN.



### Nota

---

Esta función sólo aparece si es admitida por la versión de Cisco IOS en su router.

---

Para escoger un método de DNS dinámico a usar, haga algo de lo siguiente:

- Introduzca el nombre de un método existente de DNS dinámico.  
Introduzca el nombre en el campo de Método DNS dinámico exactamente como aparece en la lista en **Configurar > Tareas adicionales > Métodos de DNS dinámico**.

- Escoja un método existente de DNS dinámico de una lista.  
Haga clic en el menú desplegable y escoja un método existente. Se abrirá una ventana con una lista de los métodos existentes de DNS dinámico. Esta opción del menú está disponible sólo si hay métodos existentes de DNS dinámico.
- Cree un nuevo método de DNS dinámico.  
Haga clic en el menú desplegable y elija crear un nuevo método de DNS dinámico.

Para borrar un método asociado de DNS dinámico de la interfaz, elija **Ninguno** del menú desplegable.

## Conexión: Módem analógico

Si está configurando una conexión de módem analógico, rellene estos campos. Dado que Cisco SDM sólo admite la encapsulación PPP sobre una conexión de módem analógico, la encapsulación que aparece no se puede editar.

### Encapsulación

PPP seleccionado.

### Número de teléfono remoto

Especifique el número de teléfono de la conexión de módem analógico de destino.

### Opciones

Haga clic en este botón cuando necesite asociar listas de control de acceso con una lista de marcación para identificar tráfico interesante o especificar la configuración del temporizador.

Al identificar el tráfico interesante, el router realizará una marcación externa y creará una conexión activa solamente cuando detecte este tipo de tráfico.

La configuración del temporizador permite que el router desconecte automáticamente una llamada cuando la línea se encuentre sin actividad durante la cantidad de tiempo especificada.

## Borrar línea

Haga clic en este botón para borrar la línea. Esta operación deberá llevarse a cabo tras la creación de una conexión asíncrona para que el tráfico interesante active la conexión.

## Dirección IP

Seleccione **Dirección IP estática**, **IP no numerado** o **IP negociado**. Si selecciona **Especificar una dirección IP**, rellene los campos a continuación.

### Dirección IP

Especifique la [Dirección IP](#) para esta subinterfaz de punto a punto. Este valor se obtiene del proveedor de servicios o del administrador de redes. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

### Máscara de subred

Especifique la [máscara de subred](#). La máscara de subred indica la parte de la dirección IP que proporciona la dirección de red. Este valor se sincroniza con los bits de la red. Obtenga el valor de la máscara de subred o los bits de red del administrador de red o proveedor de servicios.

### Bits de subred

Como alternativa, especifique los [bits de red](#) para indicar los bits de la dirección IP que proporcionan la dirección de red.

## Autenticación

Haga clic en este botón si necesita especificar información de autenticación [CHAP](#) o [PAP](#).

## DNS dinámico

Active el DNS dinámico si desea actualizar los servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN.



### Nota

---

Esta función sólo aparece si es admitida por la versión de Cisco IOS en su router.

---

Para escoger un método de DNS dinámico a usar, haga algo de lo siguiente:

- Introduzca el nombre de un método existente de DNS dinámico.  
Introduzca el nombre en el campo de Método DNS dinámico exactamente como aparece en la lista en **Configurar > Tareas adicionales > Métodos de DNS dinámico**.
- Escoja un método existente de DNS dinámico de una lista.  
Haga clic en el menú desplegable y escoja un método existente. Se abrirá una ventana con una lista de los métodos existentes de DNS dinámico. Esta opción del menú está disponible sólo si hay métodos existentes de DNS dinámico.
- Cree un nuevo método de DNS dinámico.  
Haga clic en el menú desplegable y elija crear un nuevo método de DNS dinámico.

Para borrar un método asociado de DNS dinámico de la interfaz, elija **Ninguno** del menú desplegable.

## Conexión: (Reserva AUX.)

Rellene estos campos si está configurando una conexión de acceso telefónico asíncrona mediante el puerto de consola para que funcione también como un puerto auxiliar en un router Cisco 831 ó 837. Cuando introduzca la información en esta ventana, haga clic en **Detalles de la copia de seguridad** y proporcione la información de conexión de acceso telefónico de reserva que se requiere para este tipo de conexión. Tenga en cuenta que dado que Cisco SDM sólo admite la encapsulación PPP sobre una conexión de módem analógico, la encapsulación que aparece no se puede editar.

La opción para configurar el puerto auxiliar como una conexión de acceso telefónico sólo se mostrará para los routers Cisco 831 y 837. Esta opción no estará disponible para dichos routers cuando se presente cualquiera de las condiciones siguientes:

- Cuando el router no utiliza una versión de Cisco IOS Zutswang
- La interfaz WAN primaria no está configurada.
- La interfaz asíncrona ya está configurada.
- La interfaz asíncrona no es configurable por Cisco SDM debido a la presencia de comandos de Cisco IOS no admitidos en la configuración existente.

## Encapsulación

[PPP](#) seleccionado.

## Número de teléfono remoto

Especifique el número de teléfono de la conexión de módem analógico de destino.

## Opciones

Haga clic en este botón cuando necesite asociar listas de control de acceso con una lista de marcación para identificar tráfico interesante o especificar la configuración del temporizador.

Al identificar el tráfico interesante, el router realizará una marcación externa y creará una conexión activa solamente cuando detecte este tipo de tráfico.

La configuración del temporizador permite que el router desconecte automáticamente una llamada cuando la línea se encuentre sin actividad durante la cantidad de tiempo especificada.

## Borrar línea

Haga clic en este botón para borrar la línea. Esta operación deberá llevarse a cabo tras la creación de una conexión asíncrona para que el tráfico interesante active la conexión.

## Dirección IP

Seleccione **Dirección IP estática**, **IP no numerado** o **IP negociado**. Si selecciona **Especifique una dirección IP**, rellene los campos a continuación.

### Dirección IP

Especifique la [Dirección IP](#) para esta subinterfaz de punto a punto. Este valor se obtiene del proveedor de servicios o del administrador de redes. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

### Máscara de subred

Especifique la [máscara de subred](#). La máscara de subred indica la parte de la dirección IP que proporciona la dirección de red. Este valor se sincroniza con los bits de la red. Obtenga el valor de la máscara de subred o los bits de red del administrador de red o proveedor de servicios.

**Bits de subred**

Como alternativa, especifique los [bits de red](#) para indicar los bits de la dirección IP que proporcionan la dirección de red.

**Detalles de la conexión de reserva**

Al hacer clic en este botón, aparecerá la ventana [Configuración de la copia de seguridad](#), la cual permite configurar la información de conexión de acceso telefónico de reserva para esta conexión. Estos datos son obligatorios para este tipo de conexión e incluso aparecerá un error si intenta finalizar la configuración de la conexión sin especificarlos.

**Autenticación**

Haga clic en este botón si necesita especificar información de autenticación [CHAP](#) o [PAP](#).

**DNS dinámico**

Active el DNS dinámico si desea actualizar los servidores de DNS automáticamente siempre que cambie la dirección IP de la interfaz WAN.

**Nota**


---

Esta función sólo aparece si es admitida por la versión de Cisco IOS en su router.

---

Para escoger un método de DNS dinámico a usar, haga algo de lo siguiente:

- Introduzca el nombre de un método existente de DNS dinámico.  
Introduzca el nombre en el campo de Método DNS dinámico exactamente como aparece en la lista en **Configurar > Tareas adicionales > Métodos de DNS dinámico**.
- Escoja un método existente de DNS dinámico de una lista.  
Haga clic en el menú desplegable y escoja un método existente. Se abrirá una ventana con una lista de los métodos existentes de DNS dinámico. Esta opción del menú está disponible sólo si hay métodos existentes de DNS dinámico.
- Cree un nuevo método de DNS dinámico.  
Haga clic en el menú desplegable y elija crear un nuevo método de DNS dinámico.

Para borrar un método asociado de DNS dinámico de la interfaz, elija **Ninguno** del menú desplegable.



# Autenticación

Esta página aparece si ha activado **PPP** para una conexión serie o encapsulación **PPPoE** para una conexión ATM o Ethernet, o bien, si está configurando una conexión ISDN (RDSI) BRI o de módem analógico. Es posible que el proveedor de servicios o administrador de redes utilice una contraseña **CHAP** (Protocolo de autenticación por desafío mutuo) o **PAP** (Protocolo de autenticación de contraseña) para garantizar la seguridad de la conexión entre dos dispositivos. Esta contraseña garantiza la seguridad para el acceso entrante y saliente.

## CHAP/PAP

Marque la casilla que corresponda al tipo de autenticación que utiliza el proveedor de servicios. Si desconoce el tipo que utiliza, puede marcar ambas casillas: el router intentará ambos tipos de autenticación (uno de ellos funcionará).

La autenticación CHAP es más segura que la autenticación PAP.

## Nombre de Inicio de Sesión

El nombre de inicio de sesión que le proporciona el proveedor de servicios y que se utiliza como nombre de usuario para la autenticación CHAP/PAP.

## Contraseña

Especifique la contraseña exactamente tal como se la ha proporcionado por el proveedor de servicios. Las contraseñas distinguen entre mayúsculas y minúsculas. Por ejemplo, la contraseña *test* no es lo mismo que *TEST*.

## Volver a especificar la nueva contraseña

Vuelva a especificar la misma contraseña que ha especificado en el cuadro anterior.

# Información de SPID

Algunos proveedores de servicios utilizan los números de identificación del proveedor de servicios (SPID) para definir los servicios suscritos por el dispositivo ISDN (RDSI) que accede al proveedor de servicios ISDN (RDSI). El proveedor de servicios asigna al dispositivo ISDN (RDSI) uno o varios SPID cuando el usuario se suscribe al servicio. Si utiliza un proveedor de servicios que requiere SPID, el dispositivo ISDN (RDSI) no podrá realizar ni recibir llamadas hasta que envíe al proveedor de servicios un SPID válido y asignado en el momento de acceder al switch para inicializar la conexión.

Sólo los tipos de switch DMS-100 y NI requieren SPID. El tipo de switch AT&T 5ESS admite un SPID, y se recomienda que establezca dicho servicio ISDN (RDSI) sin SPID. Además, los SPID sólo tienen significado en la interfaz ISDN (RDSI) de acceso local. Los routers remotos nunca reciben elb/bSPID.

Normalmente, un SPID es un número de teléfono de siete dígitos con algunos números opcionales. No obstante, es posible que los proveedores de servicios utilicen esquemas de numeración diferentes. Para el tipo de switch DMS-100, se asignan dos SPID; uno para cada canal B.

## SPID1

Especifique el SPID para el primer canal B BRI que le proporciona el ISP.

## SPID2

Especifique el SPID para el segundo canal B BRI que le proporciona el ISP.

# Opciones de marcación

Tanto las interfaces ISDN (RDSI) BRI como las de módem analógico pueden configurarse para el enrutamiento de marcación bajo demanda (DDR), que hace que la conexión realice una marcación externa o se active solamente bajo condiciones específicas, lo que ahorra tiempo y costos de conexión. Esta ventana permite configurar las opciones que indican cuándo deben iniciarse y finalizarse las conexiones ISDN (RDSI) BRI o de módem analógico.

## Asociación de la lista de marcaciones

La lista de marcaciones permite asociar la conexión ISDN (RDSI) BRI o de módem analógico con una lista de control de acceso para identificar el *tráfico interesante*. Al identificar dicho tráfico, la interfaz realizará una marcación externa y establecerá una conexión activa solamente cuando detecte tráfico de datos que coincide con la lista de control de acceso.

### Permitir todo el tráfico IP

Seleccione esta opción para que la interfaz realice una marcación externa y establezca una conexión cada vez que se envíe tráfico IP a través de la interfaz.

### Filtrar el tráfico según la lista de control de acceso seleccionada

Seleccione esta opción para asociar con la interfaz una lista de control de acceso, que deberá crearse mediante la interfaz Reglas. Únicamente el tráfico que coincida con el tráfico identificado en la lista de control de acceso hará que la interfaz realice una marcación externa y establezca una conexión.

Puede especificar el número de lista de control de acceso (ACL) que desea asociar a la interfaz de marcación para identificar el tráfico interesante, o puede hacer clic en el botón junto al campo para examinar la lista de ACL o crear una nueva ACL y seleccionarla.

## Timer Settings (Configuración del temporizador)

La configuración del temporizador permite definir el tiempo máximo que permanecerá activa una conexión sin tráfico. Al definir la configuración del temporizador, las conexiones se cerrarán automáticamente, lo que ahorrará tiempo y costos de conexión.

**Límite de tiempo de inactividad**

Especifique el número de segundos que podrá transcurrir antes de que se cierre una conexión inactiva (conexión en la que no se transmite tráfico).

**Límite de tiempo rápido de inactividad**

El tiempo rápido de inactividad se usa cuando una conexión está activa mientras que una conexión competitiva está esperando a realizarse. El tiempo rápido de inactividad fija el número máximo de segundos sin un tráfico interesante antes de que se termine la conexión activa y se haga la conexión competitiva.

Esto ocurre cuando la interfaz tiene una conexión activa con una dirección IP de próximo salto (next hop) y recibe datos interesantes con un destino de IP de próximo salto (next hop) distinto. Puesto que la conexión de marcación es de punto a punto, el paquete que compite no podrá entregarse hasta que no se cierre la conexión vigente. Este temporizador establece la cantidad de tiempo de inactividad que debe transcurrir para la primera conexión antes de que ésta se cierre y se establezca la conexión competitiva.

**Enable Multilink PPP (Activar PPP multienlace)**

PPP multienlace permite establecer un equilibrado de carga de los datos a través de varios canales B ISDN (RDSI) BRI e interfaces asíncronas. Con PPP multienlace, cuando se establece inicialmente una conexión ISDN (RDSI), se utiliza un solo canal B para la conexión. Si la carga de tráfico en la conexión supera el umbral especificado (porcentaje del ancho de banda total), se establecerá una segunda conexión con el canal B y el tráfico de datos se compartirá entre ambas conexiones. Este proceso presenta la ventaja de reducir el tiempo y los costos de la conexión cuando haya poco tráfico de datos, a la vez que permite utilizar el total del ancho de banda ISDN (RDSI) BRI cuando sea necesario.

Marque esta casilla de verificación cuando desee activar el PPP multienlace. Desmarque si no lo hace.

**Umbral de la carga**

Utilice este campo para configurar el porcentaje de ancho de banda que debe utilizarse en un solo canal ISDN (RDSI) BRI antes de que se establezca otra conexión de canal ISDN (RDSI) BRI para realizar el balance de carga del tráfico. Especifique un número entre 1 y 255, donde 255 equivale al 100% del ancho de banda en la primera conexión que se esté utilizando.

**Data Direction (Dirección de datos)**

Cisco SDM sólo admite PPP multienlace para el tráfico de red saliente.

# Configuración de la copia de seguridad

Las interfaces ISDN (RDSI) BRI y de módem analógico pueden configurarse para que funcionen como interfaces de reserva para otras interfaces principales. En este caso, una conexión ISDN (RDSI) o de módem analógico sólo se establecerá si se produce un error en la interfaz principal. Si se produce un error en la interfaz principal y la conexión, la interfaz ISDN (RDSI) o de módem analógico realizará inmediatamente una marcación externa e intentará establecer una conexión para evitar la pérdida de los servicios de red.

## Activar conexión de reserva

Marque esta casilla de verificación cuando desee que esta interfaz ISDN (RDSI) BRI o de módem analógico funcione como una conexión de reserva. Desmarque esta casilla de verificación cuando no desee que la interfaz ISDN (RDSI) BRI o de módem analógico funcione como una conexión de reserva.

## Interfaz principal

Seleccione la interfaz del router que mantendrá la conexión principal. La conexión ISDN (RDSI) BRI o de módem analógico sólo se establecerá si se produce un error en la conexión de la interfaz seleccionada.

## Detalles del seguimiento

Utilice esta sección para identificar un host específico con el que debe mantenerse la conectividad. El router realizará un seguimiento de la conectividad con dicho host y, si detecta que la interfaz principal perdió la conectividad con el host especificado, se iniciará la conexión de reserva a través de la interfaz ISDN (RDSI) BRI o de módem analógico.

### Nombre de host o dirección IP objeto del seguimiento

Especifique el nombre de host o la dirección IP del host de destino para el que se realizará un seguimiento de la conectividad. Especifique un destino contactado infrecuentemente como el sitio a darle seguimiento.

### Número de objeto de seguimiento

Campo de sólo lectura que muestra un número de objeto interno que Cisco SDM genera y utiliza para el seguimiento de la conectividad con el host remoto.

## Envío de próximo salto (next hop)

Estos campos son opcionales. Puede especificar la dirección IP a la que se conectarán las interfaces principal y de reserva cuando estén activas. Se denomina “dirección IP de próximo salto (next hop)”. Si no especifica direcciones IP de próximo salto, Cisco SDM utilizará el nombre de interfaz para configurar rutas estáticas. Tenga en cuenta que cuando establece una conexión WAN multipunto de reserva, como, por ejemplo, una conexión Ethernet, debe especificar direcciones IP de próximo salto para que el enrutamiento se realice correctamente. Sin embargo, al establecer una conexión punto a punto de reserva, esta información no es necesaria.

### **Dirección IP de próximo salto (next hop) principal**

Especifique la dirección IP de próximo salto (next hop) de la interfaz principal.

### **Dirección IP de próximo salto (next hop) de reserva**

Especifique la dirección IP de próximo salto (next hop) de la interfaz de reserva ISDN (RDSI) BRI o de módem analógico.



# CAPÍTULO 6

## Crear un firewall

---

Un firewall es un conjunto de reglas que se utilizan para proteger los recursos de la LAN y filtrar los paquetes que llegan al router. Si un paquete no cumple los criterios especificados en la regla, se tira. En caso contrario, se le autoriza pasar por la interfaz a la que la regla es aplicable. Este asistente permite crear un firewall para la LAN mediante un sistema de respuestas a mensajes de un conjunto de pantallas.

En esta ventana, seleccione el tipo de firewall que desea crear.



### Nota

- El router que va a configurar debe utilizar una imagen de Cisco IOS que admita la función de firewall para poder utilizar Cisco Router and Security Device Manager (Cisco SDM) en la configuración de un firewall en el router.
  - Para poder configurar un firewall, es necesario haber finalizado las configuraciones de LAN y WAN.
- 

### Firewall básico

Haga clic en esta opción si desea que Cisco SDM cree un firewall mediante reglas por defecto. El escenario del ejemplo muestra una configuración de red típica en la que se utiliza este tipo de firewall.

## Firewall avanzado

Haga clic en esta opción si desea que Cisco SDM le guíe por el proceso de configuración de un firewall. Tiene la opción de crear una red [DMZ](#) y especificar una [regla de inspección](#). El escenario del ejemplo que se muestra al seleccionar esta opción presenta una configuración típica de firewall en Internet.

### ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
<p>Que Cisco SDM cree un firewall en mi sistema.</p> <p>Es conveniente que seleccione esta opción si no desea configurar una red DMZ, o bien si sólo existe una interfaz externa.</p>	<p>Haga clic en <b>Firewall básico</b>. A continuación, haga clic en <b>Iniciar la tarea seleccionada</b>.</p> <p>Cisco SDM le pide que identifique las interfaces en el router y, a continuación, utiliza las reglas de inspección y de acceso por defecto de Cisco SDM para crear el firewall.</p>
<p>Que Cisco SDM me ayude a crear un firewall avanzado.</p> <p>Si el router dispone de varias interfaces internas y externas y desea configurar una red DMZ, debería seleccionar esta opción.</p>	<p>Seleccione <b>Firewall avanzado</b>. A continuación, haga clic en <b>Iniciar la tarea seleccionada</b>.</p> <p>Cisco SDM le mostrará la regla de inspección por defecto y le permitirá utilizarla en el firewall. Si lo prefiere, puede crear su propia regla de inspección. Cisco SDM utilizará una regla de acceso por defecto en el firewall.</p>



Si desea:	Haga lo siguiente:
<p>Obtener información acerca de una tarea que este asistente no me ayuda a llevar a cabo.</p>	<p>Seleccione un tema en la lista siguiente:</p> <ul style="list-style-type: none"> <li>• ¿Como se visualiza la actividad en el firewall?</li> <li>• ¿Cómo se configura un firewall en una interfaz no compatible?</li> <li>• ¿Cómo se configura un firewall después de configurar una VPN?</li> <li>• ¿Cómo se puede permitir que pase determinado tráfico por una interfaz DMZ?</li> <li>• ¿Cómo se modifica un firewall existente para permitir el tráfico procedente de una nueva red o host?</li> <li>• ¿Cómo se configura NAT en una interfaz no admitida?</li> <li>• ¿Cómo se configura el paso de NAT (NAT Passthrough) para un firewall?</li> <li>• ¿Cómo se permite que el tráfico llegue al concentrador Easy VPN a través del firewall?</li> <li>• ¿Cómo se asocia una regla a una interfaz?</li> <li>• ¿Cómo se anula la asociación de una regla de acceso con una interfaz?</li> <li>• ¿Cómo se elimina una regla que esté asociada a una interfaz?</li> <li>• ¿Cómo se crea una regla de acceso para una lista Java?</li> <li>• ¿Cómo se visualizan los comandos de IOS que se envían al router?</li> <li>• ¿Cómo se permite que tráfico determinado entre en la red si no se dispone de una red DMZ?</li> </ul>

# Asistente de configuración para firewall básico

Cisco SDM protegerá la LAN con un firewall por defecto cuando seleccione esta opción. Para que Cisco SDM pueda hacerlo, debe especificar las interfaces interna y externa en la ventana siguiente. Haga clic en **Siguiente** para empezar la configuración.

## Configuración de la interfaz de firewall básico

Identifique las interfaces en el router de modo que el firewall se aplique a la interfaz correcta.

### Interfaz externa (no fiable)

Seleccione la interfaz del router que está conectada a Internet o a la WAN de la organización.

**Nota**

No seleccione la interfaz mediante la cual ha accedido a Cisco SDM como interfaz externa (no fiable). De hacerlo, perdería la conexión con Cisco SDM. Dado que estará protegido por un firewall, no podrá iniciar Cisco SDM desde la interfaz externa (no fiable) una vez finalizado el asistente para firewall.

### Permitir acceso seguro a Cisco SDM de la casilla de verificación interfaces externas

Marque esta casilla si desea que los usuarios fuera del firewall puedan acceder al router usando Cisco SDM. El asistente mostrará una pantalla que le permitirá especificar una dirección IP o una dirección de la red. El firewall se modificará para permitir el acceso a la dirección que usted especifique. Si usted especifica una dirección de la red, a todos los hosts en esa red se les permitirá pasar por el firewall.

### Interfaz interna (fiable)

Compruebe las interfaces físicas y lógicas que están conectadas a la LAN. Puede seleccionar varias interfaces.

## Configuración del firewall para acceso remoto

Crear un firewall puede bloquear el acceso al router que los administradores remotos pueden necesitar. Puede especificar las interfaces del router a usar para el acceso de administración remota y los hosts donde los administradores pueden entrar al Cisco SDM para administrar el router. El firewall se modificará para permitir el acceso remoto seguro del host o la red que usted especifique.

### Seleccionar la interfaz externa

Si está usando el Asistente para Firewall avanzado, seleccione la interfaz a través de la cual los usuarios iniciarán Cisco SDM. Este campo no aparece en el Asistente del Firewall Básico.

### Host/Red origen

Si desea permitir el acceso a un único host a través del firewall, elija **Dirección del host** e introduzca la dirección IP de un host. Elija **Dirección de red** e introduzca la dirección de una red y una máscara de subred para permitirle a los hosts en esa red acceder a través del firewall. El host o la red deben ser accesibles desde la interfaz que usted especificó. Elija **Cualquiera** para permitir que cualquier host conectado a las interfaces especificadas acceda de forma segura a la red.

## Asistente de configuración para firewall avanzado

Cisco SDM le ayudará a crear un firewall de [Internet](#), solicitándole información acerca de las interfaces en el router, si desea configurar una red DMZ y qué reglas desea utilizar en el firewall.

Haga clic en **Siguiente** para empezar la configuración.

## Configuración de la interfaz de firewall avanzado

Identifique las interfaces interna y externa del router y la interfaz que se conecta a la red DMZ.

Marque la opción **externa** o **interna** para identificar la interfaz según corresponda. Las interfaces externas se conectan a la [WAN](#) de la organización o a Internet. Las internas, en cambio, se conectan a la [LAN](#).

## Permitir acceso seguro a Cisco SDM de la casilla de verificación interfaces externas

Marque esta casilla si desea que los usuarios fuera del firewall puedan acceder al router usando Cisco SDM. El asistente mostrará una pantalla que le permitirá especificar una dirección IP o una dirección de la red. El firewall se modificará para permitir el acceso a la dirección que usted especifique. Si usted especifica una dirección de la red, a todos los hosts en esa red se les permitirá pasar por el firewall.

## Interfaz DMZ

Seleccione la interfaz de router que se conecta a una red DMZ, si la hay. Una red DMZ es una zona de búfer que se utiliza para aislar el tráfico que proviene de una red no fiable. Si dispone de una red de este tipo, seleccione la interfaz que se conecta a ella.

## Configuración del servicio DMZ de firewall avanzado

Esta ventana permite ver las entradas de regla que especifican qué servicios disponibles en la red DMZ desea hacer accesibles por medio de las interfaces externas del router. Se autorizará el paso del tráfico de los tipos de servicio especificados a la red DMZ por medio de las interfaces externas.

## Configuración de servicio DMZ

Esta área muestra las entradas de servicios DMZ configuradas en el router.

### Dirección IP inicial

La primera dirección IP del intervalo que especifica los hosts de la red DMZ.

### Dirección IP final

La última dirección IP del intervalo que especifica los hosts de la red DMZ. Si en esta columna no figura ningún valor, se supone que la dirección IP de la columna de dirección IP inicial será el único host de la red DMZ. El intervalo puede especificar un máximo de 254 hosts.

**Tipo de servicio**

El tipo de servicio: TCP (Transmission Control Protocol) o UDP (User Datagram Protocol).

**Servicio**

El nombre del servicio, como Telnet o FTP, o un número de protocolo.

**Para configurar una entrada de servicio DMZ:**

Haga clic en **Agregar** y cree la entrada en la ventana Configuración de servicio DMZ.

**Para editar una entrada de servicio DMZ:**

Seleccione la entrada de servicio y haga clic en **Editar**. A continuación, modifique la entrada en la ventana Configuración de servicio DMZ.

**Configuración de servicio DMZ**

En esta ventana puede crear o editar un servicio DMZ.

**Dirección IP del host**

Especifique el intervalo de direcciones que especificará los hosts en la DMZ a la que se aplica esta entrada. El firewall autorizará al tráfico el acceso a estos hosts para el servicio TCP o UDP especificado.

**Dirección IP inicial**

Especifique la primera dirección IP del intervalo; por ejemplo, 172.20.1.1. Si está activada la traducción de direcciones de red (**NAT**), deberá especificar la dirección traducida, conocida como la dirección *global interna*.

**Dirección IP final**

Especifique la última dirección IP del intervalo; por ejemplo, 172.20.1.254. Si está activada la NAT, deberá especificar la dirección traducida por dicho servicio.

## Servicio

### TCP

Haga clic en esta opción si desea permitir tráfico para un servicio TCP.

### UDP

Haga clic en esta opción si desea permitir tráfico para un servicio UDP.

### Servicio

Especifique el número o nombre del servicio en este campo. Si desconoce el nombre o número, haga clic en el botón y seleccione el servicio de la lista mostrada.

## Configuración de seguridad de la aplicación

Cisco SDM proporciona las políticas preconfiguradas de seguridad de la aplicación que usted puede usar para proteger la red. Use la barra de desplazamiento para seleccionar el nivel de seguridad que desee y para ver una descripción de la seguridad que proporciona. La pantalla de resumen del asistente muestra el nombre de la política, SDM\_HIGH, SDM\_MEDIUM, o SDM\_LOW y las declaraciones de configuración en la política. Usted también puede ver los detalles de la política al hacer clic en el la ficha Seguridad de la Aplicación y escoger el nombre de la política.

### Botón Previsualizar comandos

Haga clic para ver los comandos de IOS que constituyen esta política.

### Botón Política personalizada de seguridad de la aplicación

Este botón y el campo Nombre de la política son visibles si está completando el Asistente del firewall avanzado. Escoja esta opción si desea crear su propia política de seguridad de la aplicación. Si la política ya existe, especifique el nombre en el campo, o haga clic en el botón situado a la derecha, elija **Seleccionar una política existente** y seleccione la política. Para crear una política, haga clic en el botón y elija **Crear una Nueva Política** y cree la política en el cuadro de diálogo mostrado.

## Configuración del servidor del nombre del dominio

El router debe configurarse con la dirección IP de al menos un servidor DNS para que la seguridad de la aplicación funcione. Haga clic en **Activar el nombre de host basado en DNS para la traducción de direcciones** y proporcione la dirección IP del servidor de DNS primario. Si un servidor de DNS secundario está disponible, especifique la dirección IP en el campo **Servidor DNS secundario**.

Las direcciones IP que usted introduzca serán visibles en la ventana de Propiedades del DNS bajo Tareas adicionales.

## Configuración del servidor de filtro URL

Los servidores de filtro de URL son capaces de almacenar y mantener más información de filtrado de URL de la que puede guardar un archivo de configuración del router. Si hay servidores de filtro de URL en la red, puede configurar el router para que los utilice. Puede configurar parámetros adicionales de servidor de filtro de URL en **Configurar > tareas adicionales > Filtrado de URL**. Consulte el apartado [Filtrado de URL](#) para obtener más información.

### Filtrar solicitud HTTP a través del servidor de filtro de URL

Marque la casilla **Filtrar solicitud HTTP a través del servidor de filtro de URL** para activar el filtrado de URL mediante servidores de filtro de URL.

### Tipo de servidor de filtro de URL

Cisco SDM admite los servidores de filtro de URL Secure Computing y Websense. Seleccione **Secure Computing** o **Websense** para especificar el tipo de servidor de filtro de URL en la red.

### Dirección IP/Nombre de host

Especifique el nombre de host o la dirección IP del servidor de filtro de URL.

## Seleccionar la zona de interfaz

Esta ventana aparece si una interfaz del router distinta de aquélla que está configurando es miembro de una [zona de seguridad](#) de Firewall de política basado en zonas. Para obtener más información acerca de este tema, consulte [Firewall de política basado en zonas](#).

### Seleccionar zona

Seleccione la zona de seguridad de la cual desea que la interfaz sea miembro. Si selecciona no asignar la interfaz a una zona, existen muchas posibilidades de que el tráfico no pase por la interfaz.

## Zonas internas de ZPF

Las zonas que incluyen interfaces usadas en túneles de encapsulación de enrutamiento genérico ([GRE](#)) deben ser designadas como zonas internas (fiables) para que el tráfico de GRE pase a través del firewall.

Esta ventana muestra las zonas configuradas y sus interfaces miembro. Para designar una zona como interna, marque la columna **interno (fiable)** en la fila de esa zona.

## Resumen

Esta pantalla resume la información del firewall. Usted puede revisar la información en esta pantalla y usar el botón Atrás para regresar a las pantallas en el asistente para hacer cambios.

La pantalla de resumen usa un lenguaje simple para describir la configuración. Puede ver los comandos del CLI que Cisco SDM envía al router si va a Editar > Preferencias y marca **Obtener una vista previa de los comandos antes de enviarlos al router**.



## Interfaces internas (fiabiles)

Cisco SDM enumera las interfaces lógicas y físicas del router que usted designó como las interfaces internas en esta sesión del asistente, junto con sus direcciones IP. Debajo, se dan descripciones de lenguaje plano para cada instrucción de configuración aplicada a las interfaces internas. Los siguientes son ejemplos:

```
Interfaces internas (fiabiles):
FastEthernet0/0 (10.28.54.205)
Aplicar la regla de acceso a la dirección entrante para permitir el
tráfico para negar el tráfico tipo spoof.
Aplicar la regla de acceso a la dirección entrante para denegar el
tráfico originado por direcciones de retrobucle local de difusión
(broadcast).
Aplicar la regla de acceso a la dirección entrante para permitir todos
los demás tipos de tráfico.
Aplicar la política de seguridad de la aplicación SDM_HIGH a la
dirección entrante.
```

Este ejemplo muestra la política de seguridad de la aplicación SDM\_HIGH de Cisco SDM aplicada al tráfico entrante en esta interfaz.

## Interfaces externas (no fiabiles)

Cisco SDM enumera las interfaces lógicas y físicas del router que usted designó como las interfaces externas en esta sesión del asistente, junto con sus direcciones IP. Debajo, se dan descripciones de lenguaje plano para cada instrucción de configuración aplicada a las interfaces externas. Los siguientes son ejemplos:

```
FastEthernet0/1 (142.120.12.1)
Activar la comprobación de envío de la ruta inversa de unidifusión
(unicast) para las interfaces sin túnel.
Aplicar la regla de acceso a la dirección entrante para permitir el
tráfico del túnel IPSec si es necesario.
Aplicar la regla de acceso a la dirección entrante para permitir el
tráfico del túnel GRE para las interfaces si es necesario.
Aplicar la regla de acceso a la dirección entrante para permitir el
tráfico de ICMP.
Aplicar la regla de acceso a la dirección entrante para permitir el
tráfico de NTP si necesario.
Aplicar la regla de acceso a la dirección entrante para permitir el
tráfico para negar el tráfico tipo spoof.
Aplicar la regla de acceso a la dirección entrante para denegar el
tráfico originado en direcciones de retrobucle locales y privadas de
difusión.
Aplicar la regla de acceso a la dirección entrante para permitir el
tráfico del servicio que va a la interfaz DMZ.
```

```
Servicio de ftp en 10.10.10.1 a 10.10.10.20
Aplicar la regla de acceso a la dirección entrante para permitir el
acceso de SDM seguro del host/red 140.44.3.0 255.255.255.0
Aplicar la regla de acceso a la dirección entrante para negar todo
tráfico.
```

Tenga en cuenta que esta configuración depende del envío de la ruta inversa, una función que permite que el router descarte los paquetes que carecen de una dirección IP de fuente verificable, y permite el tráfico de ftp a las direcciones DMZ 10.10.10.1 a 10.10.10.20.

## Interfaz DMZ

Si ha configurado un firewall avanzado, esta área muestra la interfaz DMZ que ha designado, junto con la dirección IP correspondiente. A continuación, Cisco SDM describe qué reglas de inspección y acceso se han asociado a esta interfaz. Los siguientes son ejemplos:

```
FastEthernet (10.10.10.1)
Aplicar la regla de inspección CBAC a la dirección saliente
Aplicar la regla de acceso a la dirección entrante para negar todo
tráfico.
```

### Para guardar esta configuración en la configuración en ejecución del router y salir de este asistente:

Haga clic en **Finalizar**. Cisco SDM guarda los cambios de configuración en la configuración en ejecución del router. Aunque los cambios se aplican inmediatamente, los mismos se perderán si se apaga el router.

Si ha marcado la opción **Obtener una vista previa de los comandos antes de enviarlos al router** de la ventana Preferencias del usuario, aparecerá la ventana Enviar configuración al router. Esta ventana permite ver los comandos del CLI que se envían al router.

## Alerta de SDM: Acceso a SDM

Esta ventana aparece cuando ha indicado que Cisco SDM debe acceder al router desde interfaces externas. Le informa que debe asegurarse de que SSH y HTTPS estén configurados y que, al menos, una de las interfaces designadas como externas estén configuradas con una dirección IP estática. Para realizar esta acción, asegúrese de que una interfaz externa esté configurada con una dirección IP estática y después asocie una política de gestión con esa interfaz.

## Determinación de si una interfaz externa está configurada con una dirección IP estática

Complete los pasos siguientes para determinar si una interfaz externa está configurada con una dirección IP estática.

- 
- Paso 1** Haga clic en **Configurar > interfaces y conexiones > Editar interfaz/conexión**.
- Paso 2** Revise la columna IP en la tabla de lista de interfaces para determinar si una interfaz externa tiene direcciones IP estáticas.
- Paso 3** Si ninguna interfaz externa tiene una dirección IP estática, seleccione una y haga clic en **Editar** para mostrar un cuadro de diálogo que le permita reconfigurar la información de dirección IP para la interfaz.

Si hay una interfaz externa con una dirección IP estática, anote el nombre de la interfaz y complete el procedimiento siguiente.

---

## Configuración de SSH y HTTPS

Complete los pasos siguientes para configurar una política de gestión para SSH y HTTPS en el router.

- 
- Paso 1** Haga clic en **Configurar > tareas adicionales > Acceso al router > Acceso a la gestión**.
- Paso 2** Si no hay una política de gestión, haga clic en **Agregar**. Si desea editar una política de gestión existente, selecciónela y haga clic en **Editar**.



**Nota** Si está editando una política de gestión, ésta se debe asociar con una interfaz que tenga una dirección IP estática.

---

- Paso 3** En el cuadro de diálogo que se muestra, especifique la información de dirección en la casilla Host/Red de origen. La información de dirección IP que especifica debe incluir la dirección IP del equipo que usará para administrar el router.
- Paso 4** Seleccione una interfaz externa con una dirección IP estática en la casilla Interfaz de gestión. Esta interfaz debe tener una ruta a la dirección IP que especificó en la casilla Host/red de origen.
- Paso 5** En la casilla Protocolos de gestión, marque **Permitir SDM**.

- Paso 6** Marque **HTTPS** y **SSH** para permitir esos protocolos.
  - Paso 7** Haga clic en **Aceptar** para cerrar el cuadro de diálogo.
  - Paso 8** Haga clic en **Aplicar cambios** en la ventana que muestra las políticas de acceso a la gestión.
- 

## Cómo...

En esta sección se incluyen procedimientos para las tareas que el asistente no le ayuda a llevar a cabo.

## ¿Como se visualiza la actividad en el firewall?

La actividad del **firewall** se supervisa mediante la creación de entradas de registro. Si en el router se ha activado el registro, siempre que se invoque una **regla** de acceso que se haya configurado para generar entradas de registro (por ejemplo, si se intentara una conexión desde una dirección IP denegada) se generará una entrada de registro y podrá verse en el modo Supervisión.

### Activar registro

El primer paso para ver la actividad del firewall consiste en activar el registro en el router. Para ello:

- 
- Paso 1** En el panel izquierdo, seleccione **Tareas adicionales**.
  - Paso 2** En el árbol Tareas adicionales, haga clic en **Registro** y, a continuación, en el botón **Editar**.
  - Paso 3** En la pantalla Syslog, marque la opción **Registro a un búfer**.
  - Paso 4** En el campo Tamaño del búfer, especifique la cantidad de memoria del router que desea utilizar para un búfer de registro. El valor por defecto es de 4096 bytes. Cuanto mayor sea el tamaño del búfer, más entradas de registro podrá almacenar, aunque el usuario debe calibrar la necesidad de aumentar el tamaño del búfer basándose en el rendimiento potencial del router.
  - Paso 5** Haga clic en **Aceptar**.
-

## Identificación de las reglas de acceso para las que desea generar entradas de registro

Además de activar el registro, debe identificar las reglas de acceso para las que desea generar entradas de registro. Para configurar reglas de acceso a fin de generar entradas de registro:

- 
- Paso 1** En el panel izquierdo, seleccione **Tareas adicionales**.
- Paso 2** En el árbol Tareas adicionales, haga clic en **Editor ACL** y, a continuación, en el botón **Reglas de acceso**.
- Cada regla de acceso aparece en la tabla superior del lateral derecho de la pantalla. La tabla inferior muestra las direcciones IP de origen y destino específicas, así como los servicios que la regla autoriza o deniega.
- Paso 3** En la tabla superior, haga clic en la regla que desea modificar.
- Paso 4** Haga clic en **Editar**.
- Aparecerá el cuadro de diálogo Editar una regla.
- Paso 5** El campo Entrada de regla muestra cada una de las combinaciones IP de origen/IP de destino/servicio que la regla autoriza o deniega. Haga clic en la entrada de regla que desea configurar para generar entradas de registro.
- Paso 6** Haga clic en **Editar**.
- Paso 7** En el cuadro de diálogo Entrada de regla, marque la casilla de verificación **Coincidencias de registro con esta entrada**.
- Paso 8** Haga clic en **Aceptar** para cerrar los cuadros de diálogo que ha visualizado.
- Llegado este punto, la entrada de regla que acaba de modificar generará entradas de registro siempre que se intente establecer una conexión desde el intervalo de direcciones IP y servicios que definen la entrada de regla.
- Paso 9** Repita los pasos 4 a 8 para cada una de las entradas de regla que desea configurar con el fin de generar entradas de registro.
-

Una vez finalizada la configuración de registro, siga los pasos a continuación para ver la actividad del firewall:

---

**Paso 1** En la barra de herramientas, seleccione el modo **Supervisión**.

**Paso 2** En el panel izquierdo, seleccione **Estado del firewall**.

En el área Estadísticas de firewall, puede verificar que el firewall se ha configurado y ver el número de intentos de conexión que se han denegado.

La tabla muestra cada una de las entradas de registro del router que ha generado el firewall, incluida la hora y el motivo por el cual se ha generado la entrada de registro.

---

## ¿Cómo se configura un firewall en una interfaz no compatible?

Cisco SDM puede configurar un [firewall](#) en un tipo de interfaz no admitido por Cisco SDM. Para poder configurar el firewall, primero es preciso utilizar la [CLI](#) del router para configurar la interfaz. La interfaz deberá tener, como mínimo, una dirección IP configurada y deberá estar en funcionamiento. Para obtener más información acerca de cómo configurar una interfaz mediante el CLI, consulte la Guía de configuración del software correspondiente al router.

Para verificar que la conexión funciona, compruebe que el estado de la interfaz es “Hacia arriba” en la ventana Interfaces y conexiones.

El extracto siguiente muestra la configuración de una interfaz ISDN (RDSI) en un router Cisco 3620:

```
!
isdn switch-type basic-5ess
!
interface BRI0/0
! This is the data BRI WIC
ip unnumbered Ethernet0/0
no ip directed-broadcast
encapsulation ppp
no ip mroute-cache
dialer map ip 100.100.100.100 name junky 883531601
dialer hold-queue 10
isdn switch-type basic-5ess
isdn tei-negotiation first-call
isdn twait-disable
isdn spid1 80568541630101 6854163
isdn incoming-voice modem
```

En la Guía de configuración del software correspondiente al router encontrará otras configuraciones.

Después de configurar la interfaz no compatible mediante el CLI, puede utilizar Cisco SDM para configurar el firewall. La interfaz no compatible aparecerá como “Otros” en los campos que enumeran las interfaces del router.

## ¿Cómo se configura un firewall después de configurar una VPN?

Si se coloca un [firewall](#) en una interfaz utilizada en una VPN, el firewall debe permitir el tráfico entre los pares VPN local y remoto. Si utiliza el asistente para firewall básico o avanzado, Cisco SDM permitirá automáticamente que el tráfico fluya entre pares VPN.

Si crea una regla de acceso en el Editor ACL disponible en Tareas adicionales, tendrá el control absoluto sobre las declaraciones de permiso y denegación y deberá cerciorarse de que el tráfico está autorizado a fluir entre homólogos VPN. Las declaraciones siguientes son ejemplos de los tipos de declaraciones que deben incluirse en la configuración para permitir el tráfico VPN:

```
access-list 105 permit ahp host 123.3.4.5 host 192.168.0.1
access-list 105 permit esp host 123.3.4.5 host 192.168.0.1
access-list 105 permit udp host 123.3.4.5 host 192.168.0.1 eq isakmp
access-list 105 permit udp host 123.3.4.5 host 192.168.0.1 eq
non500-isakmp
```

## ¿Cómo se puede permitir que pase determinado tráfico por una interfaz DMZ?

Siga los pasos siguientes para configurar el acceso a través del firewall a un servidor Web de una red [DMZ](#):

---

**Paso 1** En el panel izquierdo, seleccione **Firewall y lista de control de acceso**.

**Paso 2** Seleccione **Firewall avanzado**.

**Paso 3** Haga clic en **Iniciar la tarea seleccionada**.

**Paso 4** Haga clic en **Siguiente**.

Aparece la pantalla Configuración de la interfaz de firewall de Internet avanzada.

- Paso 5** En la tabla Interfaz, seleccione qué interfaces se conectan a las redes dentro del firewall y cuáles lo hacen a redes de fuera del firewall.
  - Paso 6** En el campo Interfaz DMZ, seleccione la interfaz que se conecta a la red DMZ.
  - Paso 7** Haga clic en **Siguiente**>.
  - Paso 8** En el campo Dirección IP, especifique la dirección IP o intervalo de direcciones IP del servidor o servidores Web.
  - Paso 9** En el campo Servicio, seleccione TCP.
  - Paso 10** En el campo Puerto, especifique **80** o **www**.
  - Paso 11** Haga clic en **Siguiente**>.
  - Paso 12** Haga clic en **Finalizar**.
- 

## ¿Cómo se modifica un firewall existente para permitir el tráfico procedente de una nueva red o host?

Puede utilizar la ficha Editar política de firewall para modificar la configuración de firewall y permitir el tráfico procedente de una nueva red o host.

- 
- Paso 1** En el panel izquierdo, seleccione **Firewall y lista de control de acceso**.
  - Paso 2** Haga clic en la ficha **Editar política de firewall**.
  - Paso 3** En el panel de selección del tráfico elija una interfaz Desde y una interfaz Hasta para especificar el flujo de tráfico al cual se ha aplicado el firewall y, a continuación, haga clic en **Ir**. Si se ha aplicado un firewall al flujo de tráfico, aparecerá un icono de firewall en el gráfico del router. Si el flujo de tráfico que selecciona no muestra la regla de acceso que debe modificar, seleccione una interfaz Desde y una interfaz Hasta distintas.
  - Paso 4** Examine la regla de acceso en el área Servicio. Utilice el botón **Agregar** para mostrar el cuadro de diálogo de una nueva entrada de regla de acceso.
  - Paso 5** Especifique una declaración de permiso para la red o host a los que desea permitir el acceso a la red. Haga clic en **Aceptar** en el cuadro de diálogo de la entrada de regla.
  - Paso 6** En el área Servicio aparece la nueva entrada.
  - Paso 7** Utilice los botones **Cortar** y **Pegar** para cambiar la posición de la entrada en la lista, si es necesario.
-



## ¿Cómo se configura NAT en una interfaz no admitida?

Cisco SDM puede configurar la traducción de direcciones de red (**NAT**) en un tipo de interfaz no compatible con Cisco SDM. Para poder configurar el firewall, primero es preciso utilizar la **CLI** del router para configurar la interfaz. La interfaz deberá tener, como mínimo, una dirección IP configurada y deberá estar en funcionamiento. Para verificar que la conexión funcione, verifique que el estado de la interfaz sea activo.

Después de configurar la interfaz no compatible mediante el CLI, puede configurar NAT. La interfaz no admitida aparecerá como “Otro” en la lista de interfaces del router.

## ¿Cómo se configura el paso de NAT (NAT Passthrough) para un firewall?

Si ha configurado la **NAT** y se dispone a configurar el **firewall**, deberá hacerlo de tal forma que autorice el tráfico procedente de la dirección IP pública. Para ello, es necesario configurar una **ACL**. Para configurar una lista de control de acceso que permita el tráfico procedente de la dirección IP pública:

- 
- Paso 1** En el panel izquierdo, seleccione **Tareas adicionales**.
  - Paso 2** En el árbol Reglas, haga clic en **Editor ACL** y, a continuación, en el botón **Reglas de acceso**.
  - Paso 3** Haga clic en **Agregar**.  
Aparecerá el cuadro de diálogo Agregar una regla.
  - Paso 4** En el campo Nombre/Número, especifique un nombre o un número exclusivo para la regla nueva.
  - Paso 5** En el campo Tipo, seleccione **Regla estándar**.
  - Paso 6** En el campo Descripción, introduzca una breve descripción de la nueva regla, como “Permitir el paso de NAT”.
  - Paso 7** Haga clic en **Agregar**.  
Aparecerá el cuadro de diálogo Agregar una entrada de regla estándar.
  - Paso 8** En el campo Acción, seleccione **Permitir**.

- Paso 9** En el campo Tipo, seleccione **Host**.
- Paso 10** En el campo Dirección IP, especifique la dirección IP pública.
- Paso 11** En el campo Descripción, introduzca una breve descripción como “Dirección IP pública”.
- Paso 12** Haga clic en **Aceptar**.
- Paso 13** Haga clic en **Aceptar**.
- Ahora, la nueva regla aparecerá en la tabla Reglas de acceso.
- 

## ¿Cómo se permite que el tráfico llegue al concentrador Easy VPN a través del firewall?

Para poder permitir el tráfico por medio del firewall hacia un concentrador VPN, debe crear o modificar las [regla](#) de acceso que permitan el tráfico [VPN](#). Para ello:

---

- Paso 1** En el panel izquierdo, seleccione **Tareas adicionales**.
- Paso 2** En el árbol Reglas, haga clic en **Editor ACL** y, a continuación, en el botón **Reglas de acceso**.
- Paso 3** Haga clic en **Agregar**.
- Aparecerá el cuadro de diálogo Agregar una regla.
- Paso 4** En el campo Nombre/Número, especifique un nombre o un número exclusivo para esta regla.
- Paso 5** En el campo Descripción, introduzca una breve descripción de la regla, como “Tráfico del concentrador VPN”.
- Paso 6** Haga clic en **Agregar**.
- Aparecerá el cuadro de diálogo Agregar una entrada de regla ampliada.
- Paso 7** En el grupo Red/host de origen, del campo Tipo, seleccione **Una red**.
- Paso 8** En los campos Dirección IP y Máscara inversa, especifique la dirección IP y la máscara de red del homólogo de origen de VPN.
- Paso 9** En el grupo Red/host de destino, del campo Tipo, seleccione **Una red**.

- Paso 10** En los campos Dirección IP y Máscara inversa, especifique la dirección IP y la máscara de red del homólogo de destino de VPN.
- Paso 11** En el grupo Protocolo y servicio, seleccione **TCP**.
- Paso 12** En los campos Puerto de origen, seleccione = y especifique el número de puerto **1023**.
- Paso 13** En los campos Puerto de destino, seleccione = y especifique el número de puerto **1723**.
- Paso 14** Haga clic en **Aceptar**.  
En el área Entrada de regla aparece la nueva entrada de regla.
- Paso 15** Repita los pasos 1 a 8 con el fin de crear entradas de regla para los protocolos y, si es aplicable, los números de puerto que se indican a continuación:
- Protocolo **IP**, protocol IP **GRE**
  - Protocolo **UDP**, Puerto de origen **500**, Puerto de destino **500**
  - Protocolo **IP**, protocol IP **ESP**
  - Protocolo **UDP**, Puerto de origen **10000**, Puerto de destino **10000**
- Paso 16** Haga clic en **Aceptar**.
- 

## ¿Cómo se asocia una regla a una interfaz?

Si utiliza el asistente para firewall de Cisco SDM, las reglas de acceso e inspección que cree se asociarán automáticamente a la interfaz para la que ha creado el firewall. Si desea crear una regla en Tareas adicionales/Editor ACL, puede asociarla a una interfaz en la ventana [Agregar/Editar una regla](#). Si no la asocia a ninguna interfaz en ese momento, podrá hacerlo igualmente más adelante.

- 
- Paso 1** Haga clic en **Interfaces y conexiones** del panel izquierdo y en **Editar interfaz/conexión**.
- Paso 2** Seleccione la interfaz a la cual desea asociar una regla y haga clic en **Editar**.

- Paso 3** En la ficha Asociación, especifique el número o nombre de la regla en los campos Entrante o Saliente de los cuadros Regla de acceso o Regla de inspección. Si desea que la regla filtre el tráfico antes de entrar en la interfaz, utilice el campo Entrante. Si desea que la regla filtre el tráfico que ya ha entrado en el router, aunque posiblemente lo abandone por medio de la interfaz seleccionada, utilice el campo Saliente.
- Paso 4** Haga clic en **Aceptar** de la ficha Asociación.
- Paso 5** En la ventana Reglas de acceso o Reglas de inspección, examine la columna Usado por para verificar que la regla se ha asociado a la interfaz.
- 

## ¿Cómo se anula la asociación de una regla de acceso con una interfaz?

Puede que sea necesario eliminar la asociación entre una regla de acceso y una interfaz, en cuyo caso no se elimina la regla de acceso. Puede asociarla a otras interfaces, si lo desea. Para eliminar la asociación entre estos dos tipos de regla, realice los pasos siguientes:

- 
- Paso 1** Haga clic en **Interfaces y conexiones** del panel izquierdo y en **Editar interfaz/conexión**.
- Paso 2** Seleccione la interfaz cuya asociación con la regla de acceso desea anular.
- Paso 3** Haga clic en **Editar**.
- Paso 4** En la ficha Asociación, busque la regla de acceso en los campos Entrante o Saliente del cuadro Regla de acceso. Ésta puede tener un nombre o número.
- Paso 5** Haga clic en el campo Entrante o Saliente y en el botón de la derecha.
- Paso 6** Haga clic en **Ninguno (Borrar la asociación de reglas)**.
- Paso 7** Haga clic en **Aceptar**.
-

## ¿Cómo se elimina una regla que esté asociada a una interfaz?

Cisco SDM no permite eliminar una regla que esté asociada a una interfaz; en primer lugar, debe anular la asociación entre la regla y la interfaz y, a continuación, eliminar la regla de acceso.

- 
- Paso 1** Haga clic en **Interfaces y conexiones** del panel izquierdo y en **Editar interfaz/conexión**.
  - Paso 2** Seleccione la interfaz cuya asociación con la regla desea anular.
  - Paso 3** Haga clic en **Editar**.
  - Paso 4** En la ficha Asociación, busque la regla en los campos Regla de acceso o Regla de inspección. Ésta puede tener un nombre o número.
  - Paso 5** Busque la regla en la ficha Asociación. **Si se trata de una regla de acceso, haga clic en Ninguno (Borrar la asociación de reglas). Si se trata de una regla de inspección, haga clic en Ninguno.**
  - Paso 6** Haga clic en **Aceptar**.
  - Paso 7** Haga clic en **Reglas** en el panel izquierdo. Utilice el árbol Reglas para ir a las ventanas Regla de acceso o Regla de inspección.
  - Paso 8** Seleccione la regla que desea quitar y haga clic en **Eliminar**.

## ¿Cómo se crea una regla de acceso para una lista Java?

Las reglas de inspección permiten especificar listas Java. Una lista Java se utiliza para permitir el flujo de tráfico de subprogramas Java procedente de fuentes fiables. Estas fuentes se definen en una regla de acceso que se menciona en la lista Java. Para crear este tipo de regla de acceso y utilizarla en una lista Java, realice los pasos siguientes:

- 
- Paso 1** Si se encuentra en la ventana Reglas de inspección y ha hecho clic en **Lista Java**, haga clic en el botón a la derecha del campo Número y en **Cree una nueva regla (ACL) y seleccione**. Se abre la ventana Agregar una regla.  
Si se encuentra en la ventana Reglas de acceso, haga clic en **Agregar** para abrir la ventana Agregar una regla.

**Paso 2** En la ventana Agregar una regla, cree una regla de acceso estándar que permita el tráfico desde las direcciones que considere fiables. Por ejemplo, si quisiera permitir los subprogramas Java de los hosts 10.22.55.3 y 172.55.66.1, podría crear las entradas de regla de acceso siguientes en la ventana Agregar una regla:

```
permit host 10.22.55.3
permit host 172.55.66.1
```

Puede proporcionar descripciones de las entradas y una descripción de la regla.

No es necesario asociar la regla a la interfaz a la que va a aplicar la regla de inspección.

**Paso 3** Haga clic en **Aceptar** en la ventana Agregar una regla.

**Paso 4** Si ha iniciado este procedimiento desde la ventana Reglas de inspección, haga clic en **Aceptar** en la ventana Lista Java. No es necesario realizar los pasos 5 y 6.

**Paso 5** Si ha iniciado este procedimiento en la ventana Reglas de acceso, vaya a la ventana Reglas de inspección y seleccione la regla de inspección para la que desea crear una lista Java y, a continuación, haga clic en **Editar**.

**Paso 6** Marque **http** en la columna Protocolos y haga clic en **Lista Java**.

**Paso 7** En el campo Número de lista Java, especifique el número de la lista de acceso que ha creado. Haga clic en **Aceptar**.

---

## ¿Cómo se permite que tráfico determinado entre en la red si no se dispone de una red DMZ?

El asistente para firewall permite especificar el tráfico que desea permitir en la red DMZ. Si no dispone de una red DMZ, puede permitir igualmente los tipos de tráfico externo que indique en la red mediante la función de política de firewall.

---

**Paso 1** Configure un firewall mediante el asistente para firewall.

**Paso 2** Haga clic en **Editar política de firewall/Lista de control de acceso**.

**Paso 3** Para mostrar la regla de acceso que necesita modificar, seleccione la interfaz externa (no fiable) como interfaz Desde, y la interfaz interna (fiable) como la interfaz Hasta. Se mostrará la regla de acceso aplicada al tráfico entrante en la interfaz no fiable.

- Paso 4** Para permitir un determinado tipo de tráfico en la red que todavía no esté autorizado, haga clic en **Agregar** en el área Servicio.
- Paso 5** Cree las entradas que necesita en el cuadro de diálogo de entrada de reglas. Debe hacer clic en **Agregar** para cada una de ellas.
- Paso 6** Las entradas que cree aparecerán en la lista de entradas del área Servicio.
-







## CAPÍTULO 7

# Política de firewall

---

La función Política de firewall permite ver y modificar las configuraciones de firewall (reglas de acceso y reglas de inspección [CBAC](#)) en el contexto de las interfaces cuyo tráfico filtran. Con la ayuda de una representación gráfica del router y sus interfaces correspondientes, puede seleccionar distintas interfaces en el router y ver si se ha aplicado una regla de acceso o regla de inspección a dicha interfaz. También puede ver los detalles de las reglas mostradas en la ventana Editar política de firewall/Lista de control de acceso.

## Editar política de firewall/Lista de control de acceso

Utilice la ventana Editar Política de firewall/Lista de control de acceso para ver las reglas de acceso e inspección en un contexto que muestre las interfaces a las que se asocian las reglas. Utilícela también para modificar las reglas de acceso e inspección que se muestran.

### Configurar un firewall antes de utilizar la función Política de firewall

Antes de utilizar la ventana Editar Política de firewall/Lista de control de acceso, debe realizar las tareas siguientes:

1. **Configurar las interfaces LAN y WAN.** Antes de crear un firewall debe configurar las interfaces LAN y WAN. Puede utilizar los asistentes para LAN y WAN, respectivamente, para configurar conexiones para el router.

2. **Utilizar el Asistente para firewall para configurar un firewall y una DMZ.** El Asistente para firewall es el modo más sencillo de aplicar reglas de acceso e inspección a las interfaces interna y externa que usted identifique. Además, le permite configurar una interfaz DMZ y especificar los servicios que deben permitirse en la red DMZ.
3. **Ir a la ventana Política de firewall para editar la política de firewall que ha creado.** Tras configurar las interfaces LAN y WAN y crear un firewall, puede abrir esta ventana y obtener una representación gráfica de la política en un flujo de tráfico. Puede ver las entradas de reglas de acceso e inspección y efectuar los cambios oportunos.

### Utilizar la función Vista de política del firewall

Una vez creado el firewall, puede utilizar la ventana Vista de política del firewall para obtener una representación gráfica del firewall en el contexto de las interfaces del router, así como para realizar las modificaciones oportunas.

Para obtener más información, haga clic en la acción que desea realizar:

- [Seleccionar un flujo de tráfico](#)
- [Examinar el diagrama de tráfico y seleccionar una dirección de tráfico](#)
- [Realizar cambios a las reglas de acceso](#)
- [Realizar cambios a las reglas de inspección](#)

Si desea ver un ejemplo, consulte [Escenario de utilización de políticas de firewall](#).



#### Nota

---

Si el router utiliza una imagen de Cisco IOS que no admite el conjunto de funciones del firewall, sólo se mostrará el área Servicios y sólo podrá crear entradas de control de acceso.

---

### Botón Aplicar cambios

Haga clic en este botón para enviar al router los cambios efectuados en esta ventana. Si abandona la ventana Editar política de firewall/Lista de control de acceso sin marcar la opción **Aplicar cambios**, Cisco SDM muestra un mensaje indicando que debe aplicar los cambios o descartarlos.

### Botón Descartar cambios

Haga clic en este botón para descartar los cambios efectuados en esta ventana. Este botón no le permite anular los cambios que haya enviado al router mediante el botón **Aplicar cambios**.

## Seleccionar un flujo de tráfico


*Flujo de tráfico* hace referencia al tráfico que entra al router en una interfaz específica (la interfaz *desde*) y sale del router en una interfaz específica (la interfaz *hasta*). Los controles de visualización del flujo de tráfico de Cisco SDM se ubican en una fila en la parte superior de la ventana Editar Política de firewall/Lista de control de acceso.



**Nota**

Es necesario que se haya configurado un mínimo de dos interfaces en el router. Si sólo hay una, Cisco SDM mostrará un mensaje indicando que el usuario debe configurar otra interfaz.

La siguiente tabla define los controles de visualización del flujo de tráfico de Cisco SDM.

<b>Desde</b>	Seleccione la interfaz desde la cual se origina el flujo de tráfico que desea. El firewall protegerá la red conectada a la interfaz Desde. La lista desplegable <b>Desde</b> sólo contiene interfaces con direcciones IP configuradas.
<b>Hasta</b>	Seleccione la interfaz desde la cual el tráfico sale del router. La lista desplegable <b>Hasta</b> sólo contiene interfaces con direcciones IP configuradas.
	Botón Detalles. Haga clic aquí para ver los detalles acerca de la interfaz. Se obtienen detalles del tipo dirección IP, tipo de encapsulación, política IPsec asociada y tipo de autenticación.

<b>Botón Ir</b>	Haga clic para actualizar el diagrama de flujo de tráfico con información acerca de las interfaces que ha seleccionado. El diagrama no se actualizará hasta que haga clic en <b>Ir</b> . El botón <b>Ir</b> estará desactivado si no ha seleccionado ninguna interfaz Desde o Hasta, o bien, si las interfaces Desde y Hasta coinciden.
<b>Opción Ver</b>	Seleccione <b>Alternar las interfaces Desde y Hasta</b> para alternar las interfaces que seleccionó originalmente en las listas desplegadas <b>Desde y Hasta</b> . Puede utilizar esta opción si desea crear un firewall que proteja la red conectada a la interfaz Desde y la red conectada a la interfaz Hasta. Puede seleccionar <b>Vista de todas las ACL en el flujo del tráfico</b> cuando se haya aplicado una regla de acceso a la interfaz Desde y otra regla de acceso a la interfaz Hasta para una dirección de tráfico que haya elegido. Las entradas de ambas reglas de acceso aparecen en otra ventana.

Cisco SDM muestra las interfaces que tienen direcciones IP en orden alfabético en las listas desplegadas **Desde** y **Hasta**. Por defecto, Cisco SDM selecciona la primera interfaz de la lista **Desde**, y la segunda interfaz de la lista **Hasta**. Utilice las listas desplegadas **Desde** y **Hasta** para seleccionar un flujo de tráfico diferente. El flujo de tráfico seleccionado se muestra en el diagrama de tráfico debajo de los controles de visualización del flujo de tráfico.

Por ejemplo, para ver el flujo de tráfico de una red conectada a la interfaz del router Ethernet 0, que abandona el router por la interfaz Serie 0, siga estos pasos:

- 
- Paso 1** Seleccione Ethernet 0 en la lista desplegable **Desde**.
  - Paso 2** Seleccione Serie 0 en la lista desplegable **Hasta**.
  - Paso 3** Haga clic en **Ir**.
  - Paso 4** Para cambiar las interfaces en las listas desplegadas **Desde** y **Hasta**, seleccione **Alternar las interfaces Desde y Hasta** desde la lista desplegable Opción Ver. Las reglas de acceso que se aplican al tráfico de origen y de vuelta pueden ser diferentes. Para obtener más información acerca de cómo alternar entre el tráfico de origen y de vuelta en la visualización en el diagrama de tráfico, consulte [Examinar el diagrama de tráfico y seleccionar una dirección de tráfico](#).
  - Paso 5** Haga clic en el botón **Detalles** junto a la lista desplegable **Desde** o **Hasta** para abrir una ventana que muestre la dirección IP, la política IPsec e información adicional de una interfaz.
-

Para trabajar con el diagrama de tráfico, consulte [Examinar el diagrama de tráfico y seleccionar una dirección de tráfico](#). Para volver a la descripción de la ventana Política de firewall principal, consulte [Editar política de firewall/Lista de control de acceso](#).

## Examinar el diagrama de tráfico y seleccionar una dirección de tráfico

El diagrama de tráfico muestra el router con las interfaces Desde y Hasta seleccionadas (para obtener más información, consulte [Seleccionar un flujo de tráfico](#)). También muestra los tipos de reglas que se aplican al flujo de tráfico seleccionado, además de la dirección en la cual se aplican.

### Tráfico de origen

Haga clic para resaltar el flujo de tráfico que entra al router en la interfaz Desde y sale del router en la interfaz Hasta. Cuando esta área se muestra resaltada, puede ver los detalles de las reglas aplicadas en la dirección del flujo de tráfico.




### Tráfico de vuelta

Haga clic para resaltar el flujo de tráfico que entra al router en la interfaz Hasta y sale del router en la interfaz Desde. Cuando esta área se muestra resaltada, puede ver los detalles de las reglas aplicadas al tráfico de vuelta.

### Iconos

Las reglas se representan mediante iconos en el flujo de tráfico:

	Un símbolo de filtro indica que se aplica una regla de acceso.
	La lupa indica que se aplica una regla de inspección.

	<p>Un icono de firewall en el router indica que se ha aplicado un firewall al flujo de tráfico de origen. Cisco SDM muestra un icono de firewall si se cumplen los criterios siguientes:</p> <ul style="list-style-type: none"> <li>• Existe una regla de inspección aplicada al tráfico de origen en la dirección entrante de la interfaz Desde, y una regla de acceso aplicada a la dirección entrante de la interfaz Hasta.</li> <li>• La regla de acceso en la dirección entrante de la interfaz Hasta es una regla de acceso ampliada que contiene como mínimo una entrada de regla de acceso.</li> </ul> <p>Si se ha aplicado un firewall al tráfico de vuelta, no aparece ningún icono de firewall. Si la función Firewall está disponible, pero no se ha aplicado ningún firewall al flujo de tráfico, aparecerá la indicación <b>Firewall IOS: Inactivo</b> debajo del diagrama de tráfico.</p>
	<p>Las reglas aplicadas al tráfico de origen se indican mediante una flecha hacia a la derecha. Un icono en la línea de tráfico de la interfaz de origen indica la presencia de una regla que filtra el tráfico que entra en el router. Un icono en la línea de tráfico de la interfaz Hasta indica la presencia de una regla que filtra el tráfico que sale del router. Si coloca el ratón encima de este icono, Cisco SDM mostrará los nombres de las reglas que se han aplicado.</p>
	<p>Las reglas aplicadas al tráfico de vuelta se indican mediante una flecha hacia a la izquierda. Un icono en la línea de tráfico de la interfaz Hasta indica la presencia de una regla que filtra el tráfico que entra en el router. Un icono en la línea de tráfico de la interfaz Desde indica la presencia de una regla que filtra el tráfico que sale del router. Al colocar el cursor encima de este icono, se muestran los nombres de las reglas aplicadas.</p>

  
**Nota**

Si bien los iconos se muestran en una interfaz concreta del diagrama, una política de firewall podría contener entradas de control de acceso que afecten al tráfico que no está representado por el diagrama. Por ejemplo, una entrada que contiene el icono comodín en la columna Destino (consulte [Realizar cambios a las reglas de acceso](#)) podría aplicarse al tráfico que sale de interfaces distintas de la representada por la interfaz Hasta seleccionada actualmente. El icono comodín aparece como un asterisco y representa cualquier red o host.


Para realizar cambios a una regla de acceso, consulte [Realizar cambios a las reglas de acceso](#). Para volver a la descripción de la ventana Política de firewall principal, consulte [Editar política de firewall/Lista de control de acceso](#).

## Realizar cambios a las reglas de acceso

El panel Política muestra los detalles de las reglas aplicadas al flujo de tráfico seleccionado. El panel Política se actualiza cuando se seleccionan las interfaces Desde y Hasta y cuando el diagrama de tráfico pasa del modo Tráfico de origen a Tráfico de vuelta, y viceversa.

El panel Política está vacío si se ha asociado a una interfaz una regla de acceso que no contiene ninguna entrada. Por ejemplo, si se ha asociado un nombre de regla a una interfaz mediante el CLI, pero no se han creado entradas para la regla, este panel aparecerá vacío. Si el panel Política está vacío, puede utilizar el botón **Agregar** para crear entradas para la regla.

### Campos de encabezado del área Servicio


<b>Disponibilidad de funciones del firewall</b>	Si la imagen de Cisco IOS que utiliza el router admite la función Firewall, este campo contiene el valor <b>Disponible</b> .
<b>Regla de acceso</b>	Nombre o número de la regla de acceso cuyas entradas se muestran.
<b>Regla de inspección</b>	Nombre de la regla de inspección cuyas entradas se muestran.
	Este icono aparece cuando se ha asociado una regla de acceso a una interfaz, pero no se ha creado ninguna regla de acceso con ese nombre o número. Cisco SDM le notifica que la política no tendrá ningún efecto a no ser que exista como mínimo una entrada de regla de acceso.


## Controles del área Servicio

La tabla siguiente describe los controles del área Servicio.

<b>Botón Agregar</b>	Haga clic aquí para agregar una entrada de regla de acceso. Especifique si desea agregar la entrada antes o después de la entrada seleccionada actualmente. A continuación, cree la entrada en la ventana Agregar una entrada. No olvide que el orden de las entradas es importante. Cisco SDM muestra el cuadro de diálogo Entrada ampliada cuando se agrega una entrada de la ventana Editar Política de firewall/Lista de control de acceso. Para agregar una entrada de regla estándar, vaya a <b>Tareas adicionales &gt; Editor ACL &gt; Reglas de acceso</b> .
<b>Botón Editar</b>	Haga clic para editar una entrada de regla de acceso seleccionada. A pesar de que sólo se pueden agregar entradas de reglas ampliadas en la ventana Editar política de firewall/Lista de control de acceso, no se le impide editar una entrada de regla estándar que ya se haya aplicado a una interfaz seleccionada.
<b>Botón Cortar</b>	Haga clic para eliminar una entrada de regla de acceso seleccionada. La entrada se coloca en el portapapeles y puede pegarse en otra posición de la lista, o bien, en otra regla de acceso. Si desea cambiar el orden de una entrada, puede cortarla desde una ubicación, seleccionar una entrada antes o después de la ubicación que desea para la entrada cortada y hacer clic en <b>Pegar</b> . El menú contextual Pegar permite colocar la entrada antes o después de la entrada que ha seleccionado.
<b>Botón Copiar</b>	Seleccione una entrada de regla y haga clic para colocarla en el portapapeles.
<b>Botón Pegar</b>	Haga clic para pegar una entrada del portapapeles en la regla seleccionada. Se le pedirá que especifique si desea pegar la entrada antes o después de la entrada seleccionada actualmente. Si Cisco SDM determina que ya existe una entrada idéntica en la regla de acceso, muestra la ventana Agregar una entrada de regla ampliada para que pueda modificar la entrada. Cisco SDM no permite entradas duplicadas en la misma regla de acceso.














<b>Lista desplegable de interfaces</b>	Si el flujo de tráfico seleccionado (de origen o de vuelta) contiene una regla de acceso en la interfaz Desde y en la interfaz Hasta, puede utilizar esta lista para alternar entre las dos reglas.
 Aplicar firewall	Si el flujo de tráfico seleccionado no tiene aplicado ningún firewall, seleccione tráfico de origen y haga clic en el botón Aplicar firewall para aplicarle uno. Por defecto, al hacer clic en Aplicar firewall se asociará una regla de inspección por defecto de Cisco SDM a la dirección entrante de la interfaz Desde, y una regla de acceso a la dirección entrante de la interfaz Hasta que deniegue el tráfico. Si la imagen de Cisco IOS que se ejecuta en el router no admite la función Firewall, este botón estará desactivado. Por ejemplo, para aplicar un firewall que proteja la red conectada a la interfaz <b>Ethernet 0</b> del tráfico que entra en la interfaz Ethernet 1, seleccione Ethernet 0 desde la lista desplegable <b>Desde</b> , y Ethernet 1 desde la lista desplegable <b>Hasta</b> . A continuación, haga clic en <b>Aplicar firewall</b> . Si desea aplicar un firewall que proteja la red conectada a la interfaz Ethernet 1 del tráfico que entra en la interfaz Ethernet 0, vaya a <b>Tareas adicionales &gt; Editor ACL &gt; Reglas de acceso</b> .

Los botones del área Servicio aparecen desactivados si la regla es de sólo lectura. Una regla es de sólo lectura cuando contiene una sintaxis no admitida en Cisco SDM. Las reglas de sólo lectura se indican con este icono: .

Si hay una regla estándar existente que filtra el flujo de tráfico de vuelta al cual va a aplicar el firewall, Cisco SDM le notifica que convertirá la regla de acceso estándar en una regla ampliada.

## Campos de entrada del área Servicio

La tabla siguiente describe los iconos y otros datos en las entradas del área Servicio.

Campo	Descripción	Iconos	Significado
<b>Acción</b>	Indica si se permitirá o denegará el tráfico		Permitir el tráfico de origen
			Denegar el tráfico de origen
<b>Origen/ Destino</b>	Dirección del host o de red, o cualquier host o red.		Dirección de una red
			Dirección de un host
			Cualquier red o host
<b>Servicio</b>	Tipo de servicio filtrado.		Ejemplos: TCP, EIGRP, UDP, GRE. Consulte <a href="#">Servicios IP</a> .
			Ejemplos: Telnet, http, FTP. Consulte <a href="#">Servicios TCP</a> .
			Ejemplos: SNMP, bootpc, RIP. Consulte <a href="#">Servicios UDP</a> .
			<b>IGMP</b> (Internet Group Management Protocol).
			Ejemplos: echo-reply, host-unreachable. Consulte <a href="#">Tipos de mensajes ICMP</a> .
<b>Registro</b>	Indica si se registra el tráfico denegado		Registro del tráfico denegado. Para configurar el servicio de registro para los firewalls, vea <a href="#">Registro de firewall</a> .
<b>Opción</b>	Opciones configuradas mediante el CLI.	No hay iconos.	
<b>Descripción</b>	Cualquier descripción suministrada.	No hay iconos.	

Para realizar cambios a las reglas de inspección, consulte [Realizar cambios a las reglas de inspección](#). Para volver a la descripción de la ventana Política de firewall principal, consulte [Editar política de firewall/Lista de control de acceso](#).

## Realizar cambios a las reglas de inspección

El área Aplicaciones aparece si la imagen de Cisco IOS que se ejecuta en el router admite las reglas de inspección **CBAC**. El área Aplicaciones muestra las entradas de reglas de inspección que filtran el flujo de tráfico, y se actualiza cada vez que se selecciona un nuevo flujo de tráfico. Se muestra la regla de inspección que afecta a la dirección seleccionada del tráfico.

El área Aplicaciones mostrará uno de los elementos siguientes para el **Tráfico de origen**:

- La regla de inspección que se ha aplicado a la dirección entrante de la interfaz de origen, si la hay.
- La regla de inspección que se aplica a la dirección saliente de la interfaz Hasta, si la dirección entrante de la interfaz Desde no tiene ninguna regla de inspección aplicada.

### Alternar las interfaces Desde y Hasta para hacer aparecer otras reglas en la vista

Las reglas de inspección aplicadas al **Tráfico de vuelta** no se muestran. Puede mostrar una regla de inspección aplicada al **Tráfico de vuelta** seleccionando **Alternar las interfaces Desde y Hasta** en el menú Opción Ver. En la ventana Seguridad de la aplicación de la tarea Firewall y Lista de control de acceso, puede ver también reglas de inspección que no se muestran en la ventana Editar política de firewall/Lista de control de acceso.



Este icono aparece cuando dos reglas de inspección se encuentran en la dirección de tráfico seleccionada. Cisco SDM también muestra un cuadro de diálogo de advertencia que le brinda la oportunidad de anular la asociación de una de las reglas de inspección con la interfaz.

## Controles del área Aplicación

La siguiente es una lista de controles del área Aplicación:

**Agregar:** haga clic para agregar una regla de inspección. Si no existe ninguna regla de inspección, puede agregar la que proporciona Cisco SDM por defecto, o bien, puede crear y agregar una regla de inspección personalizada. Si agrega la regla de inspección por defecto de Cisco SDM a un flujo de tráfico sin ninguna regla de inspección, se asociará al tráfico entrante en la interfaz Desde. Puede agregar una entrada para una aplicación específica tanto si existe una regla de inspección como si no.

**Editar:** haga clic para editar una entrada seleccionada.

**Eliminar:** haga clic para eliminar una entrada seleccionada.

**Configuración global:** haga clic para mostrar un cuadro de diálogo que le permita definir límites de tiempo y umbrales globales.

**Resumen:** haga clic para mostrar el nombre de protocolo o aplicación y una descripción de cada entrada.

**Detalle:** haga clic para mostrar el nombre de protocolo o aplicación, la descripción, el estado de la alerta, el estado del seguimiento de auditoría y la configuración del límite de tiempo de cada entrada.

## Campos de entrada del área Aplicación

La lista siguiente describe los campos de entrada del área Aplicación:

**Protocolo de aplicación:** muestra el nombre de la aplicación o del protocolo. Por ejemplo, **vdolive**.

**Alerta:** indica si una alerta está activada (por defecto) o desactivada.

**Seguimiento de auditoría:** indica si un seguimiento de auditoría está activado o desactivado (por defecto).

**Límite de tiempo:** muestra el tiempo, en segundos, que debe esperar el router antes de bloquear el tráfico de vuelta para este protocolo o aplicación.

**Descripción:** muestra una breve descripción. Por ejemplo, **VDOLive protocol**.

Para volver a la descripción de la ventana Política de firewall principal, consulte [Editar política de firewall/Lista de control de acceso](#).

## Agregar entrada de aplicación *nombre\_aplicación*

Utilice esta ventana para agregar una entrada de aplicación que desee que inspeccione el firewall del Cisco IOS.

### Acción de alerta

Elija una de las siguientes opciones:

- **por defecto (activado)**: deje el valor por defecto. El valor por defecto es **activado**.
- **activado**: activa la alerta.
- **desactivado**: desactiva la alerta.

### Acción de auditoría

Elija una de las siguientes opciones:

- **por defecto (desactivado)**: deje el valor por defecto. El valor por defecto es **desactivado**.
- **activado**: activa el seguimiento de auditoría.
- **desactivado**: desactiva el seguimiento de auditoría.

### Límite de tiempo

Especifique el tiempo que debe esperar el router antes de bloquear el tráfico de vuelta para este protocolo o aplicación. El campo contiene el valor por defecto del protocolo o aplicación.

## Agregar entrada de aplicación RPC

Agregue un número de programa Remote Procedure Call (RPC) en esta ventana y especifique la configuración de Alerta, Auditoría, Límite de tiempo y Tiempo de espera.

### Acción de alerta

Elija una de las siguientes opciones:

- **por defecto (activado)**: deje el valor por defecto. El valor por defecto es **activado**.
- **activado**: activa la alerta.
- **desactivado**: desactiva la alerta.

### Acción de auditoría

Elija una de las siguientes opciones:

- **por defecto (desactivado)**: deje el valor por defecto. El valor por defecto es **desactivado**.
- **activado**: activa el seguimiento de auditoría.
- **desactivado**: desactiva el seguimiento de auditoría.

### Límite de tiempo

Especifique el tiempo que debe esperar el router antes de bloquear el tráfico de vuelta para este protocolo o aplicación. El campo contiene el valor por defecto.

### Número de programa

Especifique un solo número de programa en este campo.

### Tiempo de espera

Opcionalmente, puede especificar el número de minutos durante los cuales se puede permitir el establecimiento de conexiones RPC subsiguientes entre la misma dirección de origen y el mismo puerto y dirección de destino. El tiempo de espera por defecto es de cero minutos.

## Agregar entrada de aplicación de fragmento

En esta ventana, puede agregar una entrada de fragmento a una regla de inspección que vaya a configurar en la ventana Editar política de firewall/Lista de control de acceso, así como especificar la configuración de Alerta, Auditoría y Límite de tiempo. Una entrada de fragmento establece el número máximo de paquetes no reensamblados que el router debe aceptar antes de rechazarlos.

### Acción de alerta

Elija una de las siguientes opciones:

- **por defecto (activado)**: deja el valor por defecto. El valor por defecto es **activada**.
- **activado**: activa la alerta.
- **desactivado**: desactiva la alerta.

### Acción de auditoría

Elija una de las siguientes opciones:

- **por defecto (desactivado)**: deja el valor por defecto. El valor por defecto es **desactivado**.
- **activado**: activa el seguimiento de auditoría.
- **desactivado**: desactiva el seguimiento de auditoría.

### Límite de tiempo

Especifique el tiempo que debe esperar el router antes de bloquear el tráfico de vuelta para este protocolo o aplicación. El campo contiene el valor por defecto.

### Intervalo (opcional)

Especifique el número máximo de paquetes no reensamblados que el router debe aceptar antes de rechazarlos. El intervalo puede tener un valor entre 50 y 10000.

## Agregar o editar entrada de aplicación HTTP

Utilice esta ventana para agregar una aplicación http a la regla de inspección.

### Acción de alerta

Elija una de las siguientes opciones:

- **por defecto (activado)**: deje el valor por defecto. El valor por defecto es **activado**.
- **activado**: activa la alerta.
- **desactivado**: desactiva la alerta.

### Acción de auditoría

Elija una de las siguientes opciones:

- **por defecto (desactivado)**: deje el valor por defecto. El valor por defecto es **desactivado**.
- **activado**: activa el seguimiento de auditoría.
- **desactivado**: desactiva el seguimiento de auditoría.

### Límite de tiempo

Especifique el tiempo que debe esperar el router antes de bloquear el tráfico de vuelta para este protocolo o aplicación. El campo contiene el valor por defecto.

### Descarga de host/redes para subprograma Java

Los hosts o redes de origen cuyo tráfico de subprogramas se inspeccionará. Se pueden especificar varios hosts o redes.

Haga clic en **Agregar** para mostrar la ventana Bloqueo del subprograma Java, donde puede especificar un host o una red.

Haga clic en **Eliminar** para quitar una entrada de la lista.



## Bloqueo del subprograma Java

Utilice esta ventana para especificar si se deben permitir o denegar los subprogramas Java de un determinado host o red.

### Acción

Elija una de las siguientes opciones:

- **No bloquear (Permitir):** permite los subprogramas Java de este host o esta red.
- **Bloquear (Denegar):** deniega los subprogramas Java de este host o esta red.

### Host/red

Especifique la red o el host.

### Tipo

Elija una de las siguientes opciones:

- **Una red:** si selecciona esta opción, proporcione una dirección de red en el campo Dirección IP. Tenga en cuenta que la máscara inversa permite especificar un número de red que puede indicar varias subredes.
- **Un nombre de host o dirección IP:** si selecciona esta opción, proporcione una dirección IP o nombre de host en el campo siguiente.
- **Cualquier dirección IP:** si selecciona esta opción, la acción especificada se aplica a cualquier host o red.

### Dirección IP/Máscara comodín

Especifique una dirección de red y, a continuación, la máscara inversa para indicar qué porción de la dirección de red debe coincidir exactamente.

Por ejemplo, si ha especificado la dirección de red 10.25.29.0 y la máscara inversa 0.0.0.255, se filtrará cualquier subprograma Java con una dirección de origen que contenga 10.25.29. Si la máscara inversa fuese 0.0.255.255, se filtraría cualquier subprograma Java con una dirección de origen que contenga 10.25.

### Nombre de host/IP

Este campo aparece si selecciona **Un nombre de host o dirección IP** en Tipo. Si especifica un nombre de host, asegúrese de que la red dispone de un servidor DNS capaz de resolver el nombre de host con la dirección IP correcta.

## Advertencia de Cisco SDM: Regla de inspección

Esta ventana aparece cuando Cisco SDM encuentra dos reglas de inspección que se han configurado para una dirección en un flujo de tráfico. Por ejemplo, puede que se haya aplicado una regla de inspección al tráfico entrante en la interfaz Desde, y otra al tráfico saliente en la interfaz Hasta. Dos reglas de inspección no afectarán negativamente al funcionamiento del router, pero podrían ser innecesarias. Cisco SDM le permite conservar las reglas de inspección en su estado original, quitarlas de la interfaz Desde o de la interfaz Hasta.

- **No realizar ningún cambio:** Cisco SDM no quitará ninguna regla de inspección.
- **Mantener el *nombre* de la regla de inspección en <nombre de interfaz> entrante y anular la asociación del *nombre* de la regla de inspección en <nombre de interfaz> saliente:** Cisco SDM conservará una regla de inspección y anulará la asociación de la regla con la otra interfaz.
- **Mantener el *nombre* de la regla de inspección en <nombre de interfaz> saliente y anular la asociación del *nombre* de la regla de inspección en <nombre de interfaz> entrante:** Cisco SDM conservará una regla de inspección y anulará la asociación de la regla con la otra interfaz.

Antes de seleccionar cualquier elemento y hacer clic en **Aceptar**, es conveniente que haga clic en **Cancelar** y determine si necesita agregar entradas a la regla de inspección que desea conservar. Para agregar entradas, utilice el botón **Agregar** situado en la barra de herramientas del área Aplicación de la ventana Editar Política de firewall/Lista de control de acceso.

## Advertencia de Cisco SDM: Firewall

Esta ventana aparece al hacer clic en **Aplicar firewall** en la ventana Editar política de firewall/Lista de control de acceso. Muestra las interfaces a las que se aplicará una regla y describe la regla que aplicará.

Ejemplo:

```
SDM aplicará la configuración de firewall a las interfaces siguientes:  
Interfaz interna (fiable): FastEthernet 0/0  
* Aplique la regla de inspección SDM por defecto entrante.  
* Aplique la lista de control de acceso entrante. (Anti-spoofing,  
difusión, retrobuclé local, etc.).
```

Interfaz externa (no fiable): Serie 1/0

\* Aplique la lista de acceso entrante para denegar el tráfico de vuelta.

Haga clic en **Aceptar** para aceptar estos cambios, o haga clic en **Cancelar** para detener la aplicación del firewall.

## Editar política de firewall

La ventana Editar política de firewall proporciona una visualización gráfica de las políticas de firewall en el router y permite agregar ACL a políticas sin salir de la ventana. Lea los procedimientos en las secciones que se indican a continuación para conocer cómo ver la información en esta ventana y agregar reglas.

### Acciones que debe realizar antes de ver la información en esta ventana

Esta ventana está vacía si no se ha configurado [zona](#), [par de zonas](#) o [mapa de política](#). Para crear una configuración básica que contenga estos elementos, vaya a **Configurar > Firewall y Lista de control de acceso > Crear firewall** y complete el asistente para Firewall avanzado. Después de esta acción, puede crear zonas adicionales, pares de zonas y políticas, cuando sea necesario, en **Configurar > Tareas adicionales > Zonas** para configurar zonas y en **Tareas adicionales > Pares de zonas** para configurar pares de zonas adicionales. Para crear los mapas de política que van a usar los pares de zonas, vaya a **Configurar > Tareas adicionales > C3PL**. Haga clic en la rama **Mapa de política** para mostrar ramas adicionales que permitan crear mapas de política y los mapas de clase que definen el tráfico para los mapas de política.

### Expandir y contraer la visualización de una política

Cuando se contrae la visualización de una política, sólo se muestra el nombre de la política, zona de origen y de destino. Para expandir la visualización de la política con el fin de mostrar las reglas que componen la política, haga clic en el botón + a la izquierda del nombre de la política. Una vista expandida de una política de firewall se podría ver de la siguiente manera:

ID	Clasificación de tráfico			Acción	Opciones de regla
	Origen	Destino	Servicio		
política de clientes y servidores (clientes a servidores)					
1	Cualquiera	Cualquiera	tcp	Permitir firewall	
			udp		
			icmp		
2	Tráfico sin coincidencias			Rechazar	

La política de clientes y servidores con nombre de política contiene dos [ACL](#). La regla con ID 1 permite el tráfico [TCP](#), [UDP](#) y [ICMP](#) desde cualquier origen a cualquier destino. La regla con ID 2 rechaza cualquier tráfico sin coincidencias.

### Agregar una nueva regla a una política

Para agregar una nueva regla a una política, siga estos pasos:

- 
- Paso 1** Haga clic en cualquier lugar de la pantalla correspondiente a esa política y después en el botón + **Agregar**.
- Para insertar una regla para tráfico nuevo en el orden que desea que seleccione una regla existente, haga clic en el botón + **Agregar** y seleccione **Insertar** o **Insertar después**. Las opciones Insertar e Insertar después están disponibles también en un menú contextual que se muestra al hacer clic con el botón derecho del mouse en una regla existente.
  - Seleccionar **Regla para nuevo tráfico** coloca automáticamente a la nueva regla en la parte superior de la lista.
  - Seleccionar **Regla para tráfico existente** le permite seleccionar un mapa de clase existente y modificarlo. Esto coloca automáticamente a la nueva regla en la parte superior de la lista.
- Paso 2** Complete el cuadro de diálogo que se muestra. Para obtener más información, haga clic en [Agregar una nueva regla](#).
-

## Reordenar reglas dentro de una política

Si una política contiene más de una regla que permite tráfico, puede reordenarla al seleccionar una regla y hacer clic en el botón **Desplazar hacia arriba** o en el botón **Desplazar hacia abajo**. El botón Desplazar hacia arriba está desactivado si selecciona una regla que ya está en la parte superior de la lista o si selecciona la regla Tráfico sin coincidencias. El botón Desplazar hacia abajo está desactivado si selecciona una regla que ya está en la parte inferior de la lista.

También puede utilizar los botones Cortar y Pegar para reordenar reglas. Para eliminar una regla de su posición actual, selecciónela y haga clic en **Cortar**. Para colocar la regla en una nueva posición, seleccione una regla existente, haga clic en **Pegar** y seleccione **Pegar** o **Pegar después**.

Las operaciones Desplazar hacia arriba, Desplazar hacia abajo, Cortar, Pegar y Pegar después están disponibles también en un menú contextual que se muestra al hacer clic con el botón derecho del mouse en una regla.

## Copiar y pegar una regla

Copiar y pegar una regla es muy útil si una política contiene una regla que se puede utilizar con pocas modificaciones o con ninguna modificación en otra política.

Para copiar una regla, selecciónela y haga clic en el botón **Copiar** o haga clic con el botón derecho en la regla y seleccione **Copiar**. Para pegar la regla en una nueva ubicación, haga clic en **Pegar** y seleccione **Pegar** o **Pegar después**. Los botones Pegar y Pegar después también están disponibles en el menú contextual. Cuando pega una regla en una nueva ubicación, se muestra el cuadro de diálogo [Agregar una nueva regla](#) para que realice cambios a la regla si es necesario.

## Mostrar el diagrama de flujo de reglas

Haga clic en cualquier lugar de una política de firewall y, a continuación, en Diagrama de regla para mostrar el Diagrama de flujo de reglas para esa política. El Diagrama de flujo de reglas muestra la zona de origen al lado derecho del icono del router, y la zona de destino al lado izquierdo del icono.

## Aplicar los cambios

Para enviar los cambios al router, haga clic en **Aplicar cambios** al final de la pantalla.

## Descartar los cambios

Para descartar los cambios que realizó, pero que no envió al router, haga clic en **Descartar cambios** al final de la pantalla.

## Agregar una nueva regla

Defina un flujo de tráfico y especifique protocolos para inspeccionar en la ventana Agregar una regla. Para agregar una nueva regla, siga estos pasos.

- 
- Paso 1** En el campo Origen y Destino, especifique que el tráfico fluye entre una red y otra, seleccionando **Red**, o que el tráfico fluye entre entidades que pueden ser redes o que pueden ser hosts individuales, seleccionando **Cualquiera**.
  - Paso 2** Especifique un nombre para el flujo de tráfico en el campo Nombre de tráfico.
  - Paso 3** Haga clic en **Agregar** junto a las columnas Red de origen y Red de destino, y agregue direcciones de red de origen y destino. Puede agregar múltiples entradas para las redes de origen y destino, y puede editar una entrada existente si la selecciona y hace clic en **Editar**.
  - Paso 4** Reordene cualquier entrada, cuando sea necesario, seleccionándola y haciendo clic en **Desplazar hacia arriba** o **Desplazar hacia abajo**. El botón Desplazar hacia arriba está desactivado cuando la entrada seleccionada ya está en la parte superior de la lista. El botón Desplazar hacia abajo está desactivado cuando la entrada seleccionada ya está en la parte inferior de la lista.
  - Paso 5** En el campo Nombre de servicio, especifique un nombre que describa los protocolos o servicios que está identificando para inspección.
  - Paso 6** Para agregar un servicio, haga clic en una rama del árbol en la columna de la izquierda, seleccione el servicio y haga clic en **Agregar>>**. Haga clic en el icono + junto a una rama para mostrar los servicios disponibles de ese tipo. Para eliminar un servicio de la columna derecha, selecciónelo y haga clic en **<<Eliminar**.

- Paso 7** Especifique cómo desea que se maneje el tráfico. Para esto, seleccione **Permitir firewall**, **Permitir lista de control de acceso** o **Rechazar** en el campo Acción. Si selecciona **Permitir firewall**, puede hacer clic en Avanzado y seleccionar un elemento de menú para definir la acción, como, por ejemplo, inspeccionar los protocolos que seleccionó en la casilla de servicio. Para obtener más información, consulte los temas de ayuda:
- [Inspección de aplicación](#)
  - [Filtro URL](#)
  - [Calidad de servicio \(QoS\)](#)
  - [Parámetro de inspección](#)
- Paso 8** Si especificó **Rechazar** como la acción, puede hacer clic en **Registrar** para registrar el evento.
- Paso 9** Haga clic en Aceptar para cerrar este cuadro de diálogo y enviar los cambios al a router.
- 

## Agregar tráfico

Utilice el cuadro de diálogo Add Traffic para crear una entrada de dirección de origen y destino para una regla.

### Acción

Utilice las opciones Incluir o Excluir para especificar si desea que la regla se aplique al tráfico intercambiado entre las direcciones de origen y destino.

Seleccione **Incluir** para incluir este tráfico en la regla.

Seleccione **Excluir** para que este tráfico se excluya de la regla.

## Host/red de origen y Host/red de destino

Especifique el origen y el destino del tráfico en estos campos.

### Tipo

Elija uno de los valores siguientes:

- Cualquier dirección IP: seleccione esta opción si no desea limitar el tráfico de origen y destino a ningún host o dirección.
- Una red: seleccione esta opción para especificar una dirección de red como el origen o el destino, y especifique la dirección de red en los campos Dirección IP y Máscara comodín.
- Nombre o dirección IP de un host: seleccione esta opción para especificar el nombre o la dirección IP de un host. Después, especifique el host en el campo Nombre de host/IP.

### Dirección IP

Especifique la dirección de la red. Este campo se muestra cuando selecciona **Una red** en el campo Tipo.

### Máscara comodín

Introduzca la máscara comodín que especifica los bits que se usan para la dirección de red. Por ejemplo, si la dirección de red es 192.168.3.0, especifique 0.0.0.255 como la máscara. Este campo se muestra cuando selecciona **Una red** en el campo Tipo.

### Nombre de host/IP

Especifique el nombre o la dirección IP de un host en este campo: Si especifica un nombre, el router debe estar activado para contactar a un servidor DNS para poder resolver el nombre como una dirección IP. Este campo se muestra cuando selecciona Un nombre de host o dirección IP en el campo Tipo.



## Inspección de aplicación

Configure la inspección profunda de paquetes para cualquiera de las aplicaciones o protocolos que se indican en esta pantalla. Para esto, haga clic en la casilla junto a la aplicación o al protocolo, haga clic en el botón a la derecha del campo y especifique **Crear** o **Seleccionar** en el menú contextual. Seleccione **Crear** para configurar un nuevo mapa de política. Especifique **Seleccionar** para aplicar un mapa de política existente al tráfico. El nombre del mapa de política aparece en el campo al terminar.

Por ejemplo, para crear un nuevo mapa de política para Mensajería instantánea, marque la casilla junto a IM, haga clic en el botón junto al campo IM y seleccione **Crear**. A continuación, cree el mapa de política en el cuadro de diálogo Configurar inspección profunda de paquetes.

## Filtro URL

Para agregar un filtro URL, seleccione un filtro URL existente en la lista Nombre de filtro de URL o haga clic en **Crear nuevo**; se muestra el cuadro de diálogo Nuevo filtro URL. La configuración del filtro URL que seleccionó o creó se resume en este cuadro de diálogo.

## Calidad de servicio (QoS)

Puede rechazar el tráfico que supere una velocidad por segundo especificada, la [velocidad de supervisión](#), y rechazar el tráfico que supere un valor de ráfaga especificado. La velocidad de supervisión puede ser un valor entre 8.000 y 2.000.000.000 bits por segundo. La [velocidad de ráfaga](#) puede ser un valor entre 1.000 y 512.000.000 bytes.

## Parámetro de inspección

Especifique un [mapa de parámetro](#) existente en la ventana Parámetro de inspección. Para esto, seleccione un mapa de parámetro en la lista Mapa de parámetro de inspección o haga clic en **Crear nuevo** para crear un nuevo mapa de parámetro para aplicar a la regla de la política que está modificando. Los detalles del mapa de parámetro que especifica se muestran en la casilla Vista previa.

Para obtener más información sobre los mapas de parámetro, haga clic en [Tiempos de inactividad y umbrales para mapas de parámetros de inspección y CBAC](#).

## Seleccionar tráfico

Seleccione un mapa de clase que especifique el tráfico que desea agregar a la política. Para ver más información sobre un mapa de clase específico, seleccione el mapa de clase y haga clic en **Ver detalles**.

Cuando hace clic en **Aceptar**, se muestra el cuadro de diálogo Agregar una nueva regla, con la información en el mapa de clase que selecciona. Puede realizar cambios adicionales al mapa de clase o dejarlo como está. Si realiza cambios, puede cambiar el nombre del mapa de clase si no desea que los cambios se apliquen a otras políticas que usan el mapa de clase original.

## Eliminar regla

Este cuadro de diálogo se muestra cuando elimina una regla que contiene un [mapa de clase](#) o una [ACL](#), que es posible que desee eliminar junto con la regla o conservarlos para uso en otras reglas.

### Eliminar automáticamente los mapas de clase y las ACL utilizados por esta regla

Haga clic en esta opción para eliminar los mapas de clase y las ACL que son parte de esta regla. Se eliminarán de la configuración de router y no estarán disponibles para uso en otras reglas.

### Eliminaré más tarde los mapas de clase y ACL no utilizados

Haga clic en esta opción para eliminar la regla, reteniendo los mapas de clase y las ACL. Puede conservarlos para usarlos en otras partes de la configuración del firewall.

## Ver detalles

Haga clic en **Ver detalles** para mostrar los nombres de los mapas de clase y las ACL relacionadas con la regla que está eliminando. El cuadro de diálogo se expande para mostrar los detalles. Cuando hace clic en Ver detalles, el nombre del botón pasa a ser Ocultar detalles.

## Ocultar detalles

Haga clic en **Ocultar detalles** para cerrar la sección de detalles del cuadro de diálogo. Cuando hace clic en Ocultar detalles, el nombre del botón pasa a ser Ver detalles.

## Eliminación manual de mapas de clase

Para eliminar manualmente un mapa de clase, siga estos pasos.

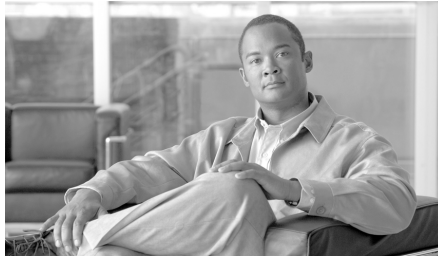
- 
- Paso 1** Vaya a **Configurar > Tareas adicionales > C3PL > Mapas de clase**.
  - Paso 2** Haga clic en el nodo del tipo de mapa de clase que está eliminando.
  - Paso 3** Seleccione el nombre del mapa de clase que se mostró en la ventana Ver detalles y haga clic en **Eliminar**.
- 

## Eliminación manual de listas de control de acceso

Para eliminar manualmente una lista de control de acceso, siga estos pasos.

- 
- Paso 1** Vaya a **Configurar > Tareas adicionales > Editor ACL**.
  - Paso 2** Haga clic en el nodo del tipo de ACL que está eliminando.
  - Paso 3** Seleccione el nombre o número de la ACL que se mostró en la ventana Ver detalles y haga clic en **Eliminar**.
-





## CAPÍTULO 8

# Seguridad de la Aplicación

---

La seguridad de la aplicación le permite a usted crear políticas de seguridad para gestionar el uso de la red y de las aplicaciones de la Web. Usted puede aplicar las políticas que crea para las interfaces específicas, a fin de duplicar una política existente para forzar las configuraciones de una nueva política, y para quitar las políticas del router.

Este capítulo contiene las secciones siguientes:

- [Ventanas de Seguridad de la Aplicación](#)
- [Ninguna Política de Seguridad de la Aplicación](#)
- [Correo electrónico](#)
- [Mensajería Instantánea](#)
- [Aplicaciones Par-a-Par](#)
- [Filtrado de URL](#)
- [HTTP](#)
- [Aplicaciones y Protocolos](#)
- [Tiempos de inactividad y umbrales para mapas de parámetros de inspección y CBAC](#)

# Ventanas de Seguridad de la Aplicación

Los controles en las ventanas de seguridad de la aplicación le permiten asociar políticas a las interfaces, hacer configuraciones globales, agregar, eliminar y duplicar las políticas de seguridad de la aplicación. Los botones de seguridad de la aplicación le permiten navegar rápidamente al área de seguridad de la aplicación en la cual usted necesita realizar cambios.

## Lista del Nombre de la Política

Seleccione la política que desee modificar de esta lista. Si no hay políticas configuradas, esta lista está vacía, y la ventana de seguridad de la aplicación mostrará un mensaje que indicará que ninguna política está disponible en el router. Para crear una política, haga clic en el botón **Acción** y elija **Agregar**.

## Botones de Seguridad de la Aplicación

- Botón **Acción**: haga clic para agregar una política, eliminar la política elegida, o duplicar la política elegida. Si no se configura ninguna política en el router, **Agregar** será la única acción disponible.
- Botón **Asociar**: haga clic para mostrar un diálogo que le permita asociar la política a una interfaz. El diálogo permite elegir la interfaz y especificar la dirección del tráfico a la cual se aplica la política.
- Botón **Configuración global**: haga clic para configurar los valores de tiempos de inactividad y umbrales que se aplican a todas las políticas. Haga clic en Configuración global para obtener más información.

## Botón de correo electrónico

Haga clic para realizar cambios en la configuración de seguridad de la aplicación de correo electrónico. Para obtener más información, haga clic en [Correo electrónico](#).

## Botón de Mensajería Instantánea

Haga clic para realizar cambios en la configuración de seguridad de Yahoo Messenger, MSN Messenger, y otras aplicaciones de mensajería instantánea. Para obtener más información, haga clic en [Mensajería Instantánea](#).

### Botón de Par-a-Par

Haga clic para realizar cambios en la configuración de seguridad de KaZaA, eDonkey y otras aplicaciones Par-a-Par. Para obtener más información, haga clic en [Aplicaciones y Protocolos](#).

### Botón de Filtrado de URL

Haga clic para agregar una lista de direcciones URL que desea filtrar mediante la política de seguridad de la aplicación. También puede agregar servidores de filtrado.

### Botón de HTTP

Haga clic para realizar cambios en la configuración de seguridad de HTTP. Para obtener más información, haga clic en [HTTP](#).

### Botón de Aplicaciones y Protocolos

Haga clic para realizar cambios en la configuración de seguridad de otras aplicaciones y protocolos. Para obtener más información, haga clic en [Aplicaciones y Protocolos](#).

## Ninguna Política de Seguridad de la Aplicación

Cisco SDM muestra esta ventana después de hacer clic en la ficha **Seguridad de la Aplicación**, pero no se ha configurado ninguna política de seguridad de la aplicación en el router. Usted puede crear una política desde esta ventana, y ver las configuraciones globales que proporcionan los valores por defecto para los parámetros que usted pueda fijar cuando cree las políticas.

### Nombre de La Política

Está vacía cuando no se ha configurado ninguna política para el router. Elegir Agregar del menú de contexto de Acción le permitirá crear un nombre de la política y comenzar a hacer las configuraciones a la política.

## Acción

Si no se ha configurado ninguna política en el router, podrá elegir **Agregar** del menú contextual para crear una política. Una vez configurada una política, las otras acciones, **Editar** y **Eliminar**, están disponibles.

## Asociar

Si no se configura ninguna política, este botón estará desactivado. Una vez creada una política, podrá hacer clic en este botón para asociar la política a una interfaz. Consulte el apartado [Asociar Política con una Interfaz](#) para obtener más información.

## Configuración global

La configuración global proporciona los límites de tiempo, umbrales y otros valores por defecto para los parámetros de las políticas. Cisco SDM proporciona los valores por defecto para cada parámetro, y usted puede cambiar cada valor para definir un nuevo valor por defecto que se aplicará a menos que se sustituya para una aplicación o un protocolo específico. Cuando usted está creando una política, podrá aceptar el valor por defecto para un parámetro particular, o elegir otra configuración. Debido a que las ventanas de configuración de seguridad de la aplicación no muestran los valores por defecto, usted deberá hacer clic en este botón para verlos en la ventana de tiempos de inactividad globales y umbrales. Consulte el apartado [Tiempos de inactividad y umbrales para mapas de parámetros de inspección y CBAC](#) para obtener más información.

# Correo electrónico

Especifique las aplicaciones de correo electrónico que desee inspeccionar en esta ventana. Para aprender sobre los botones y cajones disponibles en la ficha Seguridad de la Aplicación, haga clic en [Ventanas de Seguridad de la Aplicación](#).

## Botón Editar

Haga clic en este botón para editar las configuraciones de la aplicación elegida. Las configuraciones que se crean sustituyen a las configuraciones globales establecidas en el router.



## Columna de aplicaciones

El nombre de la aplicación de correo electrónico, por ejemplo, *bliff*, *esmtip* y *smtip*. Para editar la configuración de una aplicación, marque la casilla situada a la izquierda del nombre de la aplicación y haga clic en **Editar**.

## Columnas de Alertas, Auditoría y Tiempo De Inactividad

Estas columnas muestran los valores que han sido establecidos explícitamente para una aplicación. Si una configuración no se ha cambiado para una aplicación, la columna quedará vacía. Por ejemplo, si se ha activado auditar para la aplicación del bliff, pero no se han realizado cambios a la alerta o a las configuraciones de tiempo de inactividad, el valor de *inicio* se mostrará en la columna **Auditoría**, pero las columnas **Alerta** y **Tiempo de inactividad** quedarán en blanco.

## Columna de opciones

Esta columna puede incluir campos si existen otras configuraciones para la aplicación elegida.

### Campo Datos Máximos

Especifica el número máximo de bytes (datos) que se pueden transferir en una sola sesión del Protocolo de Transporte de Correo Simple (SMTP, Simple Mail Transport Protocol). Después de que se exceda el valor máximo, el firewall mostrará un mensaje de advertencia y cerrará la sesión. Valor por defecto: 20 MB.

### Casilla de verificación Inicio de sesión seguro

Causa que un usuario en una ubicación no segura use encriptación para autenticación.

### Reiniciar

Reinicia la conexión TCP si el cliente introduce un comando sin protocolo antes de que se complete la autenticación.

### Tráfico del Router

Activa la inspección de tráfico destinada a u originada por un router. Aplicable solamente para H.323, TCP, y protocolos de UDP.

# Mensajería Instantánea

Use esta ventana para controlar el tráfico de las aplicaciones de mensajería instantánea (IM, Instant Messaging) tales como Yahoo Messenger y MSN Messenger. Para aprender sobre los botones y cajones disponibles en la ficha Seguridad de la aplicación, haga clic en [Ventanas de Seguridad de la Aplicación](#).

Haga clic en [Controles Permitir, Bloquear y Alerta](#) para aprender cómo especificar la acción que el router deberá tomar cuando encuentre tráfico con las características especificadas en esta ventana.

El ejemplo siguiente muestra el tráfico bloqueado para el tráfico de Yahoo Messenger, y las alarmas generadas cuando el tráfico de esa aplicación llega a:

Yahoo Messenger      Bloquear      Enviar Alarma (marcado)

El perfil SDM\_HIGH bloquea las aplicaciones de IM. Si el router usa el perfil SDM\_HIGH, y no bloquea las aplicaciones de IM, esas aplicaciones pudieron haberse conectado a un servidor nuevo que no está especificado en el perfil. Para activar el router para que bloquee estas aplicaciones, marque la casilla de verificación **Enviar alarma** situada al lado de las aplicaciones de IM para descubrir los nombres de los servidores con los cuales se conectan las aplicaciones. Luego use el CLI para bloquear el tráfico de estos servidores. El ejemplo siguiente usa el nombre del servidor newserver.yahoo.com:

```
Router(config)# appfw policy-name SDM_HIGH
Router(cfg-appfw-policy)# application im yahoo
Router(cfg-appfw-policy-ymsgr)# server deny name newserver.yahoo.com
Router(cfg-appfw-policy-ymsgr)# exit
Router(cfg-appfw-policy)# exit
Router(config)#
```



## Nota

- Las aplicaciones de IM pueden comunicarse sobre puertos de protocolo no nativos, tales como HTTP, así como a través de sus puertos nativos de TCP y UDP. Cisco SDM configura las acciones de bloquear y permitir basadas en el puerto nativo para la aplicación, y siempre bloquea la comunicación conducida sobre los puertos HTTP.
- Algunas aplicaciones de IM, tales como MSN Messenger 7.0, usan los puertos de HTTP por defecto. Para permitir estas aplicaciones, configure la aplicación de IM para usar su puerto nativo.

# Aplicaciones Par-a-Par

Esta página permite crear las configuraciones de las políticas para aplicaciones Par-a-Par, tales como Gnutella, BitTorrent y eDonkey. Para aprender sobre los botones y cajones disponibles en la ficha Seguridad de la Aplicación, haga clic en [Ventanas de Seguridad de la Aplicación](#).

Haga clic en [Controles Permitir, Bloquear y Alerta](#) para aprender cómo especificar la acción que el router deberá tomar cuando encuentre tráfico con las características especificadas en esta ventana.

El ejemplo siguiente muestra el tráfico bloqueado para el tráfico de BitTorrent, y las alarmas generadas cuando llega el tráfico de esa aplicación.

## **Ejemplo 8-1 Bloqueo de tráfico de BitTorrent**

BitTorrent                      Bloquear



### **Nota**

- Las aplicaciones Par-a-Par pueden comunicarse sobre puertos de protocolo no nativos, tal como HTTP, así como a través de sus puertos nativos de TCP y UDP. Cisco SDM configura las acciones de bloquear y permitir basadas en el puerto nativo para la aplicación, y siempre bloquea la comunicación conducida sobre los puertos HTTP.
- Las políticas de seguridad de la aplicación no bloquearán los archivos si están siendo proporcionados por un servicio de pago tal como altnet.com. Los archivos descargados de redes de punto a punto serán bloqueados.

# Filtrado de URL

El filtrado de URL permite controlar el acceso de los usuarios a los sitios Web de Internet mediante listas de direcciones URL. En estas listas se puede especificar si una URL tiene o no permiso. Para incluir capacidades de filtrado URL en la política de seguridad de la aplicación, haga clic en **Activar filtrado de URL** en esta ventana.

Puede configurar una lista de direcciones URL local en el router para utilizarla en todas las políticas de seguridad de la aplicación. Las listas de direcciones URL también se pueden almacenar en servidores de filtro de URL a los que se puede conectar el router. La información de estos servidores se almacena en una lista de servidores de filtro de URL. Puede configurar una lista de servidores de filtro de URL en el router para utilizarla en todas las políticas de seguridad de la aplicación.

La lista de direcciones URL local se puede mantener en esta ventana mediante los botones **Agregar URL**, **Editar URL** e **Importar lista de URL**. Puesto que el software Cisco IOS puede mantener estas listas con o sin una política de seguridad de la aplicación configurada, también puede actualizar estas listas en la ventana Tareas adicionales.

Para aprender cómo mantener una lista de direcciones URL local, haga clic en [Lista de URL local](#).

Para aprender cómo mantener una lista de servidores de filtro de URL, haga clic en [Servidores de filtro de URL](#).

Para obtener información sobre cómo utiliza el router una lista de direcciones URL local junto con las listas de direcciones URL de servidores de filtro de URL, haga clic en [Preferencia del filtrado de URL](#).

Para obtener información general acerca del filtrado de URL, haga clic en [Ventana de filtrado de URL](#).

## HTTP

Especifica las configuraciones generales para la inspección del tráfico de HTTP en esta ventana. Para aprender sobre los botones y cajones disponibles en la ficha Seguridad de la Aplicación, haga clic en [Ventanas de Seguridad de la Aplicación](#).

Haga clic en [Controles Permitir, Bloquear y Alerta](#) para aprender cómo especificar la acción que el router deberá tomar cuando encuentre tráfico con las características especificadas en esta ventana.

Para obtener información más detallada sobre cómo el router puede inspeccionar el tráfico de HTTP, consulte *HTTP Inspection Engine* en el vínculo siguiente:

[http://www.cisco.com/en/US/products/ps6350/products\\_configuration\\_guide\\_chapter09186a0080455acb.html](http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455acb.html)

### Casilla de verificación Detectar Tráfico HTTP No Compatible

Marque esta casilla si desea que Cisco SDM examine si en el tráfico HTTP hay paquetes que no cumplan con el protocolo HTTP. Use los controles Permitir, Bloquear y Alarma para especificar la acción que el router debe tomar cuando se encuentre este tipo de tráfico.

**Nota**

Bloquear el tráfico HTTP no compatible puede causar que el router descarte el tráfico de los sitios Web populares que no se pudieron bloquear en base al contenido, si esos sitios Web no son compatibles con el protocolo HTTP.

### Casilla de verificación Detectar aplicaciones de arquitectura de túneles

Marque esta casilla si desea que Cisco SDM examine el tráfico HTTP para los paquetes generados por las aplicaciones de arquitectura de túneles. Use los controles Permitir, Bloquear y Alarma para especificar la acción que Cisco SDM debe realizar cuando se encuentre con este tipo de tráfico.

### Casilla de verificación Fijar la inspección de la longitud máxima del URI

Marque esta casilla si desea definir una longitud máxima para los Indicadores de Recursos Universales (URIs, Universal Resource Indicators). Especifique la longitud máxima en bytes y, luego, use los controles Permitir, Bloquear y Alarma para especificar la acción que el router deberá tomar cuando se encuentre una URL que sea más larga que este valor.

### Casilla de verificación Activar la inspección de HTTP

Marque esta casilla si desea que el router inspeccione el tráfico HTTP. Si desea bloquear el tráfico de las aplicaciones de Java, podrá especificar un filtro de bloqueo de Java al hacer clic en el botón ... y al especificar una ACL existente, o al crear nueva ACL para la inspección de Java.

### Casilla de verificación Activar la inspección de HTTPS

Marque esta casilla si desea que el router inspeccione el tráfico HTTPS.

### Casilla de verificación Fijar el valor del tiempo de Inactividad

Marque esta casilla si desea fijar un límite de tiempo para las sesiones HTTP, e introduzca el número de segundos en el campo Límite de tiempo. Se cerrarán las sesiones que excedan a esta cantidad de tiempo.

### Activar la prueba de auditoría

Usted puede hacer las configuraciones de la prueba de auditoría de CBAC para el tráfico de HTTP que sustituya a las configuraciones en la ventana de tiempos de Inactividad globales y de los umbrales. Un valor **por defecto** significa que se usará la configuración global actual. **Activado** activa explícitamente el seguimiento retrospectivo del CBAC para el tráfico HTTP y para el tráfico HTTPS si se activa la inspección de HTTPS, y se sustituye la configuración global de la prueba de auditoría. **Desactivado** desactiva explícitamente el seguimiento retrospectivo del CBAC para el tráfico HTTP y para el tráfico HTTPS si se activa la inspección de HTTPS, y se sustituye la configuración global de la prueba de auditoría.

## Opciones del encabezado

Usted puede hacer que el router permita o niegue el tráfico que se base en el tamaño del encabezado de HTTP y el método de solicitud contenido en el encabezado. Los métodos de solicitud son los comandos enviados a los servidores de HTTP para retomar URLs, páginas Web, y realizar otras acciones. Para aprender sobre los botones y cajones disponibles en la ficha Seguridad de la Aplicación, haga clic en [Ventanas de Seguridad de la Aplicación](#).

### Casilla de verificación Fijar el tamaño máximo del encabezado

Marque esta casilla si desea que el router permita o deniegue el tráfico que se base en el tamaño del encabezado HTTP, y especifique el tamaño máximo del encabezado de solicitud y de respuesta. Use los controles **Permitir**, **Bloquear** y **Alarma** para especificar la acción que el router deberá tomar cuando el tamaño del encabezado exceda estas longitudes.

## Casillas de verificación del Método de Solicitud de Extensión

Si desea que el router permita o deniegue el tráfico HTTP que se base en un método de solicitud de extensión, marque la casilla situada al lado de ese método de solicitud. Use los controles **Permitir**, **Bloquear** y **Alarma** para especificar la acción que el router deberá tomar cuando encuentre tráfico que use ese método de solicitud.

## Casillas de verificación Configurar el método de solicitud del RFC

Si desea que el router permita o deniegue el tráfico HTTP que se base en uno de los métodos de solicitud HTTP especificados en RFC 2616, *Protocolo para Transferencia de Hipertexto—HTTP/1.1*, marque la casilla situada al lado de ese método de solicitud. Use los controles **Permitir**, **Bloquear** y **Alarma** para especificar la acción que el router deberá tomar cuando encuentre tráfico que use ese método de solicitud.

## Opciones del contenido

Usted puede hacer que el router examine el contenido del tráfico de HTTP y permitir o bloquear tráfico, y generar alarmas basadas en cosas que usted haga y que el router verifica. Para aprender sobre los botones y cajones disponibles en la ficha Seguridad de la Aplicación, haga clic en [Ventanas de Seguridad de la Aplicación](#).

Haga clic en [Controles Permitir, Bloquear y Alerta](#) para aprender cómo especificar la acción que el router deberá tomar cuando encuentre tráfico con las características especificadas en esta ventana.

## Casilla de verificación Verificar el tipo de contenido

Marque esta casilla si desea que el router verifique el contenido de los paquetes HTTP al hacer corresponder la respuesta con la solicitud, al activar una alarma para tipos de contenido desconocidos, o al usar los dos métodos anteriores. Use los controles Permitir, Bloquear y Alarma para especificar la acción que el router deberá tomar cuando las solicitudes no puedan corresponder con las respuestas, y cuando encuentre un tipo de contenido desconocido.

**Casilla de verificación Fijar el tamaño del contenido**

Marque esta casilla para fijar un tamaño mínimo y máximo para los datos en un paquete de HTTP, e introduzca los valores en los campos proporcionados. Use los controles Permitir, Bloquear y Alarma para especificar la acción que el router deberá tomar cuando la cantidad de datos caiga por debajo del tamaño mínimo o cuando exceda el tamaño máximo.

**Casilla de verificación Configurar codificación de transferencia**

Marque esta casilla para hacer que el router verifique cómo se codifican los datos en el paquete. Use los controles Permitir, Bloquear y Alarma para especificar la acción que el router deberá tomar cuando encuentre las codificaciones de transferencia que elija.

**Casilla de verificación Trozos**

El formato de codificación especificado en RFC 2616, Protocolo para Transferencia de Hipertexto—HTTP/1. El cuerpo del mensaje se transfiere en una serie de trozos; cada trozo contiene su propio indicador de tamaño.

**Casilla de verificación Comprimir**

El formato de codificación producido por la utilidad de “comprimir” de UNIX.

**Casilla de verificación Desvalorar**

El formato de “ZLIB” definido en RFC 1950, Especificación del Formato de Datos Comprimidos ZLIB, versión 3.3, combinado con un mecanismo de compresión para “desvalorar” descrito en RFC 1951, Especificación del Formato de Datos Comprimidos para DESVALORAR, versión 1.3.

**Casilla de verificación Gzip**

El formato de codificación producido por el programa GNU zip (“gzip”).

**Casilla de verificación Identidad**

Codificación de un valor por defecto que indica que no se ha realizado ninguna codificación.



# Aplicaciones y Protocolos

Esta ventana le permite crear las configuraciones de políticas para las aplicaciones y protocolos que no se encuentren en las otras ventanas. Para aprender sobre los botones y cajones disponibles en la ficha Seguridad de la Aplicación, haga clic en [Ventanas de Seguridad de la Aplicación](#).

## Árbol de Aplicaciones y Protocolos

El árbol de aplicaciones y protocolos le permite filtrar la lista a la derecha de acuerdo al tipo de aplicaciones y protocolos que usted quiera ver. Primero elija la rama para el tipo general que desee mostrar. El marco a la derecha muestra los artículos disponibles para el tipo que usted elija. Si un símbolo de sumar (+) aparece a la izquierda de la rama, hay subcategorías que usted puede usar para refinar el filtro. Haga clic en el símbolo de + para expandir la rama y después seleccionar la subcategoría que usted desee mostrar. Si la lista a la derecha está vacía, no hay aplicaciones o protocolos disponibles para ese tipo. Para elegir una aplicación, usted podrá marcar la casilla al lado de ella en el árbol, o podrá marcar la caja al lado de ella en la lista.

Ejemplo: Si desea mostrar todas las aplicaciones de Cisco, haga clic en la carpeta de la rama **Aplicaciones** y, luego, haga clic en la carpeta **Cisco**. Verá aplicaciones como *clp*, *cisco-net-mgmt* y *cisco-sys*.

## Botón Editar

Haga clic en este botón para editar las configuraciones de la aplicación elegida. Las configuraciones que usted haga sustituirán las configuraciones globales configuradas en la router.

## Columna de aplicaciones

El nombre de la aplicación o del protocolo, por ejemplo, *tcp*, *smtp*, or *ms-sna*. Para editar la configuración de una aplicación, marque la casilla situada a la izquierda del nombre de la aplicación y haga clic en **Editar**.

## Columnas de Alertas, Auditoría y Tiempo De Inactividad

Estas columnas muestran los valores que han sido establecidos explícitamente para una aplicación. Si una configuración no se ha cambiado para una aplicación, la columna quedará vacía. Por ejemplo, si se ha activado auditar para la aplicación de ms-sna, pero no se han realizado cambios a la alerta o a las configuraciones de tiempo de inactividad, el valor de *inicio* se mostrará en la columna **Auditoría**, pero las columnas **Alerta** y **Tiempo De Inactividad** quedarán en blanco.

## Columna de opciones

Esta columna puede incluir campos si existen otras configuraciones para la aplicación elegida.

### Datos Máximos

Especifica el número máximo de bytes (datos) que se pueden transferir en una sola sesión del Protocolo de Transporte de Correo Simple (SMTP, Simple Mail Transport Protocol). Después de que se exceda el valor máximo, el firewall mostrará un mensaje de advertencia y cerrará la sesión. Valor por defecto: 20 MB.

### Inicio de Sesión Seguro

Causa que un usuario en una ubicación no segura use encriptación para autenticación.

### Reiniciar

Reinicia la conexión TCP si el cliente introduce un comando sin protocolo antes de que se complete la autenticación.

### Tráfico del Router

Activa la inspección de tráfico destinada a u originada por un router. Aplicable solamente para H.323, TCP, y protocolos de UDP.

# Tiempos de inactividad y umbrales para mapas de parámetros de inspección y CBAC

Use esta información como ayuda para crear o editar un mapa de parámetros para propósitos de inspección o para establecer tiempos de inactividad y umbrales globales de control de acceso basado en contexto (CBAC). CBAC usa tiempos de inactividad y umbrales para determinar cuánto tiempo gestionará la información del estado de una sesión y para determinar cuándo cerrará las sesiones que no se establezcan completamente. Estos tiempos de inactividad y umbrales se aplican a todas las sesiones.

Los valores del temporizador global se pueden especificar en segundos, minutos, u horas.

## Valor del tiempo de Inactividad de la conexión de TCP

El tiempo que se debe esperar para el establecimiento de una conexión TCP. El valor por defecto es 30 segundos.

## Valor del tiempo de Inactividad de espera del TCP Final

El tiempo en que una sesión TCP todavía será gestionada después de que el firewall detecte un intercambio FIN. El valor por defecto es 5 segundos.

## Valor del tiempo de Inactividad e inactivo del TCP

El tiempo en que una sesión TCP todavía será gestionada después de que no se haya detectado ninguna actividad. El valor por defecto es de 3.600 segundos.

## Valor del tiempo de Inactividad e inactivo del UDP

El tiempo durante el cual una sesión de protocolo de datagrama de usuario (UDP) se seguirá gestionando después de que no se haya detectado ninguna actividad. El valor por defecto es 30 segundos.

## Valor del tiempo de Inactividad del DNS

El tiempo durante el cual una sesión de búsqueda de nombre en el sistema de nombres de dominio (DNS) se seguirá gestionando después de que no se haya detectado ninguna actividad. El valor por defecto es 5 segundos.

## Umbrales de ataques de DoS SYN Flood

Un número inusualmente alto de sesiones medio abiertas podrían indicar que un ataque de Denegación de Servicios (DoS, Denial of Service) está en camino. Los umbrales de ataques de DoS permiten que el router comience a eliminar sesiones medio abiertas después de que el número total de ellas haya alcanzado un umbral máximo. Al definir los umbrales, usted podrá especificar cuándo el router deberá comenzar a eliminar sesiones medio abiertas y cuándo podrá parar de eliminarlas.

**Umbrales de sesiones de un minuto.** Estos campos le permiten especificar los valores del umbral para los intentos de una nueva conexión.

Bajo	Para de eliminar las nuevas conexiones después de que el número de las nuevas conexiones caiga debajo de este valor. El valor por defecto es 400 sesiones.
Alto	Comienza a eliminar las nuevas conexiones cuando el número de las nuevas conexiones exceda este valor. El valor por defecto es 500 sesiones.

**Umbral máximo de sesiones incompletas. Estos campos permiten** especificar los valores de umbral para el número total de sesiones medio abiertas existentes.

**Inferior** Para de eliminar las nuevas conexiones después de que el número de las nuevas conexiones caiga debajo de este valor. El valor por defecto es 400 sesiones para versiones de Cisco IOS posteriores a 12.4(11)T. Cuando un valor bajo no se ha definido explícitamente, Cisco IOS detendrá la eliminación de nuevas sesiones cuando el número de sesiones descienda a 400.

Para la versión 12.4(11)T y posteriores de Cisco IOS, el valor por defecto es ilimitado. Cuando un valor bajo no se ha definido explícitamente, Cisco IOS no detendrá la eliminación de nuevas conexiones.

**Alto** Comienza a eliminar las nuevas conexiones cuando el número de las nuevas conexiones exceda este valor. El valor por defecto es 500 sesiones para versiones de Cisco IOS posteriores a 12.4(11)T. Cuando un valor alto no se ha definido explícitamente, Cisco IOS comienza a eliminar sesiones cuando se han establecido más de 500 sesiones nuevas.

Para la versión 12.4(11)T y posteriores de Cisco IOS, el valor por defecto es ilimitado. Cuando un valor alto no se ha definido explícitamente, Cisco IOS no comenzará a eliminar nuevas conexiones.

#### **Número máximo de sesiones incompletas por host de TCP:**

El router comienza a eliminar sesiones medio abiertas para el mismo host cuando el número total para dicho host supera este número. El número por defecto de sesiones es de 50. Si activa el campo **Hora de bloqueo** y especifica un valor, el router seguirá bloqueando conexiones nuevas a dicho host durante el número de minutos especificado.

## Activar auditoría globalmente

Seleccione esta casilla si desea activar los mensajes de seguimiento de auditoría [CBAC](#) para todos los tipos de tráfico.

## Activar alerta globalmente

Marque esta casilla si desea activar los mensajes de alerta del CBAC para todos los tipos de tráfico.

## Asociar Política con una Interfaz

En esta ventana, seleccione la interfaz a la cual usted desea aplicarle la política seleccionada. También especifique si la política debe aplicarse al tráfico entrante, al tráfico saliente, o al tráfico en ambas direcciones.

Por ejemplo, si el router tiene interfaces de FastEthernet 0/0 y FastEthernet 0/1, y desea aplicar la política a la interfaz de FastEthernet 0/1 en el tráfico que fluye en ambas direcciones, marque la casilla situada al lado de FastEthernet 0/1 y las casillas en la columna entrante y la columna saliente. Para sólo inspeccionar el tráfico entrante, marque solamente la casilla en la columna entrante.

## Editar la Regla de Inspección

Use esta ventana para especificar las configuraciones de la regla de inspección personalizada para una aplicación. Las configuraciones hechas aquí y aplicadas a la configuración del router sustituirán los ajustes globales.

Haga clic en el botón **Configuración global** en la ventana de seguridad de la aplicación para mostrar las configuraciones globales para los parámetros que pueda establecer en esta ventana. Consulte el apartado [Tiempos de inactividad y umbrales para mapas de parámetros de inspección y CBAC](#) para obtener más información.

## Campo Alerta

Elija uno de los valores siguientes:

- **por defecto**: usar la configuración global para las alertas.
- **activado**: generar una alerta cuando se encuentra tráfico de este tipo.
- **desactivado**: no generar una alerta cuando se encuentra tráfico de este tipo.

## Campo Auditoría

Elija uno de los valores siguientes:

- **por defecto:** usar la configuración global para las pruebas de auditoría.
- **activado:** generar una prueba de auditoría cuando se encuentra el tráfico de este tipo.
- **desactivado:** no generar una prueba de auditoría cuando se encuentra el tráfico de este tipo.

## Campo Tiempo de inactividad

Introduce el número de segundos en que una sesión para esta aplicación debe gestionarse después de que no se haya detectado ninguna actividad. El valor del tiempo de Inactividad que usted introduzca, establecerá el valor del tiempo de Inactividad e inactivo del TCP si esto es una aplicación de TCP, o el valor del tiempo de Inactividad e inactivo del UDP si esto es una aplicación del UDP.

## Otras opciones

Ciertas aplicaciones pueden tener opciones adicionales establecidas. Dependiendo de la aplicación, usted podrá ver después las opciones descritas.

### Campo Datos Máximos

Especifica el número máximo de bytes (datos) que se pueden transferir en una sola sesión del Protocolo de Transporte de Correo Simple (SMTP, Simple Mail Transport Protocol). Después de que se exceda el valor máximo, el firewall mostrará un mensaje de advertencia y cerrará la sesión. Valor por defecto: 20 MB.

### Casilla de verificación Inicio de sesión seguro

Causa que un usuario en una ubicación no segura use encriptación para la autenticación.

### Casilla de verificación Reiniciar

Reinicia la conexión TCP si el cliente introduce un comando sin protocolo antes de que se complete la autenticación.

### Casilla de verificación Tráfico del Router

Activa la inspección de tráfico destinada a u originada por un router. Aplicable solamente para H.323, TCP, y protocolos de UDP.

## Controles Permitir, Bloquear y Alerta

Use los controles Permitir, Bloquear y Alerta para especificar lo que debe hacer el router cuando encuentre tráfico con las características que especifica. Para hacer una configuración de las políticas para una opción con estos controles, marque la casilla al lado de ella. Luego, en la columna de acción, elija **Permitir** para permitir el tráfico relacionado con esa opción, o elija **Bloquear** para denegar el tráfico. Si desea que una alarma se envíe al registro cuando se encuentre este tipo de tráfico, marque **Enviar Alarma**. El control Enviar Alarma no se usa en todas las ventanas.

El inicio de sesión debe activarse para que la seguridad de la aplicación pueda enviar alarmas al registro. Si desea obtener más información, consulte este enlace: [Registro de Seguridad de la aplicación](#).





## CAPÍTULO 9

# VPN sitio a sitio

---

Los temas de ayuda en esta sección describen las pantallas de configuración VPN sitio a sitio y las pantallas de Guía de diseño de VPN.

## Guía de diseño de VPN

Si está configurando una red [VPN](#) como administrador, la Guía de diseño de VPN le ayuda a determinar la clase de VPN que debe configurar. Usted proporcionará información acerca de su tipo de usuario, del tipo de equipamiento con el que el router establece conexiones VPN, del tipo de tráfico que transportará la VPN y de otras características que debe configurar. Una vez que haya proporcionado esta información, la Guía de diseño de VPN le recomendará un tipo de VPN y le permitirá iniciar el asistente que le ayudará a configurar esa clase de VPN.

## Crear VPN sitio a sitio

Una red privada virtual (VPN) permite proteger el tráfico que viaja por líneas que no son propiedad de la empresa o que ésta no controla. Las VPN pueden cifrar el tráfico enviado por estas líneas y autenticar pares antes de que se envíe tráfico.

Cisco Router and Security Device Manager (Cisco SDM) (Cisco SDM) puede guiarle a través de un proceso sencillo de configuración de VPN haciendo clic en el icono de VPN. Si utiliza el Asistente de la ficha Crear VPN sitio a sitio, Cisco SDM proporcionará los valores por defecto de algunos parámetros de configuración a fin de facilitar el proceso de configuración.

Si desea obtener más información acerca de la tecnología VPN, consulte el enlace [Información adicional acerca de VPN](#).

## Crear VPN sitio a sitio

Esta opción permite crear una red VPN que conecte a dos routers.

### Crear un túnel GRE seguro (GRE sobre IPSec)

Esta opción permite configurar un túnel GRE (Generic Routing Encapsulation Protocol) entre el router y un sistema de pares.

### ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
<p>Configurar el router como parte de una red <b>VPN</b> que conecte a dos routers.</p> <p>Cuando configure una red VPN entre dos routers, podrá controlar cómo se autentica el router remoto, cómo se cifra el tráfico y qué tráfico se cifra.</p>	<p>Seleccione <b>Crear VPN sitio a sitio</b>. A continuación, haga clic en <b>Iniciar la tarea seleccionada</b>.</p>
<p>Configurar un túnel <b>GRE</b> entre su router y otro router.</p> <p>Probablemente prefiera configurar un túnel GRE si necesita conectar redes que utilicen protocolos LAN diferentes o si necesita enviar protocolos de enrutamiento por la conexión al sistema remoto.</p>	<p>Seleccione <b>Crear un túnel GRE seguro (GRE sobre IPSec)</b>. A continuación, haga clic en <b>Iniciar la tarea seleccionada</b>.</p>

Si desea:	Haga lo siguiente:
<p>Saber cómo ejecutar otras tareas relacionadas con VPN para las que este asistente no proporciona ninguna guía.</p>	<p>Seleccione un tema en la lista siguiente:</p> <ul style="list-style-type: none"><li>• ¿Cómo se visualizan los comandos de IOS que se envían al router?</li><li>• ¿Cómo se crea una VPN para más de un sitio?</li><li>• Después de configurar una VPN, ¿cómo se configura la VPN en el router del par?</li><li>• ¿Cómo se edita un túnel VPN existente?</li><li>• ¿Cómo se puede confirmar que mi VPN funciona?</li><li>• ¿Cómo se puede confirmar que mi VPN funciona?</li><li>• ¿Cómo se configura un par de reserva para mi VPN?</li><li>• ¿Cómo se acomodan varios dispositivos con diferentes niveles de admisión de VPN?</li><li>• ¿Cómo se configura una VPN en una interfaz no compatible?</li><li>• ¿Cómo se configura una VPN después de configurar un firewall?</li><li>• ¿Cómo se configura el paso de NAT (NAT Passthrough) para una VPN?</li><li>• ¿Cómo se configura una red DMVPN manualmente?</li></ul>

Si desea:	Haga lo siguiente:
<p>Configurar un concentrador Easy VPN.</p> <p>Las instrucciones de configuración para servidores y concentradores Easy VPN están disponibles en <a href="http://www.cisco.com">www.cisco.com</a>.</p>	<p>El enlace siguiente proporciona directrices que deben seguirse cuando se configura un concentrador Cisco VPN serie 3000 para que funcione con un cliente Easy VPN remoto de fase II, así como otra información útil:</p> <p><a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a00800a8565.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a00800a8565.html</a></p> <p>El enlace siguiente le conectará con la documentación de Cisco VPN serie 3000:</p> <p><a href="http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_getting_started_guide_book09186a00800bbe74.html">http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_getting_started_guide_book09186a00800bbe74.html</a></p>

## Asistente para VPN sitio a sitio

Puede hacer que Cisco SDM utilice los valores por defecto para la mayoría de los valores de configuración, o bien, permitir que Cisco SDM le guíe en la configuración de [VPN](#).

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
<p>Configurar rápidamente una VPN sitio a sitio mediante los valores por defecto proporcionados por Cisco SDM.</p>	<p>Marque <b>Configuración rápida</b> y, a continuación, haga clic en <b>Siguiente</b>.</p> <p>Cisco SDM proporcionará automáticamente una política <b>IKE</b> por defecto para regir la autenticación, un conjunto de transformación por defecto para controlar el cifrado de los datos y una regla IPsec por defecto que cifrará todo el tráfico existente entre el router y el dispositivo remoto.</p> <p>El rendimiento de la configuración rápida mejora cuando tanto el router local como el sistema remoto son routers de Cisco que utilizan Cisco SDM.</p> <p>La configuración rápida configurará el cifrado 3DES si la imagen de IOS lo admite. De lo contrario, configurará el cifrado DES. Si necesita cifrado AES o SEAL, haga clic en <b>Asistente por pasos</b>.</p>
<p>Ver la política IKE, el conjunto de transformación y la regla IPsec por defecto que se utilizarán para configurar una VPN con un solo paso.</p>	<p>Haga clic en <b>Ver valores por defecto</b>.</p>
<p>Configurar una VPN sitio a sitio mediante parámetros que usted mismo especifique.</p>	<p>Active el <b>Asistente por pasos</b> y, a continuación, haga clic en <b>Siguiente</b>.</p> <p>Puede crear una configuración personalizada de la VPN y utilizar cualquier valor por defecto de Cisco SDM que necesite.</p> <p>El Asistente por pasos le permitirá especificar un cifrado más potente que el permitido por el Asistente para la configuración rápida.</p>

## Ver valores por defecto

Esta ventana muestra la política de Intercambio de claves por Internet (IKE), el conjunto de transformación y la regla IPSec por defecto que Cisco SDM utilizará para configurar rápidamente una VPN sitio a sitio. Si necesita una configuración distinta de la mostrada en la ventana, marque **Asistente por pasos** para definir los valores de la configuración personalmente.

## Información acerca de la conexión VPN

Utilice esta ventana para identificar la **Dirección IP** o el nombre de host del sitio remoto que terminará el túnel **VPN** que está configurando, especificar la interfaz del router que se utilizará y escribir la clave previamente compartida que ambos routers utilizarán para autenticarse entre sí.

### Seleccione la interfaz para esta conexión VPN

Seleccione la interfaz del router que permite conectarse con el sitio remoto. El router que está configurando aparecerá designado como router local en el diagrama del escenario de utilización.

### Identidad del par

Especifique la dirección IP del par de seguridad IP remoto (**IPSec**) que terminará el túnel VPN que está configurando. El par IPSec remoto puede ser otro router, un concentrador VPN o cualquier otro dispositivo de gateway que admita IPSec.

#### **Pares con dirección IP dinámica**

Seleccione esta opción si los pares con los que se conecta el router utilizan direcciones IP asignadas dinámicamente.

#### **Par con dirección IP estática**

Seleccione esta opción si el par con el que se conecta el router utiliza una dirección IP fija.

#### **Especifique la dirección IP válida para el par remoto**

(Activado cuando se activa el par con dirección IP estática). Especifique la dirección IP del par remoto.

## Autenticación

Haga clic en este botón si los pares VPN utilizan una clave previamente compartida para realizar **autenticación** las conexiones entre sí. La clave deberá ser la misma a ambos lados de la conexión VPN.

Escriba la **clave previamente compartida** y, a continuación, vuelva a especificarla para confirmarla. Intercambie la clave previamente compartida con el administrador del sitio remoto mediante algún método cómodo y seguro como, por ejemplo, un mensaje de correo electrónico cifrado. Los signos de interrogación (?) y los espacios no pueden utilizarse en la clave previamente compartida. La clave previamente compartida puede contener un máximo de 128 caracteres.



### Nota

- Los caracteres especificados para la clave previamente compartida no se verán en el campo a medida que los escriba. Le recomendamos que anote la clave antes de especificarla a fin de poder comunicarla al administrador del sistema remoto.
- Las claves previamente compartidas deben intercambiarse entre cada par IPsec que necesite establecer túneles seguros. Este método de autenticación es adecuado para una red estable con un número limitado de pares IPsec. No obstante, en una red con un gran número de pares IPsec o un número creciente de éstos, pueden surgir problemas de escalabilidad.

## Certificado digital

Haga clic en este botón si los pares VPN van a utilizar certificados digitales para la autenticación.



### Nota

Para autenticarse a sí mismo, es preciso que el router cuente con un certificado digital que haya sido emitido por una Autoridad certificadora. Si no ha configurado ningún certificado digital para el router, vaya a Componentes VPN y utilice el Asistente para certificados digitales para suscribirse a un certificado digital.

## Tráfico para cifrar

Si está efectuando una configuración rápida de una conexión VPN sitio a sitio, deberá especificar las subredes de origen y de destino en esta ventana.

### Origen

Elija la interfaz del router que será el origen del tráfico para esta conexión VPN. Todo el tráfico que provenga de esta interfaz cuya dirección IP de destino esté en la subred especificada en el área Destino, se cifrará.

### Detalles

Haga clic en este botón para obtener los detalles de la interfaz seleccionada. La ventana Detalles mostrará todas las reglas de acceso, políticas IPSec, reglas de traducción de direcciones de red (NAT) o reglas de inspección asociadas a la interfaz. Para examinar con más detalle cualquiera de estas reglas, vaya a Tareas adicionales/Editor ACL y examínelas en las ventanas Reglas.

### Destino

**Dirección IP y máscara de subred.** Especifique la dirección IP y la máscara de subred del destino de este tráfico. Para obtener información acerca de cómo especificar valores en estos campos, consulte [Direcciones IP y máscaras de subred](#).

El destino está indicado como router remoto en el diagrama del escenario de utilización que aparece en la ventana principal del Asistente para VPN.

## Propuestas IKE

Esta ventana muestra una lista de todas las políticas de Intercambio de claves por Internet (**IKE**) configuradas en el router. Si no se ha configurado ninguna política definida por el usuario, esta ventana mostrará la política IKE por defecto de Cisco SDM. Las políticas IKE rigen la forma en que los dispositivos de una **VPN** se autentican a sí mismos.

El router local utilizará las políticas IKE indicadas en esta ventana para negociar la autenticación con el router remoto.

El router local y el dispositivo par deben utilizar la misma política. El router que inicie la conexión VPN ofrecerá primero la política con el número de prioridad más bajo. Si el sistema remoto la rechaza, el router local ofrecerá a continuación la segunda política con el número más bajo y así hasta que el sistema remoto acepte la política ofrecida. Será preciso establecer una estrecha coordinación con el administrador del sistema par para configurar políticas idénticas en ambos routers.

En el caso de las conexiones Easy VPN, las políticas IKE sólo se configuran en el servidor Easy VPN. El cliente Easy VPN envía propuestas y el servidor responde de acuerdo con las políticas IKE que tenga configuradas.



## Prioridad

Orden en que se ofrecerán las políticas durante la negociación.

## Cifrado

Cisco SDM admite varios tipos de cifrado, ordenados según su seguridad en una lista. Cuanto más seguro sea un tipo de cifrado, más tiempo de proceso necesitará.



### Nota

- No todos los routers admiten todos los tipos de cifrado. Los tipos que no se admitan no aparecerán en la pantalla.
- No todas las imágenes de IOS admiten todos los tipos de cifrado que Cisco SDM admite. Los tipos que la imagen de IOS no admita no aparecerán en la pantalla.
- Si el cifrado de hardware está activado, sólo aparecerán en la pantalla los tipos de cifrado admitidos por el cifrado de hardware.

Cisco SDM admite los tipos de cifrado siguientes:

- DES: Data Encryption Standard. Esta forma de cifrado admite un cifrado de 56 bits.
- 3DES: Triple DES. Forma de cifrado más potente que DES que admite un cifrado de 168 bits.
- AES-128: cifrado AES (Advanced Encryption Standard) con una clave de 128 bits. AES aporta mayor seguridad que DES y, desde un punto de vista computacional, es más eficiente que 3DES.
- AES-192: cifrado AES con una clave de 192 bits.
- AES-256: cifrado AES con una clave de 256 bits.

## Hash

Algoritmo de autenticación que se utilizará para negociar. Cisco SDM admite los algoritmos siguientes:

- SHA\_1: algoritmo de hash seguro. Algoritmo de hash utilizado para autenticar los datos del paquete.
- MD5: Message Digest 5. Algoritmo de hash utilizado para autenticar los datos del paquete.

## Grupo D-H

El grupo Diffie-Hellman: Diffie-Hellman es un protocolo de criptografía de clave pública que permite a dos routers establecer un secreto compartido en un canal de comunicaciones que no es seguro. Cisco SDM admite los grupos siguientes:

- group1: grupo 1 de D-H; Grupo D-H de 768 bits.
- group2: grupo 2 de D-H; Grupo D-H de 1.024 bits. Este grupo brinda más seguridad que el grupo 1, aunque necesita más tiempo de proceso.
- group5: grupo 5 de D-H; Grupo D-H de 1.536 bits. Este grupo brinda más seguridad que el grupo 2, aunque necesita más tiempo de proceso.

## Autenticación

Método de autenticación que se utilizará. Se admiten los valores siguientes:

- PRE\_SHARE: la autenticación se ejecutará mediante claves previamente compartidas.
- RSA\_SIG: la autenticación se ejecutará mediante certificados digitales.



### Nota

---

Debe elegir el tipo de autenticación que especificó al identificar las interfaces que utiliza la conexión VPN.

---

## Tipo

Puede ser Cisco SDM por defecto o Definido por el usuario. Si no se ha creado ninguna política definida por el usuario en el router, esta ventana mostrará la política IKE por defecto.

## Para agregar o editar una política IKE:

Si desea agregar una política IKE que no está incluida en esta lista, haga clic en **Agregar** y cree la política en la ventana que aparezca. Edite una política existente seleccionándola y haciendo clic en **Editar**. Las políticas de Cisco SDM por defecto son de sólo lectura y no se pueden editar.

## Para aceptar la lista de políticas:

Para aceptar la lista de políticas IKE y seguir, haga clic en **Siguiente**.

## Conjunto de transformación

Esta ventana muestra una lista de los conjuntos de transformación por defecto de Cisco SDM y los conjuntos de transformación adicionales que se han configurado en este router. Estos conjuntos de transformación estarán disponibles para que los utilice VPN o DMVPN. Un [conjunto de transformación](#) es una combinación determinada de algoritmos y protocolos de seguridad. Durante la negociación de la asociación de seguridad IPSec, los pares acuerdan utilizar un conjunto de transformación determinado para proteger un flujo de datos concreto. Una [transformación](#) describe un protocolo de seguridad determinado junto con sus algoritmos correspondientes.

En esta ventana sólo puede seleccionar un conjunto de transformación, aunque puede asociar conjuntos de transformación adicionales a la conexión VPN o DMVPN mediante las fichas Editar de VPN o DMVPN.

### Seleccionar conjunto de transformación

Seleccione en esta lista el conjunto de transformación que desee utilizar.

### Detalles del conjunto de transformación seleccionado

En esta área se muestran los detalles del conjunto de transformación seleccionado. No es obligatorio configurar todos los tipos de cifrado, autenticación y compresión; por consiguiente, es posible que algunas columnas no contengan ningún valor.

Para saber cuáles son los posibles valores que cada columna puede contener, haga clic en [Agregar/Editar conjunto de transformación](#).

#### Nombre

Nombre de este conjunto de transformación.

#### Cifrado ESP

Tipo de cifrado ESP (Encapsulating Security Protocol) utilizado. Si el cifrado ESP no está configurado para este conjunto de transformación, esta columna estará vacía.

**Autenticación ESP**

Tipo de autenticación ESP utilizada. Si la autenticación ESP no está configurada para este conjunto de transformación, esta columna estará vacía.

**Autenticación AH**

Tipo de autenticación AH (encabezado de autenticación) utilizado. Si la autenticación AH no está configurada para este conjunto de transformación, esta columna estará vacía.

**Compresión IP**

Si la compresión IP está configurada para este conjunto de transformación, este campo contendrá el valor COMP-LZS.



---

**Nota** No todos los routers admiten la compresión IP.

---

**Modo**

Esta columna contiene uno de los valores siguientes:

- **Transporte:** cifrar datos solamente. El modo de transporte se utiliza cuando ambos puntos finales admiten IPSec. El modo de transporte coloca el encabezado de autenticación o la carga útil de seguridad encapsulada después del encabezado IP original, por lo que sólo se cifra la carga útil de IP. Este método permite a los usuarios aplicar servicios de red como controles de calidad de servicio (QoS) a paquetes cifrados.
- **Túnel:** cifrar datos y encabezado IP. El modo de túnel brinda mayor protección que el modo de transporte. Dado que todo el paquete IP se encapsula en AH o ESP, se adjunta un encabezado IP nuevo y se puede cifrar el datagrama completo. El modo de túnel permite a los dispositivos de red, como los routers, actuar como proxy de IPSec para varios usuarios de VPN.

**Tipo**

Puede ser Definido por el usuario o Cisco SDM por defecto.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Seleccionar un conjunto de transformación para que VPN lo utilice.	Seleccione un conjunto de transformación y haga clic en <b>Siguiente</b> .
Agregar un conjunto de transformación a la configuración del router.	Haga clic en <b>Agregar</b> y cree el conjunto de transformación en la ventana Agregar conjunto de transformación. A continuación, haga clic en <b>Siguiente</b> para seguir configurando VPN.
Editar un conjunto de transformación existente.	Seleccione un conjunto de transformación y haga clic en <b>Editar</b> . A continuación, edite el conjunto de transformación en la ventana Editar conjunto de transformación. Después de editar el conjunto de transformación, haga clic en <b>Siguiente</b> para seguir configurando VPN. Los conjuntos de transformación de Cisco SDM por defecto son de sólo lectura y no se pueden editar.
Asociar conjuntos de transformación adicionales a esta VPN.	Seleccione en esta ventana un conjunto de transformación y complete el Asistente para VPN. A continuación, asocie otros conjuntos de transformación a la VPN en la ficha Editar.

## Tráfico para proteger

Esta ventana permite definir el tráfico que esta [VPN](#) protege. La VPN puede proteger tráfico entre subredes especificadas o proteger el tráfico especificado en una regla IPSec que seleccione.

### Proteger todo el tráfico entre las subredes siguientes

Utilice esta opción para especificar una única subred de origen (subred en la LAN) cuyo tráfico saliente desee cifrar y una subred de destino admitida por el par especificado en la ventana de la conexión VPN.

Todo el tráfico que fluya entre otros pares de origen y de destino se enviará sin cifrar.

### Origen

Especifique la dirección de subred cuyo tráfico saliente desee proteger e indique la máscara de subred. Si desea obtener más información, consulte [Configuraciones de interfaz disponibles](#).

Se protegerá todo el tráfico que provenga de esta subred de origen y tenga una dirección IP de destino en la subred de destino.

### Destino

Especifique la dirección de la subred de destino e indique la máscara de dicha subred. Puede seleccionar una máscara de subred en la lista o bien escribir una máscara personalizada. El número de subred y la máscara deben especificarse en formato de decimales con puntos, tal como se muestra en los ejemplos anteriores.

Se protegerá todo el tráfico que vaya a los hosts de esta subred.

## Crear o seleccionar una lista de acceso para el tráfico IPSec

Utilice esta opción si necesita especificar varios orígenes y destinos o tipos específicos de tráfico para cifrar. Una regla IPSec puede estar formada por varias entradas, cada una de ellas especificando diferentes tipos de tráfico y diferentes orígenes y destinos.

Haga clic en el botón situado al lado del campo y especifique una [regla IPSec](#) existente que defina el tráfico que desee cifrar o cree una regla IPSec para utilizar con esta VPN. Si sabe el número de la regla IPSec, indíquelo en el cuadro situado a la derecha. Si no sabe el número de la regla, haga clic en el botón ... y desplácese hasta ésta. Cuando seleccione la regla, el número aparecerá en el cuadro.



### Nota

---

Dado que las reglas IPSec pueden especificar el tipo de tráfico, así como el origen y el destino, se trata de reglas ampliadas. Si especifica el nombre o el número de una regla estándar, aparecerá un mensaje de alerta indicando que ha especificado el nombre o el número de una regla estándar.

---

Todos los paquetes que no cumplan los criterios especificados en la regla IPSec se enviarán sin cifrar.

## Resumen de la configuración

Esta ventana muestra la configuración VPN o DMVPN que ha creado. Puede revisar la configuración en ella y utilizar el botón Atrás para cambiar cualquier parámetro, si así lo desea.

### Configuración de spoke

Si ha configurado un hub DMVPN, puede hacer que Cisco SDM genere un procedimiento que ayudará tanto al usuario como a otros administradores a configurar spokes DMVPN. Dicho procedimiento explica qué opciones deben seleccionarse en el asistente y qué información debe especificarse en las ventanas de configuración de spoke. Esta información puede guardarse en un archivo de texto que el usuario u otro administrador puede utilizar.

### Una vez realizada la configuración, pruebe la conectividad

Haga clic para probar la conexión VPN que acaba de configurar. Los resultados de la prueba se mostrarán en otra ventana.

### Para guardar esta configuración en la configuración en ejecución del router y salir de este asistente:

Haga clic en **Finalizar**. Cisco SDM guarda los cambios de configuración en la configuración en ejecución del router. Aunque los cambios se aplican inmediatamente, los mismos se perderán si se apaga el router.

Si ha marcado la opción **Obtener una vista previa de los comandos antes de enviarlos al router** de la ventana Preferencias de Cisco SDM, aparecerá la ventana Enviar. Esta ventana permite ver los comandos del CLI que se envían al router.

### Configuración de spoke

Esta ventana contiene información que puede utilizar para dar a un router spoke una configuración compatible con el hub DMVPN que ha configurado. Muestra una lista de las ventanas que es preciso completar y aporta datos que deberá especificar en la ventana para que el spoke pueda comunicarse con el hub.

Proporciona los datos siguientes que se deben introducir en la configuración del spoke:

- La dirección IP pública del hub. Se trata de la dirección IP de la interfaz del hub que admite el túnel mGRE.
- La dirección IP del túnel mGRE del hub.
- La máscara de subred que todas las interfaces de túnel de DMVPN deben utilizar.
- La información de la configuración de túnel avanzada.
- El protocolo de enrutamiento que se utilizará y cualquier información asociada al protocolo, como el número de sistema autónomo (para EIGRP) o el ID de proceso OSPF.
- El hash, el cifrado, el grupo DH y el tipo de autenticación de las políticas IKE que utiliza el hub, para que se puedan configurar políticas IKE compatibles en el spoke.
- La información de ESP y de modo de los conjuntos de transformación que el hub utiliza. Si no se han configurado conjuntos de transformación similares en el spoke, podrá configurarlos gracias a esta información.

## Túnel GRE seguro (GRE sobre IPSec)

La encapsulación genérica de enrutamiento ([GRE](#)) es un protocolo de arquitectura de túneles desarrollado por Cisco que puede encapsular una amplia variedad de tipos de paquetes de protocolos dentro de túneles IP, creando un enlace de punto a punto virtual a routers de Cisco situados en puntos remotos de una interred IP. Gracias a la conexión de subredes de varios protocolos a un entorno con una base de protocolo único, la creación de túneles IP mediante GRE permite la expansión de la red en un entorno de protocolo único.

Este asistente permite crear un túnel GRE con cifrado IPSec. Cuando cree una configuración de túnel GRE, cree también una [regla IPSec](#) que describa los puntos finales del túnel.



## Información acerca del túnel GRE

En esta pantalla se proporciona información general del túnel GRE.

### Origen del túnel

Seleccione el nombre de la interfaz o la dirección IP de la interfaz que el túnel utilizará. La dirección IP de la interfaz debe ser alcanzable desde el otro extremo del túnel y, por lo tanto, debe tratarse de una dirección IP pública que se pueda enrutar. Se generará un error si se especifica una dirección IP que no esté asociada a ninguna interfaz configurada.



#### Nota

---

Cisco SDM muestra una lista de interfaces con direcciones IP estáticas e interfaces configuradas como no numeradas en la lista de interfaces. Esta lista no incluye las interfaces de retrobucle.

---

### Detalles

Haga clic en esta opción para obtener los detalles de la interfaz seleccionada. La ventana Detalles mostrará todas las reglas de acceso, políticas IPsec, reglas NAT o reglas de inspección asociadas a la interfaz. Si se ha aplicado una regla NAT a esta interfaz que impide el enrutamiento de la dirección, el túnel no funcionará correctamente. Para examinar con más detalle cualquiera de estas reglas, vaya a Tareas adicionales/Editor ACL y examínelas en la ventana Reglas.

### Destino del túnel

Especifique la dirección IP de la interfaz en el router remoto del otro extremo del túnel. Desde el punto de vista del otro extremo del túnel, se trata de la interfaz de origen.

Asegúrese de que se pueda alcanzar la dirección mediante el comando **ping**. El comando **ping** está disponible en el menú Herramientas. Si no se puede alcanzar la dirección de destino, el túnel no se creará correctamente.

### Dirección IP del túnel GRE

Especifique la dirección IP del túnel. Las direcciones IP de ambos extremos del túnel deben estar en la misma subred. Se proporciona una dirección IP independiente al túnel para que, si es preciso, ésta pueda ser una dirección privada.

**Dirección IP**

Especifique la dirección IP del túnel en formato de decimales con puntos. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

**Máscara de subred**

Especifique la máscara de subred de la dirección del túnel en formato de decimales con puntos.

## Información de autenticación VPN

Los pares VPN utilizan una clave previamente compartida para realizar la [autenticación](#) de las conexiones entre sí. La clave deberá ser la misma a ambos lados de la conexión VPN.

**Clave previamente compartida**

Haga clic en este botón si los pares VPN utilizan una clave previamente compartida para autenticar; a continuación, especifique la [clave previamente compartida](#) y, por último, vuelva a escribirla para confirmarla. Intercambie la clave previamente compartida con el administrador del sitio remoto mediante algún método cómodo y seguro como, por ejemplo, un mensaje de correo electrónico cifrado. Los signos de interrogación (?) y los espacios no pueden utilizarse en la clave previamente compartida.

**Nota**

- Los caracteres especificados para la clave previamente compartida no se verán en el campo a medida que los escriba. Le recomendamos que anote la clave antes de especificarla a fin de poder comunicarla al administrador del sistema remoto.
- Las claves previamente compartidas deben intercambiarse entre cada par IPSec que necesite establecer túneles seguros. Este método de autenticación es adecuado para una red estable con un número limitado de pares IPSec. No obstante, en una red con un gran número de pares IPSec o un número creciente de éstos, pueden surgir problemas de escalabilidad.

## Certificado digital

Haga clic en este botón si los pares VPN van a utilizar certificados digitales para la autenticación.

Para autenticarse a sí mismo, es preciso que el router cuente con un certificado digital que haya sido emitido por una Autoridad certificadora. Si no ha configurado ningún certificado digital para el router, vaya a Componentes VPN y utilice el Asistente para certificados digitales para suscribirse a un certificado digital.



### Nota

---

Si autentica mediante certificados digitales, es posible que no se cree el túnel VPN si el servidor de la Autoridad certificadora (CA) contactado durante la negociación IKE no está configurado para responder a solicitudes CRL (de listas de revocación de certificados). Para solucionar este problema, vaya a la página Certificados digitales, seleccione el punto de confianza configurado y, a continuación, None for Revocation (Ninguno para revocar).

---

## Información acerca del túnel GRE de reserva

Se puede configurar un túnel GRE sobre IPsec de reserva para que el router lo utilice en caso de fallar el túnel principal. Este túnel utilizará la misma interfaz que la que configuró para el túnel principal, aunque debe configurarse con el router de la VPN de reserva como par. Si el enrutamiento está configurado para el túnel GRE sobre IPsec principal, los paquetes “keepalive” que envíe el protocolo de enrutamiento se utilizarán para verificar que el túnel siga activo. Si el router deja de recibir paquetes “keepalive” en el túnel principal, el tráfico se enviará a través del túnel de reserva.

### Cree un túnel GRE de reserva para aumentar la flexibilidad

Active esta casilla si desea crear un túnel de reserva.

### Dirección IP del destino del túnel GRE de reserva:

Especifique la dirección IP de la interfaz en el router remoto del otro extremo del túnel. (Desde el punto de vista del otro extremo del túnel, se trata de la interfaz de origen).

Asegúrese de que se pueda alcanzar la dirección mediante el comando **ping**. El comando **ping** está disponible en el menú Herramientas. Si no se puede alcanzar la dirección de destino especificada en el cuadro de diálogo Ping, el túnel no se creará correctamente.

### Dirección IP del túnel

Especifique la dirección IP del túnel. Las direcciones IP de ambos extremos del túnel deben estar en la misma subred. Se proporciona una dirección IP independiente al túnel para que, si es preciso, ésta pueda ser una dirección privada.

#### Dirección IP

Especifique la dirección IP del túnel en formato de decimales con puntos. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

#### Máscara de subred

Especifique la máscara de subred de la dirección del túnel en formato de decimales con puntos.

## Información de enrutamiento

Esta ventana permite configurar el enrutamiento del tráfico del túnel. La información que agregue a esta ventana aparecerá en la ventana Enrutamiento. Los cambios que efectúe en la ventana Enrutamiento pueden influir en el tráfico VPN. La configuración del enrutamiento le permitirá especificar las redes que participarán en la VPN GRE sobre IPsec. Asimismo, si configura un túnel GRE sobre IPsec de reserva, los paquetes “keepalive” enviados por protocolos de enrutamiento permitirán al router determinar si ha fallado el túnel principal.

Seleccione un protocolo de enrutamiento dinámico si este router se está utilizando en una gran implementación de [VPN](#) con un amplio número de redes en la [VPN GRE sobre IPsec](#). Seleccione un enrutamiento estático si van a participar pocas redes en la VPN.

## EIGRP

Marque este cuadro para utilizar **EIGRP** (Enhanced Interior Gateway Routing Protocol) para enrutar tráfico. Luego haga clic en **Próximo** para especificar qué red participará en la VPN GRE sobre IPsec en la ventana de información del enrutamiento dinámico.

## OSPF

Marque este cuadro para utilizar el protocolo **OSPF** (Open Shortest Path First) para enrutar tráfico. Luego haga clic en **Próximo** para especificar qué red participará en la VPN GRE sobre IPsec en la ventana de información del enrutamiento dinámico.

## RIP

Marque este cuadro para utilizar el protocolo **RIP** (Routing Information Protocol) para enrutar tráfico. Luego haga clic en **Siguiente** para especificar qué redes participarán en la VPN GRE sobre IPsec en la ventana de información de enrutamiento dinámico.

**Nota**

---

Esta opción no está disponible si se configura un túnel GRE sobre IPsec de reserva.

---

## Enrutamiento estático

El enrutamiento estático puede utilizarse en implementaciones de VPN más pequeñas en las que sólo unas cuantas redes privadas participen en VPN GRE sobre IPsec. Se puede configurar una ruta estática por cada red remota para que el tráfico destinado a las redes remotas pase por los túneles adecuados.

## Información sobre el enrutamiento estático

Se puede configurar una ruta estática por cada red remota para que el tráfico destinado a las redes remotas pase por los túneles adecuados. Configure la primera ruta estática en la ventana Información sobre el enrutamiento estático. Si necesita configurar rutas estáticas adicionales, vaya a la ventana Enrutamiento.

Marque este cuadro si desea especificar una ruta estática para el túnel y seleccione una de las opciones siguientes:

- **Enviar todo el tráfico por el túnel:** todo el tráfico se enrutará a través de la interfaz de túnel y se cifrará. Cisco SDM crea una entrada de ruta estática por defecto con la interfaz de túnel indicada como el próximo salto.

Si ya existe una ruta por defecto, Cisco SDM modifica dicha ruta para que utilice la interfaz de túnel como salto siguiente (para ello, sustituye la interfaz que estaba originalmente en ese punto y crea una entrada estática nueva a la red de destino del túnel, que especifique la interfaz de la ruta por defecto original como próximo salto).

En el ejemplo siguiente, se presupone que la red del otro extremo del túnel es 200.1.0.0, tal como se especifica en los campos de la red de destino:

```
! Original entry
ip route 0.0.0.0 0.0.0.0 FE0
! Entry changed by SDM
ip route 0.0.0.0 0.0.0.0 Tunnel0
! Entry added by SDM
ip route 200.1.0.0 255.255.0.0 FE0
```

Si no existe ninguna ruta por defecto, Cisco SDM crea una con la interfaz de túnel como salto siguiente. Por ejemplo:

```
ip route 0.0.0.0 0.0.0.0 Tunnel0
```

- **Dividir la arquitectura en distintos túneles:** la división de la arquitectura en túneles permite cifrar y enrutar, a través de la interfaz de túnel, el tráfico destinado a la red especificada en los campos Dirección IP y Máscara de red. El tráfico restante no se cifrará. Cuando se selecciona esta opción, Cisco SDM crea una ruta estática a la red mediante la dirección IP y la máscara de red.

En el ejemplo siguiente, se presupone que la dirección de red 10.2.0.0/255.255.0.0 se ha especificado en los campos de la dirección de destino:

En el ejemplo siguiente, se presupone que la dirección de red 10.2.0.0/255.255.0.0 se ha especificado en los campos de la dirección de destino:

```
ip route 10.2.0.0 255.255.0.0 Tunnel0
```

Cuando se seleccione la división de la arquitectura de túneles, aparecerán los campos Dirección IP y Máscara de Subred, lo que requiere que usted introduzca la Dirección IP y la Máscara de Subred del destino. Debe asegurarse de que se pueda alcanzar la dirección IP de destino especificada en el campo Destino del túnel de la ventana Información acerca del túnel GRE. Si no se puede alcanzar, no se establecerá ningún túnel.

## Dirección IP

Activada con la división de la arquitectura en túneles. Especifique la dirección IP de la red del otro extremo del túnel. Cisco SDM creará una entrada de ruta estática para los paquetes que tengan una dirección de destino en dicha red. Este campo se desactiva cuando se selecciona **Enviar todo el tráfico por el túnel**.

Antes de configurar esta opción, asegúrese de que se pueda alcanzar la dirección IP de destino especificada en este campo. Si no se puede alcanzar, no se establecerá ningún túnel.

## Máscara de red

Activada con la división de la arquitectura en túneles. Especifique la máscara de red utilizada en la red del otro extremo del túnel. Este campo se desactiva cuando se selecciona **Enviar todo el tráfico por el túnel**.

## Seleccionar el protocolo de enrutamiento

Utilice esta ventana para especificar el modo en que otras redes detrás del router se anunciarán a los demás routers de la red. Seleccione uno de los siguientes:

- **EIGRP**: Extended Interior Gateway Routing Protocol.
- **OSPF**: Open Shortest Path First.
- **RIP**: Routing Internet Protocol.
- Enrutamiento estático: esta opción está activada cuando se configura un túnel GRE sobre IPsec.

**Nota**

RIP no se admite para la topología de spoke y hub DMVPN, pero está disponible para la topología de malla completa de DMVPN.

## Resumen de la configuración

Esta pantalla resume la configuración de **GRE** que ha llevado a cabo. Puede revisar la información de esta pantalla y hacer clic en el botón **Atrás** para regresar a cualquier ventana en la que desee efectuar cambios. Si desea guardar la configuración, haga clic en **Finalizar**.

La configuración de túnel GRE crea una regla IPsec que especifica los hosts entre los que podrá fluir el tráfico GRE. La regla IPsec se indica en el resumen.

### Para guardar esta configuración en la configuración en ejecución del router y salir de este asistente:

Haga clic en **Finalizar**. Cisco SDM guarda los cambios de configuración en la configuración en ejecución del router. Aunque los cambios se aplican inmediatamente, los mismos se perderán si se apaga el router.

Si ha marcado la opción **Obtener una vista previa de los comandos antes de enviarlos al router** de la ventana Preferencias de Cisco SDM, aparecerá la ventana **Enviar**. Esta ventana permite ver los comandos del CLI que se envían al router.



# Editar VPN sitio a sitio

Las redes privadas virtuales (VPN) protegen, mediante el cifrado del tráfico, los datos entre el router y el sistema remoto, para que los que estén utilizando la misma red pública no puedan leerlos. De hecho, brindan la protección de una red privada sobre líneas públicas que otras organizaciones o empresas pueden utilizar.

Utilice esta ventana para crear y gestionar conexiones VPN a sistemas remotos. Puede crear, editar o eliminar conexiones VPN y restablecer conexiones ya existentes. También puede utilizar esta ventana para configurar el router como un cliente Easy VPN con conexiones a uno o varios concentradores o servidores Easy VPN.

Haga clic en el enlace de la parte de la ventana para la cual necesite ayuda:

## Conexiones VPN sitio a sitio

Las conexiones VPN, en ocasiones conocidas como *túneles*, se crean y gestionan desde el cuadro de conexiones VPN. Una conexión VPN enlaza la interfaz de un router con uno o varios pares especificados mediante un mapa criptográfico definido en una política IPSec (Seguridad IP). Las conexiones VPN de esta lista pueden verse, agregarse, editarse y eliminarse.

### Columna Estado

Estado de la conexión, indicado mediante los iconos siguientes:



La conexión está activa.



La conexión está inactiva.



Estableciendo la conexión.

### Interfaz

Interfaz del router conectada con los pares remotos en esta conexión VPN. Una interfaz se puede asociar con una sola política IPSec. La misma interfaz aparecerá en varias líneas si hay más de un [mapa criptográfico](#) definido para la política IPSec utilizada en esta conexión.

### Descripción

Breve descripción de esta conexión.

**Política IPsec**

Nombre de la política IPsec utilizada en esta conexión VPN. La política IPsec especifica cómo se cifran los datos, qué datos se cifrarán y adónde se enviarán los datos. Para obtener más información, haga clic en [Información adicional acerca de conexiones VPN y políticas IPsec](#).

**Número de secuencia**

Número de secuencia de esta conexión. Dado que una misma política IPsec puede utilizarse en más de una conexión, la combinación del número de secuencia y del nombre de la política IPsec identifica de forma exclusiva esta conexión VPN. El número de secuencia no sirve para dar prioridad a una conexión VPN; el router intentará establecer todas las conexiones VPN configuradas con independencia del número de secuencia.

**Pares**

Direcciones IP o nombres de host de los dispositivos del otro extremo de la conexión VPN. Si una conexión contiene varios pares, sus direcciones IP o nombres de host se separan con comas. Se pueden configurar varios pares para proporcionar rutas alternativas para el enrutamiento de la conexión VPN.

**Conjunto de transformación**

Muestra el nombre del [conjunto de transformación](#) utilizado para esta conexión VPN. En caso de haber varios nombres de conjuntos de transformación, éstos están separados mediante comas. Un conjunto de transformación especifica los algoritmos que se utilizarán para cifrar datos, asegurar su integridad y proporcionar la compresión de los mismos. Ambos pares deben utilizar el mismo conjunto de transformación, por lo que negociarán para determinar qué conjunto de transformación utilizarán. Se pueden definir varios conjuntos de transformación para asegurarse de que el router pueda ofrecer un conjunto de transformación que el par negociador acepte utilizar. Los conjuntos de transformación son un componente de la política IPsec.

**Regla IPsec**

Regla que determina qué tráfico debe cifrarse en esta conexión. La regla IPsec es un componente de la política IPsec.

**Tipo**

Uno de los siguientes:

- Estático: túnel VPN sitio a sitio estático. El túnel VPN utiliza mapas criptográficos estáticos.
- Dinámico: túnel VPN sitio a sitio dinámico. El túnel VPN utiliza mapas criptográficos dinámicos.

**Botón Agregar**

Haga clic en este botón para agregar una conexión VPN.

**Botón Eliminar**

Haga clic en este botón para eliminar una conexión VPN seleccionada.

**Botón Probar túnel**

Haga clic para probar un túnel VPN determinado. Los resultados de la prueba se mostrarán en otra ventana.

**Botón Establecer conexión**

Haga clic en este botón para establecer una conexión con un par remoto. Este botón se desactiva si ha seleccionado un túnel VPN sitio a sitio dinámico.

**Botón Generar una copia**

Haga clic en este botón para crear un archivo de texto que capture la configuración VPN del router local, de modo que se pueda dar a un router remoto una configuración VPN que le permita establecer una conexión VPN con el router local. Este botón se desactiva si ha seleccionado un túnel VPN sitio a sitio dinámico.

**Nota**

---

Si Cisco SDM detecta conexiones VPN configuradas anteriormente que no utilizan mapas criptográficos ISAKMP, dichas conexiones aparecerán como entradas de sólo lectura en la tabla de conexiones VPN y no se podrán editar.

---

## Agregar nueva conexión

Utilice esta ventana para agregar una conexión VPN nueva entre el router local y un sistema remoto conocido como *par*. La conexión VPN se crea asociando una política IPsec a una interfaz.

### Para crear una conexión VPN:

- 
- Paso 1** Seleccione la interfaz que desee utilizar para la VPN en la lista Seleccionar la interfaz. En esta lista sólo se muestran las interfaces que no se están utilizando en otras conexiones VPN.
- Paso 2** Seleccione una política en la lista Elegir una política IPsec. Haga clic en **Aceptar** para regresar a la ventana de conexiones VPN.
- 

## Agregar mapa criptográfico

Utilice esta ventana para agregar un mapa criptográfico nuevo a una política IPsec existente. La ventana muestra la interfaz asociada a la conexión VPN seleccionada en la ventana de conexiones VPN, la política IPsec asociada a ella y los mapas criptográficos que la política ya contiene.

El mapa criptográfico especifica un número de secuencia, el dispositivo par situado al otro extremo de la conexión, el conjunto de transformaciones que cifran el tráfico y la regla IPsec que determina el tráfico que se cifrará.



### Nota

---

Agregar un mapa criptográfico a una política IPsec existente es la única manera de agregar un túnel VPN a una interfaz que ya se está utilizando en una conexión VPN existente.

---

## Interfaz

Interfaz utilizada en esta conexión VPN.

## Política IPsec

Nombre de la política IPsec que controla la conexión VPN. Los mapas criptográficos que forman la política IPsec aparecen en la lista situada bajo este campo. Para obtener más información, haga clic en [Información adicional acerca de conexiones VPN y políticas IPsec](#).

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Configurar el mapa criptográfico por sí mismo.	Haga clic en <b>Agregar nuevo mapa criptográfico</b> y utilice la ventana Agregar mapa criptográfico para crear el mapa criptográfico nuevo. Haga clic en <b>Aceptar</b> cuando haya acabado. A continuación, haga clic en <b>Aceptar</b> en esta ventana.
Use Cisco Router and Security Device Manager (Cisco SDM) (Cisco SDM) para agregar un mapa criptográfico nuevo a esta conexión.	Marque el cuadro <b>Utilizar el asistente para agregar</b> y haga clic en <b>Aceptar</b> . Cisco SDM le guiará por el proceso de creación de un mapa criptográfico nuevo y lo asociará con la política IPsec.

## Asistente para mapas criptográficos: Bienvenido

Este asistente le guiará por el proceso de creación de un mapa criptográfico. Un mapa criptográfico especifica los dispositivos pares del otro extremo de la conexión VPN, define cómo se cifrará el tráfico e identifica qué tráfico se cifrará.

Haga clic en **Siguiente** para empezar a crear un mapa criptográfico.

## Asistente para mapas criptográficos: Resumen de la configuración

La página de resumen del Asistente para mapas criptográficos muestra los datos especificados en las ventanas del asistente. Puede revisarla, hacer clic en **Atrás** para regresar a una pantalla para introducir cambios y, a continuación, regresar a la ventana Resumen y hacer clic en **Finalizar** para suministrar la configuración del mapa criptográfico al router.

## Eliminar conexión

Utilice esta ventana para eliminar un túnel VPN o, sencillamente, disociarlo de una interfaz, pero conservando su definición para utilizarla en el futuro.

### Eliminar el mapa criptográfico con el número de secuencia *n* de la política IPsec *nombre de la política*

Haga clic en este botón y, a continuación, en **Aceptar** para quitar la definición del túnel VPN. Las asociaciones creadas entre la interfaz, la política IPsec y los dispositivos pares se perderán cuando ejecute esta operación. Si esta definición de túnel tiene más de una interfaz asociada, también se eliminarán dichas asociaciones.

### Eliminar el mapa criptográfico dinámico con el número de secuencia *n* del conjunto de mapas criptográficos dinámicos *nombre del conjunto*

Este botón se muestra si ha seleccionado un túnel VPN sitio a sitio dinámico. Haga clic en este botón y, a continuación, en **Aceptar** para quitar la definición del túnel VPN. Las asociaciones creadas entre la interfaz, la política IPsec y los dispositivos pares se perderán cuando ejecute esta operación. Si esta definición de túnel tiene más de una interfaz asociada, también se eliminarán dichas asociaciones.

### Anular la política IPsec *nombre de la política de la interfaz nombre de la interfaz* y conserve la política IPsec para su eventual reutilización

Haga clic en este botón y, a continuación, en **Aceptar** para conservar la definición del túnel y, a la vez, quitar su asociación de la interfaz. Si así lo desea, podrá asociar esta definición con la interfaz de otro router.

## Ping

Puede realizar un ping en un dispositivo par en esta ventana. En ella puede seleccionar el origen y el destino de la operación ping. Es posible que después de restablecer un túnel VPN, desee realizar un ping a un par remoto.

### Origen

Seleccione o especifique la dirección IP en la que desee que se origine el ping. Si la dirección que desea utilizar no se encuentra en la lista, especifique otra en el campo. El ping puede tener su origen en cualquier interfaz del router. Por defecto, el comando **ping** tiene su origen en la interfaz exterior de la conexión con el dispositivo remoto.

### Destino

Seleccione la dirección IP para la que desea realizar el ping. Si la dirección que desea utilizar no se encuentra en la lista, especifique otra en el campo.

### Para enviar un ping a un par remoto:

Especifique el origen y el destino y haga clic en **Ping**. Para saber si el ping ha sido satisfactorio, puede leer la salida del comando **ping**.

### Para borrar la salida del comando ping:

Haga clic en **Borrar**.

## Generar el reflejo...

Esta ventana muestra la política IPsec utilizada por el túnel VPN para el par seleccionado, y permite guardar la política en un archivo de texto que puede utilizar para configurar la conexión VPN en el dispositivo par.

### Dispositivo par

Seleccione la dirección IP o el nombre de host del dispositivo par para ver la política IPsec configurada para el túnel a dicho dispositivo. La política aparecerá en el cuadro situado bajo la dirección IP del par.

## Para crear un archivo de texto de la política IPsec:

Haga clic en **Guardar** y especifique el nombre y ubicación del archivo de texto. Puede suministrar este archivo de texto al administrador del dispositivo para a fin de que dicho administrador cree una política que refleje la que ha creado en el router. Haga clic en [Después de configurar una VPN, ¿cómo se configura la VPN en el router del par?](#) para saber cómo utilizar el archivo de texto para crear una política de reflejo.



### Precaución

El archivo de texto que genere no debe copiarse en el archivo de configuración del sistema remoto, sino que sólo debe utilizarse para mostrar qué se ha configurado en el router local y, de esta manera, ofrecer la posibilidad de que el dispositivo remoto pueda configurarse de forma compatible. Pueden utilizarse nombres idénticos para políticas IPsec, políticas IKE y conjuntos de transformación en el router remoto, pero las políticas y los conjuntos de transformación pueden ser diferentes. Si se copia el archivo de texto en el archivo de configuración remota, es probable que se produzcan errores de configuración.

## Advertencia de Cisco SDM: Reglas NAT con ACL

Esta ventana aparece cuando se configura una VPN mediante interfaces asociadas a reglas NAT que utilizan reglas de acceso. Este tipo de regla NAT puede cambiar las direcciones IP de los paquetes antes de que éstos dejen la LAN o entren en ella. Una regla NAT impedirá que las conexiones VPN funcionen correctamente si cambia las direcciones IP de origen y éstas no coinciden con la regla IPsec configurada para la VPN. Para evitar que esto ocurra, Cisco SDM puede convertir estas reglas en reglas NAT que utilizan mapas de ruta. Los mapas de ruta especifican las subredes que no deben traducirse.

La ventana muestra las reglas NAT que deben cambiarse para asegurarse de que la conexión VPN funciona correctamente.

### Dirección original

Dirección IP que NAT traducirá.

### Dirección traducida

Dirección IP que NAT sustituirá por la dirección original.



## Tipo de regla

Tipo de regla NAT, ya sea estática o dinámica.

### Para que las reglas NAT de la lista utilicen mapas de ruta:

Haga clic en **Aceptar**.

## Cómo...

En esta sección se incluyen procedimientos para las tareas que el asistente no le ayuda a llevar a cabo.

## ¿Cómo se crea una VPN para más de un sitio?

Puede utilizar Cisco SDM para crear varios [túneles VPN](#) en una interfaz del router. Cada túnel VPN conectará la interfaz seleccionada del router a una subred diferente del router de destino. Se pueden configurar varios túneles VPN para que se conecten a la misma interfaz pero a diferentes subredes del router de destino, o bien, se pueden configurar varios túneles VPN para conectarse a diferentes interfaces del router de destino.

Primero, es preciso crear el túnel VPN inicial. Los pasos que indicamos a continuación, describen cómo crear el túnel VPN inicial. Si ya ha creado el primer túnel VPN y necesita agregar un túnel adicional a la misma interfaz, omita el primer procedimiento y siga los pasos del procedimiento siguiente de este tema de ayuda.

### Creación del túnel VPN inicial:

- 
- Paso 1** En el panel izquierdo, seleccione **VPN**.
  - Paso 2** Seleccione **Crear una VPN sitio a sitio**.
  - Paso 3** Haga clic en **Iniciar la tarea seleccionada**.  
Se iniciará el Asistente para VPN.
  - Paso 4** Haga clic en **Configuración rápida**.
  - Paso 5** Haga clic en **Siguiente>**.

- Paso 6** En el campo **Seleccione la interfaz para esta conexión VPN**, elija la interfaz del router de origen en la que se creará el túnel VPN. Ésta es la interfaz que aparece conectada a Internet en el sistema local en el diagrama del escenario de utilización.
- Paso 7** En el campo **Identidad del par**, especifique la dirección IP de la interfaz del router de destino.
- Paso 8** En los campos **Autenticación**, escriba y vuelva a escribir la clave previamente compartida que utilizarán los dos pares VPN.
- Paso 9** En el campo **Origen**, seleccione la interfaz que se conecta a la subred cuyo tráfico IP desea proteger. Éste es el router local en el diagrama del escenario de utilización y, por lo general, se trata de una interfaz conectada a la LAN.
- Paso 10** En los campos de **Destino**, especifique la dirección IP y la máscara de subred del router de destino.
- Paso 11** Haga clic en **Siguiente>**.
- Paso 12** Haga clic en **Finalizar**.
- 

### Creación de un túnel adicional desde la misma interfaz de origen

Una vez haya creado el túnel VPN inicial, siga los pasos descritos a continuación para crear un túnel adicional desde la misma interfaz de origen a otra interfaz o subred de destino:

---

- Paso 1** En el panel izquierdo, seleccione **VPN**.
- Paso 2** Seleccione **Crear una VPN sitio a sitio**.
- Paso 3** Haga clic en **Iniciar la tarea seleccionada**.  
Se iniciará el Asistente para VPN.
- Paso 4** Haga clic en **Configuración rápida**.
- Paso 5** Haga clic en **Siguiente>**.
- Paso 6** En el campo **Seleccione la interfaz para esta conexión VPN**, elija la misma interfaz que ha utilizado para crear la conexión VPN inicial.

- Paso 7** En el campo Identidad del par, especifique la dirección IP de la interfaz del router de destino. Puede especificar la misma dirección IP que introdujo al crear la conexión VPN inicial. Esto significa que esta otra conexión VPN debe utilizar la misma interfaz en el router de destino que la conexión VPN inicial. Si no desea que las dos conexiones VPN se conecten a la misma interfaz de destino, especifique la dirección IP de otra interfaz en el router de destino.
- Paso 8** En los campos Autenticación, escriba y vuelva a escribir la clave previamente compartida que utilizarán los dos pares VPN.
- Paso 9** En el campo Origen, seleccione la misma interfaz utilizada para crear la conexión VPN inicial.
- Paso 10** En los campos Destino, dispone de las opciones siguientes:
- Si, en el campo Identidad del destino, usted introdujo la dirección IP de una interfaz diferente en el router de destino y desea proteger el tráfico IP que viene desde alguna subred específica, introduzca la dirección IP y la máscara de subred de esa subred en los campos apropiados.
  - Si usted introdujo la misma dirección IP en el campo Identidad del destino, como la que usó para la conexión de la VPN inicial indicando que este túnel de VPN usará la misma interfaz del router que el túnel de VPN inicial, después tendrá que introducir la dirección IP y la máscara de subred nueva que desea proteger en los campos apropiados.
- Paso 11** Haga clic en **Siguiente**>.
- Paso 12** Haga clic en **Finalizar**.
- 

## Después de configurar una VPN, ¿cómo se configura la VPN en el router del par?

Cisco SDM genera configuraciones **VPN** en el router. Cisco SDM incluye una función que genera un archivo de texto de la configuración, que puede utilizarse como plantilla para crear una configuración VPN para el router **par** con el que el túnel VPN se conecta. Este archivo de texto sólo puede usarse como plantilla que muestra los comandos que es preciso configurar. No se puede utilizar sin editar, ya que contiene información que sólo es correcta para el router local que configuró.

Para generar la configuración de una plantilla para el router de la VPN del par.

---

**Paso 1** En el panel izquierdo, seleccione **VPN**.

**Paso 2** Seleccione **VPN sitio a sitio** en el árbol de VPN y haga clic en la ficha Editar.

**Paso 3** Seleccione la conexión VPN que desee utilizar como plantilla y haga clic en **Generar una copia**.

Cisco SDM muestra la pantalla Generar una copia.

**Paso 4** En el campo Dispositivo par, seleccione la dirección IP del dispositivo par para el que desea generar una configuración sugerida.

La configuración sugerida para el dispositivo par aparecerá en la pantalla Generar una copia.

**Paso 5** Haga clic en **Guardar** para que se abra el cuadro de diálogo Guardar archivo de Windows y pueda guardar el archivo.




---

**Precaución**

No aplique la configuración de reflejo en el dispositivo par sin editarla. Esta configuración es una plantilla que precisa una configuración manual adicional. Utilícela sólo como punto de partida para crear la configuración del par VPN.

---

**Paso 6** Después de guardar el archivo, use un editor de textos para introducir los cambios necesarios en la configuración de la plantilla. Algunos comandos pueden necesitar edición:

- Los comandos de la dirección IP del par
- Los comandos de la política de transformación
- Los comandos de la dirección IP del mapa criptográfico
- Los comandos de la ACL
- Los comandos de la dirección IP de la interfaz

**Paso 7** Una vez que haya acabado de editar el archivo de configuración del par, súntrelo al router del par mediante un servidor TFTP.

---

## ¿Cómo se edita un túnel VPN existente?

Para editar un túnel **VPN** existente:

- 
- Paso 1** En el panel izquierdo, seleccione **VPN**.
  - Paso 2** Seleccione **VPN sitio a sitio** en el árbol de VPN y haga clic en la ficha Editar.
  - Paso 3** Haga clic en la conexión que desee editar.
  - Paso 4** Haga clic en **Agregar**.
  - Paso 5** Seleccione **Mapas criptográficos estáticos a <nombre de política>**.
  - Paso 6** En la ventana Agregar Mapas criptográficos estáticos, puede agregar más mapas criptográficos a la conexión VPN.
  - Paso 7** Si es preciso modificar algunos de los componentes de la conexión como, por ejemplo, la política IPSec o el mapa criptográfico existente, anote los nombres de los componentes en la ventana VPN y vaya a las ventanas adecuadas de Componentes VPN para efectuar los cambios.
- 

## ¿Cómo se puede confirmar que mi VPN funciona?

Se puede verificar que la conexión **VPN** funciona mediante el modo Supervisión en Cisco SDM. Si la conexión VPN funciona, el modo Supervisión mostrará la conexión VPN identificando las direcciones IP del **par** de origen y de destino. El modo Supervisión mostrará el número de paquetes transferidos en la conexión o el estado actual de ésta, en función de si la conexión VPN es un **túnel IPSec** o una asociación de seguridad (**SA**) Intercambio de claves por Internet (**IKE**). Para mostrar la información actual de una conexión VPN:

- 
- Paso 1** En la barra de herramientas, seleccione el modo **Supervisión**.
  - Paso 2** En el panel izquierdo, seleccione **Estado de la red VPN**.
  - Paso 3** En el campo Seleccionar una categoría, seleccione si desea ver información para asociaciones de seguridad IKE o túneles IPSec.

Cada conexión VPN configurada aparecerá como una fila en la pantalla.

Si está viendo información de túnel IPSec, puede verificar la información siguiente para determinar si la conexión VPN funciona:

- Las direcciones IP del par local y remoto son correctas; es decir, que la conexión VPN está entre las interfaces de router y sitios correctos.
- El estado del túnel es “activo”. Si el estado del túnel es “inactivo” o “administrativamente inactivo”, la conexión VPN no está activada.
- El número de paquetes de encapsulación y de desencapsulación no es igual a cero; es decir, los datos se han transferido por la conexión y los errores enviados y recibidos no son demasiado elevados.

Si está viendo información de una asociación de seguridad IKE, puede verificar que la conexión VPN funciona comprobando que las direcciones IP de origen y de destino sean correctas y que el estado sea “QM\_IDLE”, es decir, que se ha autenticado la conexión y que puede efectuarse la transferencia de datos.

---

## ¿Cómo se configura un par de reserva para mi VPN?

Para configurar varios [pares VPN](#) en un único [mapa criptográfico](#):

---

- Paso 1** En el panel izquierdo, seleccione **VPN**.
- Paso 2** En el árbol de VPN, seleccione **Componentes VPN** y, a continuación, **Políticas IPSec**.
- Paso 3** En la tabla Políticas IPSec, haga clic en la política IPSec a la que desea agregar otro par VPN.
- Paso 4** Haga clic en **Editar**.  
Aparecerá el cuadro de diálogo Editar la política IPSec.
- Paso 5** Haga clic en **Agregar**.
- Paso 6** Se abrirá el cuadro de diálogo Agregar mapa criptográfico para establecer los valores del mapa criptográfico nuevo. Ajuste los valores del mapa criptográfico nuevo mediante las cuatro fichas del cuadro de diálogo. La ficha Información del par contiene el campo Especificar pares, que permite especificar la dirección IP del par que desea agregar.

- Paso 7** Cuando haya acabado, haga clic en **Aceptar**.  
Aparecerá el mapa criptográfico con la nueva dirección IP del par en la tabla “Mapas criptográficos en esta política IPSec”.
- Paso 8** Para agregar pares adicionales, repita el proceso indicado de los pasos 4 a 8.
- 

## ¿Cómo se acomodan varios dispositivos con diferentes niveles de admisión de VPN?

Para agregar más de un [conjunto de transformación](#) a un único [mapa criptográfico](#):

---

- Paso 1** En el panel izquierdo, seleccione **VPN**.
- Paso 2** En el árbol de VPN, seleccione **Componentes VPN** y, a continuación, **Políticas IPSec**.
- Paso 3** En la tabla Políticas IPSec, haga clic en la política IPSec que contenga el mapa criptográfico al que desee agregar otro conjunto de transformación.
- Paso 4** Haga clic en **Editar**.  
Aparecerá el cuadro de diálogo Editar la política IPSec.
- Paso 5** En la tabla “Mapas criptográficos en esta política IPSec”, haga clic en el mapa criptográfico al que desee agregar otro conjunto de transformación.
- Paso 6** Haga clic en **Editar**.  
Aparecerá el cuadro de diálogo Editar el mapa criptográfico.
- Paso 7** Haga clic en la ficha **Conjuntos de transformación**.
- Paso 8** En el campo Conjuntos de transformación disponibles, haga clic en el conjunto de transformación que desee agregar al mapa criptográfico.
- Paso 9** Haga clic en >> para agregar el conjunto de transformación seleccionado al mapa criptográfico.
- Paso 10** Si desea agregar conjuntos de transformación adicionales a este mapa criptográfico, repita los pasos 9 y 10 hasta que haya agregado todos los conjuntos de transformación que desee.  
Haga clic en **Aceptar**.
-

## ¿Cómo se configura una VPN en una interfaz no compatible?

Cisco SDM puede configurar una [VPN](#) en un tipo de interfaz no admitido por Cisco SDM. Para poder configurar la conexión VPN, primero es preciso utilizar la [CLI](#) del router para configurar la interfaz. La interfaz deberá tener, como mínimo, una dirección IP configurada y deberá estar en funcionamiento. Para verificar que la conexión funcione, verifique que el estado de la interfaz sea activo.

Después de configurar la interfaz no admitida mediante el CLI, puede utilizar Cisco SDM para configurar la conexión VPN. La interfaz no compatible aparecerá en los campos en los que es preciso elegir una interfaz para la conexión VPN.

## ¿Cómo se configura una VPN después de configurar un firewall?

Para que una [VPN](#) funcione con un [firewall](#) in situ, es preciso configurar el firewall para permitir el tráfico entre las direcciones IP de los [pares](#) local y remoto. Cisco SDM crea esta configuración por defecto al configurar una VPN después de haber configurado un firewall.

## ¿Cómo se configura el paso de NAT (NAT Passthrough) para una VPN?

Si está utilizando [NAT](#) para traducir direcciones de redes que no son la propia y está conectando a un sitio específico situado fuera de la red mediante una [VPN](#), deberá configurar una transmisión NAT para la conexión VPN, a fin de que la traducción de la dirección de la red no se produzca en el tráfico VPN. Si ya ha configurado NAT en el router y ahora está configurando una conexión VPN nueva mediante Cisco SDM, recibirá un mensaje de advertencia que le informará que Cisco SDM configurará NAT para que no traduzca tráfico VPN. Deberá aceptar el mensaje para que Cisco SDM cree las [ACL](#) necesarias para proteger el tráfico VPN contra la traducción.



Si está configurando NAT mediante Cisco SDM y ya ha configurado una conexión VPN, ejecute el procedimiento siguiente para crear las ACL.

- 
- Paso 1** En el panel izquierdo, seleccione **Tareas adicionales/Editor ACL**.
- Paso 2** En el árbol Reglas, seleccione **Reglas de acceso**.
- Paso 3** Haga clic en **Agregar**.  
Aparecerá el cuadro de diálogo Agregar una regla.
- Paso 4** En el campo Nombre/Número, especifique un nombre o un número exclusivo para la regla nueva.
- Paso 5** En el campo Tipo, seleccione **Regla ampliada**.
- Paso 6** En el campo Descripción, introduzca una breve descripción de la nueva regla.
- Paso 7** Haga clic en **Agregar**.  
Aparecerá el cuadro de diálogo Agregar una entrada de regla estándar.
- Paso 8** En el campo Acción, seleccione **Permitir**.
- Paso 9** En el grupo Red/host de origen, del campo Tipo, seleccione **Una red**.
- Paso 10** En los campos Dirección IP y Máscara con Comodín, introduzca la dirección IP y la máscara de subred del puerto de origen de la VPN.
- Paso 11** En el grupo Red/host de destino, del campo Tipo, seleccione **Una red**.
- Paso 12** En los campos Dirección IP y Máscara comodín, especifique la dirección IP y la máscara de subred del par de destino de VPN.
- Paso 13** En el campo Descripción, introduzca una breve descripción de la red o del host.
- Paso 14** Haga clic en **Aceptar**.  
Ahora, la nueva regla aparecerá en la tabla Reglas de acceso.
-





# CAPÍTULO 10

## Easy VPN remoto

---

### Creación de Easy VPN remoto

Cisco SDM le permite configurar su router como un cliente a un servidor o concentrador de Easy VPN. Su router debe estar ejecutando una imagen del software Cisco IOS que admita la Fase II de Easy VPN.

Para poder llevar a cabo la configuración, es necesario tener a mano la información siguiente.

- Nombre de host o dirección IP del servidor Easy VPN
- Nombre de grupo IPsec
- Clave

Obtenga esta información del administrador del servidor Easy VPN.

### Configurar un cliente de Easy VPN remoto

Este asistente le guía por el proceso de configuración de un cliente de Easy VPN remoto de fase II.



**Nota**

---

Si el router no ejecuta una imagen de Cisco IOS que admita la fase II o posterior de Easy VPN remoto, no será posible configurar un cliente Easy VPN.

---

## Información del servidor

La información introducida en esta ventana identifica el túnel de la Easy VPN, el servidor o concentrador de la Easy VPN a los que se conectará el router, y la ruta que usted desea que el tráfico tome en la VPN.

### Nombre de conexión

Especifique el nombre que desea asignar a esta conexión Easy VPN. El nombre de este router debe ser exclusivo dentro de los nombres de túnel Easy VPN y no puede contener espacios ni caracteres especiales como signos de interrogación (?).

### Servidores Easy VPN

Puede especificar información para un servidor Easy VPN primario y para uno secundario.

#### Servidor Easy VPN 1

Especifique el nombre de host o la dirección IP del concentrador o servidor Easy VPN principal a los que se conectará el router. Si especifica un nombre de host, la red debe disponer de un servidor **DNS** (Domain Name System) capaz de resolver el nombre de host con la dirección IP del dispositivo par.

#### Servidor Easy VPN 2

El campo Servidor Easy VPN 2 aparece cuando la imagen de Cisco IOS del router admite la fase III de Easy VPN remoto. De lo contrario, el campo no se mostrará.

Especifique el nombre de host o la dirección IP del concentrador o servidor Easy VPN secundario a los que se conectará el router. Si especifica un nombre de host, la red debe disponer de un servidor **DNS** capaz de resolver el nombre de host con la dirección IP correcta del dispositivo par.

### Modo de operación

Elija Cliente o Extensión de la red.

Elija **Cliente** si desea que los PC y demás dispositivos de las redes internas del router formen una red privada con direcciones IP privadas. Se utilizarán los procesos de traducción de direcciones de red (**NAT**) y traducción de direcciones de puerto (**PAT**). Los dispositivos externos a la LAN no podrán efectuar ningún ping en dispositivos de la LAN ni acceder a ellos directamente.

Elija **Extensión de la red**, si desea que los dispositivos conectados con las interfaces internas tengan direcciones IP que se puedan enrutar y a las que se pueda acceder por la red de destino. Los dispositivos en ambos extremos de la conexión formarán una red lógica. PAT se desactivará automáticamente, para permitir que los equipos y los hosts en ambos extremos de la conexión tengan acceso directo entre ellos.

Consulte con el administrador del servidor o concentrador de la Easy VPN antes de seleccionar esta configuración.

Si elige Extensión de la red, podrá activar la administración remota del router, al marcar la casilla para solicitar una dirección IP asignada con servidor para su router. Esta dirección IP puede usarse para conectarse a su router correspondiente para la administración remota y la resolución de problemas (ping, Telnet, y Secure Shell). Este modo se denomina **Network Extension Plus**.

**Nota**

---

Si el router no está ejecutando una imagen de Cisco IOS que admita la Fase IV o posterior de Easy VPN remoto, no podrá ajustar Network Extension Plus.

---

## Autenticación

Use esta ventana para especificar la seguridad del túnel de Easy VPN remoto.

### Autenticación del dispositivo

Elija Certificados digitales o Clave previamente compartida.

**Nota**

---

La opción Certificados digitales sólo está disponible si está respaldada por la imagen de Cisco IOS en su router.

---

Para utilizar una clave previamente compartida, especifique el nombre del grupo IPsec. El nombre del grupo debe corresponder al nombre del grupo definido en el concentrador o servidor de la VPN. Obtenga esta información de su administrador de redes.

Especifique la clave de grupo IPsec, La Clave del grupo debe corresponder a la Clave del grupo definida en el concentrador o servidor de la VPN. Obtenga esta información de su administrador de redes. Introduzca nuevamente la Clave para confirmar su exactitud.

## Autenticación de usuario (XAuth)

La autenticación de usuario (XAuth) aparece en esta ventana, si la imagen de Cisco IOS en el router admite la Fase III de Easy VPN remoto. Si la autenticación de usuario no aparece, deberá establecerse desde la interfaz de la línea de comandos.

Elija uno de estos métodos para introducir el nombre de usuario y la contraseña de XAuth:

- Manualmente en una ventana del explorador Web



**Nota** La opción del explorador Web aparecerá solamente si es admitida por la imagen de Cisco IOS en su router.

- Manualmente desde la línea de comandos o Cisco SDM
- Automáticamente al guardar el nombre del usuario y la contraseña en el router

El servidor Easy VPN puede utilizar **Xauth** para autenticar el router. Si el servidor permite la opción de guardar contraseña, usted puede eliminar la necesidad de introducir el nombre del usuario y la contraseña cada vez que se establezca el túnel de la Easy VPN por esta opción. Introduzca el nombre del usuario y la contraseña proporcionada por el administrador del servidor de la Easy VPN, y luego, vuelva a introducir la contraseña para confirmar su precisión. La información se guarda en el archivo de configuración del router y se usa cada vez que se establezca el túnel.



### Precaución

El almacenamiento del nombre de usuario y la contraseña de autenticación ampliada (Xauth) en la memoria del router crea un riesgo de seguridad, porque todos los usuarios que tengan acceso a la configuración del router podrán obtener esta información. Si no desea que esta información se almacene en el router, no la introduzca aquí. El servidor Easy VPN simplemente exigirá al router el nombre de usuario y la contraseña cada vez que se establezca la conexión. Además, Cisco SDM no puede determinar por sí misma si el servidor Easy VPN admite la opción de guardar la contraseña. Usted debe determinar si el servidor permite esta opción. Si el servidor no admite esta opción, no debe crear un riesgo de seguridad especificando la información en esta ventana.

## Interfaces y configuración de conexiones

En esta ventana, el usuario especifica las interfaces que se utilizarán en la configuración de Easy VPN.

### Interfaces

En esta casilla seleccione las interfaces internas y externas.

#### Interfaces internas

Compruebe las interfaces internas (LAN) que sirven a las redes locales que desea incluir en esta configuración de Easy VPN. Usted puede elegir interfaces internas múltiples, con las siguientes restricciones:

- Si elige una interfaz que esté en uso en otra configuración de la Easy VPN, se le indicará que una interfaz no puede ser parte de dos configuraciones de la Easy VPN.
- Si elige interfaces que estén en uso en una configuración de la VPN, se le informará que la configuración de la Easy VPN que está creando no podrá coexistir con la configuración de la VPN existente. Se le preguntará si desea eliminar los túneles de la VPN existente desde esas interfaces y aplicarle la configuración Easy VPN.
- Una interfaz existente no aparece en interfaces, si no puede usarse en una configuración de la Easy VPN. Por ejemplo, las interfaces del bucle de prueba configuradas en el router no aparecen en esta lista.
- Una interfaz no puede asignarse tanto para una interfaz interna como para una externa.

En los puertos Cisco 800 y Cisco 1700 se admite un máximo de tres interfaces internas. En la ventana Editar Easy VPN remoto se pueden eliminar interfaces de una configuración de Easy VPN.

#### Interfaces externas

En la lista de interfaces, elija la interfaz externa que se conecta al servidor o al concentrador de Easy VPN.



#### Nota

---

Los routers Cisco 800 no admiten el uso de la interfaz E 0 como interfaz externa.

---

## Ajustes de conexión

Elija automático, manual o la activación del túnel de la VPN basado en el tráfico.

Con el ajuste manual, debe hacer clic en el botón **Conectar** o **Desconectar** en la ventana Editar Easy VPN remoto para establecer o no el túnel, aunque tendrá el control manual completo sobre el túnel en la ventana Editar Easy VPN remoto. Además, si se establece un límite de tiempo de asociación de seguridad (SA) para el router, deberá restablecer manualmente el túnel VPN siempre que se alcance un límite de tiempo. Puede cambiar la configuración del límite de tiempo de SA en la ventana Componentes de VPN [Configuración VPN global](#).

Con el ajuste automático, el túnel VPN se establece automáticamente cuando la configuración de Easy VPN se envía al archivo de configuración del router. Sin embargo, no podrá controlar el túnel manualmente en la ventana Conexiones de VPN. El botón Conectar o Desconectar se desactiva cuando se selecciona esta conexión de Easy VPN.

Con el ajuste basado en el tráfico, el túnel VPN se establece en cualquier momento que se detecte el tráfico local saliente (lado de la LAN).



### Nota

---

La opción para la activación basada en el tráfico sólo aparecerá si es admitida por la imagen de Cisco IOS en su router.

---

## Resumen de la configuración

Esta ventana muestra la configuración de Easy VPN que ha creado y permite guardarla. Aparece un resumen similar al siguiente:

```
Nombre del Túnel de Easy VPN: test1
Servidor Easy VPN: 222.28.54.7
Grupo: miCompañía
Clave: 1234
Control: Automático
Modo: Cliente
Interfaz externa: BVI222
Interfaces internas: Marcación0
```

Puede revisar la configuración en esta ventana y hacer clic en el botón **Atrás** para cambiar cualquier parámetro.



Al hacer clic en el botón **Finalizar** se grabará la información en la configuración actual del router y, si el túnel se ha configurado para funcionar en modo automático, el router tratará de contactar con el concentrador o servidor VPN.

Si desea cambiar la configuración de Easy VPN más adelante, puede realizar los cambios en la ventana Editar Easy VPN remoto.

**Nota**

---

En muchos casos, el router establecerá la comunicación con el concentrador o servidor de Easy VPN después de hacer clic en **Finalizar**, o después de hacer clic en **Conectar** en la ventana Editar Easy VPN remoto o en las ventanas de Conexiones de VPN. No obstante, si el dispositivo se ha configurado para usar **Xauth**, preguntará al router por el nombre y contraseña del usuario. Cuando ocurra esto, primero deberá proporcionar una identificación de acceso Secure Shell (SSH) y una contraseña para entrar al router y, luego, proporcionar el acceso XAuth y la contraseña correspondiente al servidor o concentrador de Easy VPN. Debe seguir este proceso cuando haga clic en **Finalizar** y la configuración se envía al router, y cuando desconecte y luego reconecte el túnel en la ventana Editar Easy VPN remoto. Averigüe si se utiliza Xauth y determine el nombre de usuario y la contraseña requeridos.

---

## Probar la conectividad de la VPN

Si decide evaluar la conexión de la VPN que acaba de configurar, los resultados de la prueba se mostrarán en otra ventana.

## Editar Easy VPN remoto

Esta ventana permite administrar las conexiones VPN. Una conexión Easy VPN es una conexión configurada entre un cliente Easy VPN y un concentrador o servidor Easy VPN para proporcionar comunicaciones seguras con otras redes que admite el servidor o concentrador.

Esta lista de conexiones muestra información acerca de las conexiones de Easy VPN remoto configuradas.

### Estado

El estado de la conexión, indicado por los iconos y alertas de texto siguientes:



La conexión está activa. Cuando una conexión Easy VPN está activa, el botón Desconectar permite desactivar la conexión si se utiliza el control de túnel manual.



La conexión está inactiva. Cuando una conexión Easy VPN está inactiva, el botón Conectar permite activar la conexión si se utiliza el control de túnel manual.



Estableciendo la conexión.

Se requiere XAuth: el concentrador o servidor Easy VPN requiere una conexión XAuth y una contraseña. Utilice el botón Conexión para especificar el ID de conexión y la contraseña, y para establecer la conexión.

Ha cambiado la configuración: la configuración de esta conexión ha cambiado y se debe enviar al router. Si la conexión usa el control de túnel manual, use el botón Conectar para establecer la conexión.

### Nombre

El nombre asignado a esta conexión Easy VPN.

### Modo

Elija **cliente** o **extensión de red**. En el modo de cliente, el concentrador o servidor de la VPN asigna una dirección IP única para el tráfico que viene desde el router; los dispositivos fuera de la LAN no tienen acceso directo a los dispositivos en la LAN. En el modo de extensión de red, el concentrador o servidor VPN no sustituye las direcciones IP y presenta una red totalmente enrutable a los homólogos del otro extremo de la conexión VPN.

## Detalles

Elija la conexión Easy VPN remoto de la lista para ver los valores de las siguientes configuraciones para esa conexión.

### Autenticación

Elija certificados digitales o Clave previamente compartida. La opción Clave previamente compartida muestra el grupo de usuarios que comparten la clave.

### Interfaz Externa

Interfaz que se conecta al servidor o concentrador de Easy VPN.

### Interfaces Internas

Interfaces internas que se incluyen en la conexión Easy VPN. Todos los hosts conectados a estas interfaces forman parte de la red VPN.

### Servidor Easy VPN

Los nombres o direcciones IP de los concentradores o servidores Easy VPN. Si la imagen de Cisco IOS del router admite la fase III de Easy VPN remoto, puede identificar dos concentradores o servidores Easy VPN durante la configuración mediante Cisco SDM.

### Compatibilidad con redes múltiples

Las direcciones de subredes que no se conectan directamente al router pero que les permite usar el túnel. Una ACL define las subredes permitidas para usar el túnel.

### Activación del túnel

Elija Automático, Manual, o basado en el tráfico.

Si la conexión se ha configurado con la opción Manual, debe hacer clic en el botón **Conectar** para establecer el túnel, aunque podrá iniciarlo o detenerlo siempre que lo desee haciendo clic en el botón **Conectar** o **Desconectar**.

Si la conexión está configurada con la opción Auto (Automático), el túnel VPN se establece automáticamente cuando se envía la configuración de Easy VPN al archivo de configuración del router. Sin embargo, el botón **Conectar** o **Desconectar** no está activado para esta conexión.

Si la conexión se configura con el ajuste basado en el tráfico, el túnel de VPN se establecerá automáticamente cuando el tráfico interno concuerde con el enrutamiento externo. Sin embargo, el botón **Conectar** o **Desconectar** no está activado para esta conexión.

**Conexión de reserva**

Conexión de reserva de Easy VPN remoto que se ha configurado. Las conexiones de reserva se configuran en la tarea de Interfaces y Conexiones de Cisco SDM.

**Método de Respuesta XAuth**

Si se activa XAuth, el valor mostrará algo tal como sigue sobre cómo se envían las credenciales XAuth:

- Se deben especificar desde Cisco SDM o consola del router
- Se deben especificar desde un explorador de PC cuando se navegue
- Las credenciales se envían automáticamente porque se han guardado en el router

**Botón Agregar**

Agrega una nueva conexión de Easy VPN remoto.

**Botón Editar**

Edita la conexión especificada de Easy VPN remoto.

**Botón Eliminar**

Elimina la conexión especificada de Easy VPN remoto.

**Botón Restablecer conexión**

Haga clic para borrar y restablecer un túnel con un destino.

**Botón Probar túnel**

Haga clic para evaluar un túnel de la VPN especificada. Los resultados del test aparecerán en otra ventana.

## Botón Conectar, Desconectar o Conexión

Este botón tiene la etiqueta Conectar si todo lo siguiente es verdadero:

- La conexión usa el control del túnel manual
- El túnel no se encuentra activo
- La respuesta XAuth *no* está establecida para que se solicite desde la sesión del explorador de un equipo

Este botón tiene la etiqueta Desconectar si todo lo siguiente es verdadero:

- La conexión usa el control del túnel manual
- El túnel se encuentra activo
- La respuesta XAuth *no* está establecida para que se solicite desde la sesión del explorador de un equipo

Este botón tiene la etiqueta Iniciar sesión si todo lo siguiente es verdadero:

- El servidor o concentrador de la Easy VPN al que está conectado usa XAuth
- La respuesta XAuth está establecida para solicitarse desde Cisco SDM o consola del router
- El túnel está esperando las credenciales XAuth (se ha iniciado la conexión)

Si la conexión está establecida para el control de túnel automático o basado en tráfico, este botón está desactivado.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Crear una nueva conexión Easy VPN.	Haga clic en <b>Agregar</b> en la ventana Editar Easy VPN remoto. Configure la conexión en la ventana Agregar Easy VPN remoto y haga clic en <b>Aceptar</b> . A continuación, haga clic en <b>Conectar</b> en esta ventana para conectarse al servidor Easy VPN.
Modificar la conexión Easy VPN existente.	En la ventana Editar Easy VPN remoto, elija la conexión que desea modificar y haga clic en <b>Editar</b> . También se recomienda consultar el procedimiento siguiente: <ul style="list-style-type: none"> <li>• <a href="#">¿Cómo se edita una conexión Easy VPN existente?</a></li> </ul>

Si desea:	Haga lo siguiente:
Eliminar una conexión Easy VPN.	En la ventana Editar Easy VPN remoto, elija la conexión que desea eliminar y haga clic en <b>Eliminar</b> .
Restablecer una conexión establecida entre el router y el homólogo VPN remoto.  Se va a quitar y restablecer la conexión.	Elija una conexión activa y haga clic en <b>Restablecer</b> . La ventana de estado que se muestra comunica si el restablecimiento se ha llevado a cabo correctamente o no.
Conectarse a un servidor Easy VPN para el cual el router tiene una conexión configurada.	<p>Si la conexión usa el control de túnel manual, elija la conexión, después haga clic en <b>Conectar</b>. Las conexiones que usan el control de túnel automático o basado en tráfico no se pueden activar manualmente a través de Cisco SDM.</p> <p><b>Nota</b> Si el servidor o concentrador de Easy VPN se configura para usar <b>Xauth</b>, el botón Conectar cambia a Iniciar Sesión, y deberá introducir el nombre del usuario y la contraseña para completar la conexión cada vez que se establezca. Obtenga esta información del administrador de redes. Si el servidor o concentrador de Easy VPN remoto solicita esta autenticación, primero deberá proporcionar una identificación de inicio de sesión Secure Shell (SSH) y la contraseña para acceder al router y, después, la conexión XAuth y la contraseña para el servidor o concentrador de Easy VPN.</p>
Desconectarse de un servidor Easy VPN para el cual el router tiene una conexión configurada.	Si la conexión usa el control de túnel manual, elija conexión, y haga clic en <b>Desconectar</b> . Las conexiones que usan el control automático o basado en tráfico no se pueden desconectar manualmente mediante Cisco SDM.
Determinar si se ha establecido una conexión Easy VPN.	El icono de conexión se muestra en la columna de estado al establecer una conexión.

Si desea:	Haga lo siguiente:
Configurar un concentrador Easy VPN. Las instrucciones de configuración para servidores y concentradores Easy VPN están disponibles en <a href="http://www.cisco.com">www.cisco.com</a> .	El siguiente enlace proporciona las líneas maestras para configurar un concentrador de la serie Cisco VPN 3000 para que funcione con un cliente Fase II de Easy VPN remoto, junto con otra información útil. <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a00800a8565.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a00800a8565.html</a> El enlace siguiente le remitirá a la documentación de Cisco VPN serie 3000. <a href="http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_getting_started_guide_book09186a00800bbe74.html">http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_getting_started_guide_book09186a00800bbe74.html</a>
Permitir el tráfico a mi concentrador de la Easy VPN mediante un firewall.	Consulte <a href="#">¿Cómo se permite que el tráfico llegue al concentrador Easy VPN a través del firewall?</a>

## Agregar o Editar Easy VPN remoto

Use esta ventana para configurar su router como un cliente de la Easy VPN. Su router debe tener una conexión a un concentrador o servidor de la Easy VPN en la red.



### Nota

Esta ventana aparece si la imagen de Cisco IOS del router admite la fase II del cliente Easy VPN.

La función Easy VPN remoto de Cisco implementa el protocolo [Unity Client](#) de Cisco, que permite definir la mayoría de los parámetros de VPN en un servidor de acceso remoto VPN. Este servidor puede ser un dispositivo VPN dedicado, como un concentrador VPN 3000 o un firewall Cisco PIX, o bien un router de Cisco IOS que admita el protocolo Unity Client de Cisco.



### Nota

- Si el concentrador o servidor Easy VPN se ha configurado para utilizar [Xauth](#), requerirá un nombre de usuario y una contraseña siempre que el router establezca la conexión, incluso cuando envíe la configuración al router y cuando desconecte y vuelva a conectar el túnel. Averigüe si se utiliza XAuth y el nombre de usuario y la contraseña requeridos.
- Si el router usa Secure Shell (SSH), usted deberá introducir el inicio de sesión y la contraseña SSH la primera vez que establezca la conexión.

## Nombre

Introduzca un nombre para la configuración de Easy VPN remoto.

## Modo

**Cliente:** elija Cliente si desea que los PC y demás dispositivos de las redes internas del router formen una red privada con direcciones IP privadas. Se utilizarán los procesos de traducción de direcciones de red (NAT) y traducción de direcciones de puerto (PAT). Los dispositivos de fuera de la LAN no podrán efectuar ningún ping en dispositivos de la LAN ni acceder a ellos directamente.

**Extensión de la Red:** elija Extensión de la Red, si desea que los dispositivos conectados con las interfaces internas tengan direcciones IP que se puedan enrutar y a las que se pueda acceder por la red de destino. Los dispositivos en ambos extremos de la conexión formarán una red lógica. PAT se desactivará automáticamente, para permitir que los PC y los hosts en ambos extremos de la conexión tengan acceso directo entre ellos.

Consulte con el administrador del servidor o concentrador de la Easy VPN antes de seleccionar esta configuración.

## Control de túneles

Elija **Auto** (Automático) o **Manual**.

Si elige la segunda opción, deberá hacer clic en el botón **Conectar** de la ventana Editar Easy VPN remoto para establecer el túnel, aunque dispondrá de control manual total sobre él en la ventana de conexiones VPN. Los botones Conectar y Desconectar están activados siempre que usted elija una conexión de la VPN con el ajuste de control manual del túnel.

Si elige la opción Auto (Automático), el túnel VPN se establece automáticamente cuando se envía la configuración de Easy VPN al archivo de configuración del router. Sin embargo, usted no podrá controlar el túnel manualmente en la ventana Conexiones de la VPN. Los botones Conectar y Desconectar se desactivan al elegir la conexión Easy VPN.



## Concentrador o Servidor de la Easy VPN

Especifique el nombre o la dirección IP del concentrador o servidor VPN al que el se conecta el router. Elija **Dirección IP**, si va a proporcionar una dirección IP o elija **Nombre del Host**, si va a proporcionar el nombre de un host del concentrador o servidor. Después especifique el valor en el campo de abajo. Si usted especifica un nombre del host, deberá existir un servidor de DNS en la red que pueda resolver el nombre del host para la dirección IP apropiada. Si indica una dirección IP, utilice el formato de decimales con puntos, por ejemplo, 172.16.44.1.

## Grupo

### Nombre del grupo

Especifique el nombre de grupo IPsec. El nombre del grupo debe corresponder al nombre del grupo definido en el concentrador o servidor de la VPN. Obtenga esta información de su administrador de redes.

### Clave de grupo

Especifique la contraseña de grupo IPsec. La contraseña de grupo debe coincidir con la contraseña de grupo definida en el servidor o concentrador VPN. Obtenga esta información de su administrador de redes.

### Confirmar clave

Vuelva a especificar la contraseña de grupo para confirmarla.

## Interfaces

### Interfaz externa hacia el servidor o concentrador

Elija la interfaz que presenta la conexión con el concentrador o servidor Easy VPN.



#### Nota

---

Los routers Cisco 800 no admiten el uso de la interfaz E 0 como la interfaz externa.

---

**Interfaces internas**

Seleccione las interfaces internas que deben incluirse en esta conexión VPN. Todos los hosts conectados a estas interfaces formarán parte de la red VPN. En los puertos Cisco 800 y Cisco 1700 se admite un máximo de tres interfaces internas.

**Nota**


---

Una interfaz no se puede designar como interfaz interna y externa al mismo tiempo.

## Agregar o Editar Easy VPN remoto: Configuración de Easy VPN

Use esta ventana para configurar su router como un cliente de la Easy VPN. Su router debe tener una conexión a un concentrador o servidor de la Easy VPN en la red.

**Nota**


---

Esta ventana aparece si la imagen de Cisco IOS del router admite la fase III del cliente Easy VPN.

La función Easy VPN remoto de Cisco implementa el protocolo [Unity Client](#) de Cisco, que permite definir la mayoría de los parámetros de VPN en un servidor de acceso remoto VPN. Este servidor puede ser un dispositivo VPN dedicado, como un concentrador VPN 3000 o un firewall Cisco PIX, o bien un router de Cisco IOS que admita el protocolo Unity Client de Cisco.

**Nombre**

Introduzca un nombre para la configuración de Easy VPN remoto.

**Modo**

Cliente: elija **Cliente** si desea que los PC y demás dispositivos de las redes internas del router formen una red privada con direcciones IP privadas. Se utilizarán los procesos de traducción de direcciones de red ([NAT](#)) y traducción de direcciones de puerto ([PAT](#)). Los dispositivos de fuera de la LAN no podrán efectuar ningún ping en dispositivos de la LAN ni acceder a ellos directamente.

Extensión de la Red: Elija **Extensión de la Red**, si desea que los dispositivos conectados con las interfaces internas tengan direcciones IP que se puedan enrutar y a las que se pueda acceder por la red de destino. Los dispositivos en ambos extremos de la conexión formarán una red lógica. PAT se desactivará automáticamente, para permitir que los PC y los hosts en ambos extremos de la conexión tengan acceso directo entre ellos.

Consulte con el administrador del servidor o concentrador de la Easy VPN antes de que elija esta configuración.

## Control de túneles

Elija **Auto** (Automático) o **Manual**.

Si elige la segunda opción, deberá hacer clic en el botón **Conectar** de la ventana Conexiones VPN para establecer el túnel, aunque dispondrá de control manual total sobre él en la citada ventana. Los botones Conectar y Desconectar están activados siempre que usted elija una conexión de la VPN con el ajuste de control manual del túnel.

Si elige la opción Auto (Automático), el túnel VPN se establece automáticamente cuando se envía la configuración de Easy VPN al archivo de configuración del router. Sin embargo, usted no podrá controlar el túnel manualmente en la ventana Conexiones de la VPN. Los botones Conectar y Desconectar se desactivan al elegir la conexión Easy VPN.

## Servidores

Usted puede especificar hasta diez servidores de la Easy VPN mediante la dirección IP o el nombre del host, y puede pedir la lista para especificar a cuáles servidores el router intenta conectarse primero.

### Agregar

Haga clic para especificar el nombre o dirección IP de un concentrador o servidor VPN al que se conectará el router y, a continuación, especifique la dirección o nombre de host en la ventana que aparece.

### Eliminar

Haga clic para eliminar la dirección IP o nombre del host especificados.

**Desplazar hacia arriba**

Haga clic para mover hacia arriba la dirección IP o nombre del host del servidor especificado en la lista. El router intentará contactarse con los routers en el orden que aparecen en esta lista.

**Desplazar hacia abajo**

Haga clic para desplazar una dirección IP o nombre de host de un servidor hacia abajo en la lista.

**Interfaz externa hacia el servidor o concentrador**

Elija la interfaz que presenta la conexión con el concentrador o servidor Easy VPN.

**Nota**


---

Los routers Cisco 800 no admiten el uso de la interfaz E 0 como la interfaz externa.

---

**Interfaces internas**

Seleccione las interfaces internas que deben incluirse en esta conexión VPN. Todos los hosts conectados a estas interfaces formarán parte de la red VPN. En los puertos Cisco 800 y Cisco 1700 se admite un máximo de tres interfaces internas.

**Nota**


---

Una interfaz no puede asignarse tanto para una interfaz interna como una externa.

---

**Agregar o Editar Easy VPN remoto: Información de autenticación**

Esta ventana aparece si la imagen de Cisco IOS del router admite la fase III del cliente Easy VPN. Si la imagen admite la fase II del cliente Easy VPN, aparece una ventana distinta.

Use esta ventana para introducir la información requerida para el router que será autenticada por el servidor o concentrador de la Easy VPN.

## Autenticación del Dispositivo

### Nombre del grupo

Especifique el nombre de grupo IPSec. El nombre del grupo debe corresponder al nombre del grupo definido en el concentrador o servidor de la VPN. Obtenga esta información del administrador de redes.

### Clave vigente

Este campo muestra asteriscos (\*) si existe un valor de clave IKE vigente, y está en blanco si no se ha configurado ninguna Clave.

### Clave nueva

Especifique una nueva clave IKE en este campo.

### Confirmar clave

Vuelva a especificar la nueva clave para confirmarla. Si los valores en el campo Clave Nueva y Confirmar Clave no son lo mismos, Cisco SDM le pedirá que introduzca los valores de la clave.

## Autenticación de usuario (XAuth)

Si el servidor o concentrador VPN se han configurado para usar [Xauth](#), requerirá un nombre de usuario y contraseña siempre que el router establezca la conexión, incluso cuando envíe la configuración al router, y cuando desconecte y reconecte el túnel. Averigüe si se utiliza XAuth y obtenga el nombre de usuario y la contraseña requeridos.

Si la autenticación del usuario no aparece, deberá establecerse desde la interfaz de la línea de comandos.

Elija uno de estos métodos para introducir el nombre del usuario de y contraseña XAuth:

- Desde un PC

Introduzca manualmente el nombre del usuario y contraseña en una ventana del explorador Web. Si elige esta opción, usted podrá marcar la casilla de verificación para usar la autenticación básica del HTTP para compensar a los exploradores Web del legado que no soportan HTML4.0 o JavaScript.



---

**Nota** La opción de Explorador Web aparecerá solamente si es admitida por la imagen de Cisco IOS en su router.

---

- Desde su router  
Introduzca manualmente el nombre del usuario y la contraseña desde la línea de comandos o Cisco SDM.
- Automáticamente al guardar el nombre del usuario y contraseña en el router  
El servidor Easy VPN puede utilizar [Xauth](#) para autenticar el router. Si el servidor permite la opción de guardar contraseña, usted puede eliminar la necesidad de introducir el nombre del usuario y la contraseña cada vez que se establezca el túnel de la Easy VPN por esta opción. Introduzca el nombre del usuario y la contraseña proporcionada por el administrador del servidor de la Easy VPN, y luego, reintroduzca la contraseña para confirmar su precisión. La información se guarda en el archivo de configuración del router y se usa cada vez que se establezca el túnel.



---

**Precaución**

Guardar el nombre del usuario y contraseña de XAuth en la memoria del router crea un riesgo para la seguridad porque cualquiera que tenga acceso a la configuración del router podrá obtener esta información. Si usted no desea que esta información se almacene en el router, no la introduzca aquí. El servidor Easy VPN simplemente exigirá al router el nombre de usuario y contraseña cada vez que se establezca la conexión. Además, Cisco SDM no puede determinar si el servidor de la Easy VPN permite que se guarden las contraseñas. Usted debe determinar si el servidor permite esta opción. Si el servidor no permite que se guarden las contraseñas, usted no deberá provocar un riesgo para la seguridad al introducir la información aquí.

---

## Especificar credenciales para SSH

Si el router usa Secure Shell (SSH), usted deberá introducir el inicio de sesión de SSH y la contraseña la primera vez que establezca la conexión. Utilice esta ventana para especificar la información de conexión SSH o Telnet.

### Especifique un nombre de usuario válido

Especifique el nombre de usuario de la cuenta SSH o Telnet que utilizará para conectarse a este router.

### Especifique una contraseña

Especifique la contraseña asociada a la cuenta SSH o Telnet que utilizará para conectarse a este router.

## Ventana Conexión a XAuth

Esta ventana aparece cuando el servidor Easy VPN solicita una autenticación ampliada. Especifique la información solicitada para responder a los desafíos como, por ejemplo, el nombre de usuario de la cuenta, contraseña o cualquier otro dato, a fin de establecer el túnel Easy VPN correctamente. Si no está seguro de la información que debe especificar, póngase en contacto con el administrador de redes VPN.

## Agregar o Editar Easy VPN remoto: Configuración general

Use esta ventana para configurar su router como un cliente de la Easy VPN. Su router debe tener una conexión a un concentrador o servidor de la Easy VPN en la red.

**Nota**

Esta ventana aparece si la imagen de IOS de Cisco en su router admite la Fase IV del Cliente de la Easy VPN.

La función Easy VPN remoto de Cisco implementa el protocolo [Unity Client](#) de Cisco, que permite definir la mayoría de los parámetros de VPN en un servidor de acceso remoto VPN. Este servidor puede ser un dispositivo VPN dedicado, como un concentrador VPN 3000 o un firewall Cisco PIX, o bien un router del Cisco IOS que admita el protocolo Unity Client de Cisco.

## Nombre

Introduzca un nombre para la configuración de Easy VPN remoto.

## Servidores

Usted puede especificar hasta diez servidores de la Easy VPN mediante la dirección IP o el nombre del host, y puede pedir la lista para especificar a cuáles servidores el router intenta conectarse primero.

Haga clic en el botón **Agregar** para especificar el nombre o dirección IP de un concentrador o servidor VPN al que se conectará el router y, a continuación, especifique la dirección o nombre de host en la ventana que aparece.

Haga clic en el botón **Eliminar** para eliminar la dirección IP especificada o nombre del host.

Haga clic en el botón **Mover hacia Arriba** para mover la dirección IP especificada o nombre del host hacia arriba en la lista. El router intentará contactarse con los routers en el orden que aparecen en esta lista.

Haga clic en el botón **Mover hacia Abajo** para mover la dirección IP especificada o nombre del host hacia abajo de la lista.

## Modo

**Cliente:** elija el modo **Cliente**, si desea que los PC y otros dispositivos en las redes internas del router formen una red privada con las direcciones IP privadas. Se utilizarán los procesos de traducción de direcciones de red ([NAT](#)) y traducción de direcciones de puerto ([PAT](#)). Los dispositivos de fuera de la LAN no podrán efectuar ningún ping en dispositivos de la LAN ni acceder a ellos directamente.

**Extensión de la Red:** elija **Extensión de la Red**, si desea que los dispositivos conectados con las interfaces internas tengan direcciones IP que puedan ser enrutadas y accedidas por la red de destino. Los dispositivos en ambos extremos de la conexión formarán una red lógica. PAT se desactivará automáticamente, para permitir que los PC y los hosts en ambos extremos de la conexión tengan acceso directo entre ellos.



Consulte con el administrador del servidor o concentrador de la Easy VPN antes de que elija esta configuración.

Si usted elige Extensión de la Red, también tiene la facultad de:

- Permitir que las subredes que no estén conectadas directamente con el router usen el túnel.

Para permitir que las subredes que no están conectadas directamente con el router usen el túnel, haga clic en el botón **Opciones** y configure las opciones de extensión de la red.

- Active la administración remota y resolución de problemas de su router.  
Puede activar la administración remota del router al marcar la casilla para solicitar una dirección IP asignada por el servidor para el router. Esta dirección IP puede usarse para conectarse a su router correspondiente para la administración remota y la resolución de problemas (ping, Telnet, y Secure Shell). Este modo se denomina **Network Extensión Plus**.

## Opciones de la Extensión de la Red

Para permitir que las subredes que no están conectadas directamente con su router usen el túnel, siga estos pasos:

- 
- Paso 1** En la ventana Opciones, marque la casilla de verificación para admitir varias subredes.
- Paso 2** Seleccione para introducir manualmente as subredes, o elija una Lista de Control de Acceso (ACL, Access Control List).
- Paso 3** Para introducir manualmente las subredes, haga clic en el botón **Agregar** e introduzca la dirección y máscara de subred. Cisco SDM generará una ACL automáticamente.



**Nota** Las subredes que especifique *no* pueden estar directamente conectadas con el router.

---

- Paso 4** Para agregar una ACL, introduzca su nombre o elíjalo de la lista desplegable.
-

## Agregar o Editar Easy VPN remoto: Información de autenticación

Use esta ventana para introducir la información requerida para el router que será autenticada por el servidor o concentrador de la Easy VPN.

### Autenticación del Dispositivo

Elija Certificados digitales o Clave previamente compartida.

Si se usa una clave previamente compartida, obtenga el nombre del grupo IPsec y el valor de la clave IKE del administrador de la red. El nombre del grupo debe corresponder al nombre del grupo definido en el concentrador o servidor de la VPN.

Introduzca el nombre del grupo de IPsec en el campo Nombre del Grupo y el nuevo valor de la Clave IKE en el campo Clave Nueva. Reintroduzca la Clave nueva para la confirmación en el campo Confirmar Clave. Si los valores en el campo Clave Nueva y Confirmar Clave no son lo mismos, Cisco SDM le pedirá que introduzca los valores de la clave.

El campo Clave Actual muestra asteriscos (\*) si existe un valor de clave IKE vigente, y está en blanco si no se ha configurado ninguna Clave.

### Autenticación del Usuario

Si el servidor o concentrador VPN se han configurado para usar [Xauth](#), requerirá un nombre de usuario y contraseña siempre que el router establezca la conexión, incluso cuando envíe la configuración al router, y cuando desconecte y reconecte el túnel. Averigüe si se utiliza XAuth y obtenga el nombre de usuario y la contraseña requeridos.

Si el servidor permite que las contraseñas se guarden, usted podrá eliminar la necesidad de introducir el nombre del usuario y la contraseña cada vez que se establezca el túnel de la Easy VPN. La información se guarda en el archivo de configuración del router y se usa cada vez que se establezca el túnel.

Elija uno de estos métodos para introducir el nombre del usuario de y contraseña XAuth:

- Manualmente en una ventana del explorador Web



---

**Nota** La opción de Explorador Web aparecerá solamente si es admitida por la imagen de Cisco IOS en su router.

---

- Manualmente desde la línea de comandos o Cisco SDM
- Automáticamente al guardar el nombre del usuario y contraseña en el router

El servidor Easy VPN puede usar [Xauth](#) para autenticar el router. Si el servidor permite guardar las contraseñas, puede eliminar la necesidad de introducir el nombre del usuario y la contraseña cada vez que se establezca el túnel de la Easy VPN mediante esta opción. Introduzca el nombre del usuario y la contraseña proporcionada por el administrador del servidor de la Easy VPN, y luego, reintroduzca la contraseña para confirmar su precisión.



---

**Nota** El campo Contraseña Actual muestra asteriscos (\*) si existe un valor de contraseña vigente, y está en blanco si no se ha configurado ninguna contraseña.

---

La información se guarda en el archivo de configuración del router y se usa cada vez que se establezca el túnel.



### Precaución

---

Guardar el nombre del usuario y contraseña de XAuth en la memoria del router crea un riesgo para la seguridad porque cualquiera que tenga acceso a la configuración del router podrá obtener esta información. Si usted no desea que esta información se almacene en el router, no la introduzca aquí. El servidor Easy VPN simplemente exigirá al router el nombre de usuario y contraseña cada vez que se establezca la conexión. Además, Cisco SDM no puede determinarse por sí mismo, si el servidor permite que se guarden las contraseñas. Usted debe determinar si el servidor permite esta opción. Si el servidor no permite que se guarden las contraseñas, usted no deberá provocar un riesgo para la seguridad al introducir la información aquí.

---

## Agregar o Editar Easy VPN remoto: Interfaces y conexiones

En esta ventana usted podrá configurar las interfaces internas y externas, y especificar cómo se levanta el túnel.

### Interfaces Internas

Elija la interfaz (LAN) interna para asociarse con esta configuración de la Easy VPN. Usted puede elegir interfaces internas múltiples, con las siguientes restricciones:

- Si usted selecciona interfaces que ya se usen en otra configuración de la Easy VPN, se le notificará que una interfaz no puede ser parte de dos configuraciones de la Easy VPN.
- Si usted elige interfaces que ya se usen en alguna configuración de la VPN estándar, se le notificará que la configuración de la Easy VPN que está creando no puede coexistir con la configuración de la VPN existente. Cisco SDM le preguntará si desea eliminar los túneles de la VPN existente de esas interfaces y aplicarles la configuración de la Easy VPN.
- Una interfaz existente no aparece en interfaces, si no puede usarse en una configuración de la Easy VPN. Por ejemplo, las interfaces del bucle de prueba configuradas en el router no aparecen en esta lista.
- Una interfaz no puede asignarse tanto para una interfaz interna como una externa.

En los puertos Cisco 800 y Cisco 1700 se admite un máximo de tres interfaces internas. En la ventana Editar Easy VPN remoto se pueden quitar interfaces de una configuración de Easy VPN.

### Interfaz Externa

Escoja la interfaz externa que se conecta al servidor o al concentrador de la Easy VPN.

**Nota**

---

Los routers Cisco 800 no soportan el uso de la interfaz E 0 como la interfaz externa.

---

### Interfaz de túnel virtual

Active esta opción si desea usar una Interfaz de túnel virtual (VTI) para esta conexión. Si las VTI que se indican en la lista son usadas por otras conexiones VPN, haga clic en **Agregar** para crear una nueva.

### Control de Conexión

Elija la activación del túnel de la VPN Automática, Manual o Tráfico interesante.

Con el ajuste manual, deberá hacer clic en el botón **Conectar** o **Desconectar** en la ventana Editar Easy VPN remoto para establecer o no el túnel, aunque tendrá el control manual completo sobre el túnel en la ventana Editar Easy VPN remoto. Además, si se establece un límite de tiempo de asociación de seguridad (SA) para el router, deberá restablecer manualmente el túnel VPN siempre que se alcance un límite de tiempo. Puede cambiar la configuración del límite de tiempo de SA en la ventana Componentes VPN [Configuración VPN global](#).

Con el ajuste automático, el túnel VPN se establece automáticamente cuando la configuración de Easy VPN se envía al archivo de configuración del router. Sin embargo, usted no podrá controlar el túnel manualmente en la ventana Conexiones de la VPN. El botón Conectar o Desconectar se desactiva cuando usted selecciona esta configuración de la conexión de la Easy VPN.

Con la activación basada en tráfico interesante, el túnel VPN se establece siempre que se detecte tráfico local saliente (lado de la LAN). El botón Conectar o Desconectar se desactiva cuando usted selecciona esta configuración de la conexión de la Easy VPN.



---

**Nota**

La opción Tráfico interesante aparece solamente si es admitida por la imagen de Cisco IOS en su router.

---

## Cómo...

Esta sección contiene procedimientos para tareas que el Asistente no le ayuda a realizar.

### ¿Cómo se edita una conexión Easy VPN existente?

Para editar una conexión remota de Easy VPN existente, siga estos pasos:

- 
- Paso 1** En el panel izquierdo, elija **VPN**.
  - Paso 2** En el árbol VPN, elija **Easy VPN remoto**.
  - Paso 3** Haga clic en la ficha **Editar equipo remoto Easy VPN** y elija la conexión que desea modificar.
  - Paso 4** Haga clic en **Editar**.  
Aparece la ventana Editar Easy VPN remoto.
  - Paso 5** En la ventana Editar Easy VPN remoto, haga clic en las fichas para desplegar los valores que desea cambiar.
  - Paso 6** Cuando haya terminado de realizar los cambios, haga clic en **Aceptar**.
- 

### ¿Cómo configuro una conexión de respaldo para una conexión de la Easy VPN?

Para configurar una conexión de respaldo para una conexión de Easy VPN remoto, el router deberá tener una RDSI y una interfaz de módem asíncrono o analógico disponible para la conexión de respaldo.

Si no se han configurado la RDSI y la interfaz de módem asíncrono o analógico, siga estos pasos:

- 
- Paso 1** En el marco izquierdo, haga clic en **Interfaces y conexiones**.
  - Paso 2** Haga clic en la ficha **Crear conexión**.

- Paso 3** Elija una RDSI y una interfaz de módem asíncrono o analógico de la lista.
- Paso 4** Haga clic en el botón **Crear nueva conexión nueva** y use el asistente para configurar la nueva interfaz.
- Paso 5** En la ventana apropiada del asistente, configure la interfaz nueva como una conexión de respaldo para una conexión de Easy VPN remoto.
- 

Si se han configurado la RDSI y la interfaz de módem asíncrono o analógico, siga estos pasos:

---

- Paso 1** En el marco izquierdo, haga clic en **Interfaces y conexiones**.
- Paso 2** Haga clic en la ficha **Editar interfaz / conexión**.
- Paso 3** Elija una RDSI y una interfaz de módem asíncrono o analógico desde la lista de interfaces configuradas.
- Paso 4** Haga clic en el botón **Editar**.
- Paso 5** Haga clic en la ficha **Conexión de respaldo** y configure la conexión de respaldo para una conexión de Easy VPN remoto.
- Paso 6** Cuando haya terminado de configurar la conexión de respaldo, haga clic en **Aceptar**.
-







# CAPÍTULO 11

## Servidor Easy VPN

---

La función Servidor Easy VPN presenta la compatibilidad del servidor en los clientes de software Cisco VPN Cliente versión 3.x y posterior y clientes de hardware Cisco VPN. Esta función permite a un usuario final remoto comunicarse mediante la política IPSec (IP Security) con cualquier gateway VPN (Virtual Private Network) del Cisco IOS. Administradas de forma centralizada, las políticas IPSec se envían al cliente mediante el servidor, lo que minimiza la configuración que debe realizar el usuario final.

El siguiente enlace proporciona información general sobre la solución Easy VPN de Cisco, y para otros enlaces para obtener información más específica:

<http://www.cisco.com/en/US/products/sw/secursw/ps5299/index.html>

## Crear un servidor Easy VPN

Este asistente le guía por los pasos necesarios para configurar un servidor Easy VPN en este router.

Este asistente le guiará en la ejecución de las siguientes tareas para configurar con éxito el servidor de una Easy VPN en este router.

- Selección de la interfaz en la cual finalizarán las conexiones del cliente y el método de autenticación usado para el servidor y los clientes de Easy VPN
- Configuración de las políticas IKE
- Configuración de un conjunto de transformación IPSec
- Configuración de la autorización de grupos y del método de búsqueda de políticas de grupo

- Configuración de la autenticación de usuario
- Configuración de servidores RADIUS externos
- Configuración de políticas para usuarios remotos que se conectan a clientes de Easy VPN

## Crear un servidor Easy VPN

Haga clic para crear una configuración de servidor Easy VPN en el router.

## Active el Botón Asistente del Servidor de Easy VPN

Haga clic para iniciar el asistente.

# Bienvenido al asistente para servidores Easy VPN

Esta ventana resume las tareas que usted realizará cuando use el asistente.

## Interfaz y Autenticación

Esta ventana le permitirá escoger la interfaz sobre la que usted desea configurar el Servidor de la Easy VPN.

Si elige una interfaz que ya esté configurada con una política IPsec de sitio a sitio, Cisco SDM mostrará un mensaje que indica que una política IPsec ya existe en la interfaz. Cisco SDM utiliza la política de IPsec existente para configurar el servidor Easy VPN.

Si la interfaz elegida es parte de una Easy VPN Remota, GREoIPsec o la interfaz DMVPN, Cisco SDM mostrará un mensaje para elegir otra interfaz.

## Detalles

Haga clic en este botón para obtener los detalles de la interfaz seleccionada. La ventana Detalles mostrará todas las reglas de acceso, políticas IPsec, reglas NAT o reglas de inspección asociadas a la interfaz.

Este botón se desactiva, cuando no se ha elegido ninguna interfaz.

## Autenticación

Elija las claves previamente compartidas, los certificados digitales, o ambos.

Si elige las claves previamente compartidas, deberá introducir un valor de la Clave cuando configure la ventana de configuración general Agregar Política de Grupo.

Si elige certificados digitales, los campos de claves previamente compartidas no aparecerán en la ventana de configuración general Agregar Política de Grupo.

Si elige tanto las claves previamente compartidas, como los certificados digitales, será opcional introducir un valor de la Clave en la ventana de configuración general Agregar Política de Grupo.

## Búsqueda de Política de grupos y Autorización de grupos

Esta ventana permite definir una nueva lista de métodos para la autorización de red AAA para la búsqueda de políticas de grupo o elegir una lista de métodos de red existente.

### Solamente local

Esta opción permite crear una lista de métodos para la base de datos local únicamente.

### Sólo RADIUS

Esta opción le permite crear una lista de los métodos para una base de datos RADIUS.

### Sólo RADIUS y Local

Esta opción le permite crear una lista de métodos tanto para la base de datos RADIUS como la local.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
<p>Definir una lista de métodos AAA para la base de datos local y RADIUS.</p> <p>Cuando defina listas de métodos para la base de datos local y RADIUS, el router buscará la autenticación de grupo primero en el servidor RADIUS y, luego, en la base de datos local.</p>	<p>Elija <b>Sólo RADIUS y Local</b>. A continuación, haga clic en <b>Siguiente</b>.</p>
<p>Definir una lista de métodos AAA para la base de datos local únicamente.</p> <p>Cuando defina listas de métodos AAA para la base de datos local, el router buscará la autenticación de grupo en la base de datos local.</p>	<p>Elija <b>Solamente local</b>. A continuación, haga clic en <b>Siguiente</b>.</p>
<p>Elegir cualquiera de las listas de métodos existentes para la autenticación de grupo.</p> <p>Si desea definir listas de métodos AAA, es recomendable que elija una lista de métodos existente.</p>	<p>Elija <b>Elegir una lista de métodos AAA existente</b>. A continuación, haga clic en <b>Siguiente</b>.</p>

## Autenticación de usuario (XAuth)

Puede configurar la autenticación de usuario en el servidor Easy VPN, y almacenar los detalles de dicha autenticación en un servidor externo, como un servidor RADIUS o una base de datos local, o en ambos. Se usa un método de autenticación de registro AAA para decidir el orden en el cual se deberán buscar los detalles de autenticación del usuario.

### Solamente local

Esta opción permite agregar detalles de la autenticación de usuario para la base de datos local únicamente.

## Sólo RADIUS y local

Esta opción permite agregar detalles de la autenticación de usuario para la base de datos local y RADIUS.

## Elegir una lista de métodos AAA existente

Esta opción permite elegir una lista de métodos de una lista en la que figuran todas las listas de métodos configuradas en el router.

La lista de métodos elegida se usa para la autenticación extendida.

## Botón Agregar Credenciales del Usuario

Haga clic para agregar una cuenta de usuario.

## Cuentas de usuario para XAuth

Agregue una cuenta para un usuario que desee autenticar una vez que IKE haya autenticado el dispositivo.

## Cuentas de usuario

Las cuentas de usuarios que XAuth autenticará se listan en este cuadro. Puede observarse el nombre de cuenta y el nivel de privilegio.

## Botones Agregar o Editar

Utilice estos botones para agregar y editar cuentas de usuario. Las cuentas de usuario pueden eliminarse en la ventana **Tareas adicionales > Acceso a router > Cuentas de usuario/Vista**.



### Nota

Las cuentas de usuario de la vista CLI existentes no pueden editarse desde esta ventana. Si necesita editar cuentas de usuario, vaya a **Tareas adicionales > Acceso a router > Cuentas de usuario/Vista CLI**.

## Agregar servidor RADIUS

Esta ventana le permite agregar un nuevo servidor RADIUS, editar o hacer ping a un servidor RADIUS existente.

### Agregar

Agregue un servidor RADIUS nuevo.

### Editar

Edite la configuración de un servidor RADIUS ya existente.

### Ping

Haga ping a un servidor RADIUS ya existente o a un servidor RADIUS recién configurado.

## Autorización de grupo: Políticas de grupos de usuarios

Esta ventana permite agregar, editar, clonar o eliminar políticas de grupo de usuario en la base de datos local.

Muestra una lista de las políticas de grupo que ya se han configurado.

### Nombre del grupo

Nombre asignado al grupo de usuarios.

### Conjunto

Nombre del conjunto de direcciones IP de las cuales una dirección IP se asigna a un usuario conectado de este grupo.

### DNS

Dirección para el Sistema de Nombre de Dominio (DNS, Domain Name System) del grupo.

Esta dirección DNS se “impone” a los usuarios que se conectan a este grupo.

## WINS

Dirección del Servicio de Nombres de Internet de Windows (WINS, Windows Internet Naming Service) del grupo.

Esta dirección WINS se “impone” a los usuarios que se conectan a este grupo.

## Nombre del Dominio

Nombre de dominio del grupo.

Este nombre de dominio se “impone” a los usuarios que se conectan a este grupo.

## Dividir lista de control de acceso

La Lista de Control de Acceso (ACL) que representa las subredes protegidas para los propósitos de división de la arquitectura de túneles.

## Temporizador inactivo

Desconectar los túneles inactivos de la VPN puede ayudar para que el Servidor de la Easy VPN funcione más eficientemente, para reutilizar los recursos sin usar.

Haga clic en la casilla de verificación **Configurar Temporizador** y especifique un valor para el tiempo máximo en que un túnel VPN podrá permanecer inactivo antes de desconectarse. Introduzca las horas en el campo izquierdo, los minutos en el campo del medio, y los segundos en el campo derecho. El tiempo mínimo permitido es 1 minuto.

## Información General del Grupo

Esta ventana permite configurar, editar y clonar políticas de grupo.

### Por favor introduzca un Nombre para Este Grupo

Especifique un nombre de grupo en el campo designado. Si se va a editar esta política de grupo, el campo estará desactivado. Si va a clonar una política de grupo, debe especificar un nuevo valor en este campo.

## Clave previamente compartida

Especifique la clave previamente compartida en los campos designados.

El campo **Clave vigente** no se puede cambiar.

**Nota**

---

No debe introducir una Clave previamente compartida, si usted está usando certificados digitales para el grupo de autenticación. Los certificados digitales también se usan para la autenticación del usuario.

---

## Información acerca del conjunto

Especifica un conjunto de direcciones IP que se usan para asignar las direcciones IP a los clientes.

### Crear un conjunto nuevo

Especifique el intervalo de direcciones IP para el conjunto de direcciones IP local en el campo Intervalo de direcciones IP.

### Seleccionar de un conjunto existente

Elija el intervalo de direcciones IP del conjunto existente de direcciones IP.

**Nota**

---

Este campo no puede editarse, si no hay ningún conjunto de direcciones IP predeterminado.

---

## Máscara de Subred (Opcional)

Introduzca una máscara de subred para enviarla con las direcciones IP destinadas a los clientes en este grupo.

## Conexiones Máximas Permitidas

Especifique el número máximo de conexiones de clientes para el Servidor de la Easy VPN de este grupo.

Cisco SDM admite un máximo de 5000 conexiones por grupo.



## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Autenticar los clientes asociados al grupo.	Especifique la clave en el campo Clave previamente compartida.
Crear un conjunto de direcciones IP que se asigne a los clientes.	Especifique el intervalo de direcciones IP en el campo Crear un conjunto nuevo en el área Información acerca del conjunto.
Elegir un intervalo de direcciones IP del conjunto existente para asignar a los clientes.	Elija el rango de la dirección IP del campo Seleccionar de un conjunto existente bajo el área Información del conjunto.

## Configuración de DNS y WINS

Esta ventana le permite especificar la información del Servicio de Nombre de Dominio (DNS, Domain Name System) y el Servicio de Nombres de Internet de Windows (WINS, Windows Internet Naming Service).

### DNS

Introduzca la dirección IP del Servidor DNS primario y secundario en los campos proporcionados. Es opcional introducir una dirección del servidor de DNS secundario.

### WINS

Introduzca la dirección IP del Servidor WINS primario y secundario en los campos proporcionados. Es opcional introducir una dirección del servidor WINS secundario.

### Nombre del Dominio

Especifique el nombre de dominio que deberá enviarse al cliente Easy VPN.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Configurar un servidor DNS.	Marque la opción <b>DNS</b> . Después, especifique las direcciones IP del servidor DNS primario y secundario en los campos proporcionados.
Configurar un servidor WINS.	Marque la opción <b>WINS</b> . Introduzca las direcciones IP del servidor WINS primario y secundario en los campos proporcionados.
Especificar el nombre que deberá enviarse al cliente Easy VPN.	Especifique el nombre de dominio en el campo <b>Nombre de dominio</b> .

## División de la arquitectura de túneles

Esta ventana permite activar la división de la arquitectura de túneles para el grupo de usuarios que desea agregar.

Se trata de la capacidad de disponer de un túnel seguro al sitio central a la vez que se dispone de túneles despejados de texto en dirección a Internet. Por ejemplo, todo tráfico originado desde el cliente se enviará a la subred de destino a través del túnel de la VPN.

También puede especificar qué grupos de listas de control de acceso representan subredes protegidas para la división de la arquitectura de túneles.

### Activar la división de la arquitectura de túneles

Esta casilla permite agregar subredes protegidas y listas de control de acceso para la división de la arquitectura de túneles.

#### Especificar las subredes protegidas

Agregue o elimine las subredes para las cuales se están enviando por un túnel los paquetes de los clientes de la VPN.

#### Elegir la lista de control de acceso de la división de arquitectura de túneles

Elija la lista de control de acceso que se utilizará para la división de la arquitectura de túneles.

## Dividir DNS

Introduzca los nombres de dominio de Internet que deberá resolverse por el servidor DNS de su red. Se aplican las siguientes restricciones:

- Se permite un máximo de 10 entradas.
- Las entradas deben estar separadas con una coma.
- No use espacios en ninguna parte de la lista de entradas.
- No se aceptan entradas duplicadas o con formatos inválidos.



**Nota**

Esta función sólo aparecerá si es admitida por la edición de IOS de su servidor de Cisco.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Activar la división de la arquitectura de túneles.	Marque la casilla <b>Activar la división de la arquitectura de túneles</b> .
Agregar una subred protegida.	Elija <b>Especificar las subredes protegidas</b> y, a continuación, haga clic en <b>Agregar</b> .
Eliminar una subred protegida.	Elija <b>Especificar las subredes protegidas</b> y, a continuación, haga clic en <b>Eliminar</b> .
Elegir la lista de control de acceso que se utilizará para la división de la arquitectura de túneles.	Elija <b>Seleccionar la lista de control de acceso de la división de arquitectura de túneles</b> y elija la lista de control de acceso de las opciones disponibles.
Utilizar el servidor DNS de la red para resolver ciertos nombres de dominio.	Marque la opción <b>Activar la división de la arquitectura de túneles</b> y especifique los nombres de dominios en el campo proporcionado. También debe establecer subredes o elegir una lista de control de acceso.

## Configuraciones del Cliente

Esta ventana le permite configurar atributos adicionales para la política de seguridad, tales como agregar o eliminar un servidor de respaldo, un Firewall Are-U-There o y un Include-Local-LAN.

**Nota**

---

Algunas de las funciones descritas abajo aparecen solamente si están respaldadas por la edición de IOS de su servidor de Cisco.

---

### Servidores de Respaldo

Puede especificar hasta 10 servidores por dirección IP o nombre de host como reserva para un servidor Easy VPN, así como ordenar la lista para controlar los servidores a los que el router intentará conectarse en primer lugar si la conexión principal al servidor Easy VPN falla.

**Agregar**

Haga clic para especificar el nombre o dirección IP del servidor Easy VPN al que se conectará el router cuando la dirección principal falle y, a continuación, especifique la dirección o nombre de host en la ventana que aparece.

**Eliminar**

Haga clic para eliminar la dirección IP o nombre del host especificados.

### Impulso de la Configuración

Usted puede especificar un archivo de configuración del cliente de la Easy VPN, al usar un URL y un número de versión. El servidor de la Easy VPN enviará la URL y el número de versión a los clientes que requieran esa información. Sólo los clientes del hardware de la Easy VPN que pertenezcan a la política del grupo que está configurando podrán solicitar la URL y el número de versión que usted introduzca en esta ventana.

Introduzca el URL del archivo de configuración en el campo de URL. La URL deberá empezar con un protocolo apropiado, y puede incluir los nombres de los usuarios y contraseñas. Los siguientes son ejemplos de URL para descargar un archivo de versión actualizada llamado sdm.exe:

- `http://username:password@www.cisco.com/go/vpn/sdm.exe`
- `https://username:password@www.cisco.com/go/vpn/sdm.exe`

- `ftp://username:password@www.cisco.com/go/vpn/sdm.exe`
- `tftp://username:password@www.cisco.com/go/vpn/sdm.exe`
- `scp://username:password@www.cisco.com/go/vpn/sdm.exe`
- `rcp://username:password@www.cisco.com/go/vpn/sdm.exe`
- `cns:`
- `xmodem:`
- `ymodem:`
- `null:`
- `flash:sdm.exe`
- `nvrám:sdm.exe`
- `usbtoken[0-9]:sdm.exe`

El intervalo de números del puerto token USB es de 0 a 9. Por ejemplo, para un token USB conectado al puerto USB 0, la URL es `usbtoken0:sdm.exe`.

- `usbflash[0-9]:sdm.exe`

El intervalo de números del puerto flash USB es de 0 a 9. Por ejemplo, para un flash USB conectado al puerto USB 0, la URL es `usbflash0:sdm.exe`.

- `disk[0-1]:sdm.exe`

El número de disco es 0 o 1. Por ejemplo, para el número de disco 0, la URL es `disk0:sdm.exe`.

- `archive:sdm.exe`
- `tar:sdm.exe`
- `system:sdm.exe`

En estos ejemplos, *username* es el nombre del usuario del sitio y *password* es la contraseña del sitio.

Introduzca el número de versión del archivo en el campo Versión. El número de versión debe estar en el rango del 1 al 32767.

## Proxy del Explorador

Usted puede especificar las configuraciones del proxy del explorador para los clientes del software de la Easy VPN. El servidor de la Easy VPN envía las configuraciones del proxy del explorador a los clientes del software de la Easy VPN, que solicitan esa información. Sólo los clientes del software de la Easy VPN que pertenezcan a la política del grupo que usted está configurando podrán solicitar las configuraciones del proxy del explorador que usted ingrese en esta ventana.

Introduzca el nombre bajo el cual se guardaron las configuraciones del proxy del explorador, o elija una de las siguientes opciones del menú desplegable:

- Elija una configuración existente  
Abre una ventana con una lista de configuraciones del proxy existentes del explorador.
- Cree una nueva configuración y elija  
Abre una ventana donde usted pueda crear nuevas configuraciones del proxy del explorador.
- Ninguno  
Borra todas las configuraciones del proxy del explorador asignados al grupo.

## Firewall Are-U-There

Puede restringir las conexiones VPN a clientes que ejecuten los firewalls personales Black Ice o Zone Alarm.

## Incluye la LAN Local

Puede permitir que una conexión de división de la arquitectura de túneles acceda a la subred local al mismo tiempo que el cliente.

## Confidencialidad Directa Perfecta (PFS, Perfect Forward Secrecy)

Active la PFS si se requiere por la asociación de seguridad IPSec, que usted está usando.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Agregar un servidor de reserva.	Haga clic en <b>Agregar</b> en el área Servidores de reserva. A continuación, agregue la dirección IP o nombre de host del servidor de reserva en la ventana que aparece.
Eliminar un servidor de reserva.	Elija el servidor de reserva que desea eliminar del área Servidores de reserva y haga clic en <b>Eliminar</b> .
Volver a ordenar servidores de reserva.	Elimine los servidores de respaldo y vuélvalos a crear en el orden que usted desee.
Activar el Firewall Are-U-There.	Marque la opción <b>Firewall Are-U-There</b> .
Activar Include-Local-LAN.	Marque la opción <b>Include-Local-LAN</b> .
Especificar el número máximo de conexiones del cliente para el grupo que usted está creando.	Especifique el número en el campo <b>Número máximo de conexiones permitidas en este grupo</b> .

## Elija las Configuraciones del Proxy del Explorador

De la lista desplegable, elija las configuraciones del proxy del explorador que desee asociar al grupo.



### Nota

Para agregar nuevas configuraciones, elija **Agregar Configuraciones del Explorador** del menú desplegable de la ventana Configuraciones del cliente, o diríjase a **Componentes VPN > Servidor Easy VPN > Configuraciones del proxy del explorador** y haga clic en **Agregar**. Para eliminar las configuraciones, diríjase a **Componentes VPN > Servidor Easy VPN > Configuraciones del proxy del explorador** y haga clic en **Eliminar**.

## Agregar o Editar Configuraciones del Proxy del Explorador

Esta ventana le permitirá agregar o editar las configuraciones del proxy del explorador.

### Nombre de las Configuraciones del Proxy del Explorador

Si está agregando las configuraciones del proxy del explorador, introduzca un nombre que aparecerá en los menús desplegables de la lista de configuraciones del proxy del explorador. Si está editando las configuraciones del proxy del explorador, el campo del nombre será de sólo lectura.

### Configuraciones del Proxy

Elija una de las siguientes opciones:

- Sin Servidor Proxy  
*No* desea que los clientes en este grupo usen un servidor proxy cuando usan el túnel de la VPN.
- Detección Automática de los Configuraciones  
Usted desea que los clientes en este grupo detecten automáticamente un servidor proxy cuando usan el túnel de la VPN.
- Configuración Proxy Manual  
Usted desea configurar manualmente un servidor proxy para los clientes en este grupo.

Si usted elige Configuración Manual del Proxy, siga estos pasos para configurar manualmente un servidor proxy:

- 
- Paso 1** Introduzca la dirección IP del servidor proxy en el campo Dirección IP del Servidor.
- Paso 2** Introduzca el número de puerto que usa el servidor proxy para recibir las solicitudes proxy en el campo Puerto.
- Paso 3** Especifique una lista de direcciones IP para las que *no* desea que los clientes usen el servidor proxy.
- Separe las direcciones con comas, y no introduzca ningún espacio.



- Paso 4** Si desea impedir que los clientes usen el servidor proxy para las direcciones locales (LAN), marque la casilla de verificación **No usar servidor proxy para direcciones locales**.
- Paso 5** Haga clic en **Aceptar** para guardar las configuraciones de proxy del explorador.
- 

## Autenticación de usuario (XAuth)

Esto le permitirá configurar atributos adicionales para la autenticación del usuario tal como el Bloqueo del Grupo, y para guardar los Atributos de la Contraseña.

### Anuncio XAuth

Introduzca el texto para un anuncio que se muestre a los usuarios durante la solicitud de XAuth.

**Nota**

Esta función sólo aparecerá si es admitida por la edición de IOS de su servidor de Cisco.

---

### Registros Máximos Permitidos por Usuario:

Especifique el número máximo de conexiones que un usuario puede establecer a la vez. Cisco SDM admite un máximo de diez registros por usuario.

### Bloqueo del grupo

Usted puede restringir a un cliente para que se comunice con el servidor de la Easy VPN solamente desde el grupo de usuarios especificado.

### Guardar Contraseña

Puede guardar el nombre de usuario y contraseña de la autenticación ampliada localmente en el cliente Easy VPN.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Restringir la conexión de usuario del grupo de usuarios específico.	Marque la opción <b>Activar el bloqueo de grupo</b> .
Guardar el nombre de usuario y la contraseña.	Marque la opción <b>Activar el almacenamiento de contraseña</b> .
Especifique el número máximo de conexiones simultáneas que un usuario puede hacer al Servidor de la Easy VPN.	Especifique el número en el campo <b>Número máximo de inicios de sesión permitidos por usuario</b>

## Actualización del Cliente

Esta ventana le permite configurar las notificaciones de actualización del software o firmware, y muestra las entradas existentes de las actualizaciones del cliente. Las entradas existentes de las actualizaciones del cliente se pueden seleccionar para editar o eliminar.

Las notificaciones se envían automáticamente a los clientes que se conecten al servidor después de que se guarde la configuración de la actualización nueva o editada. Los clientes ya conectados requerirán notificación manual. Para enviar una notificación IKE manual de disponibilidad de actualización, elija una política del grupo en la ventana políticas del grupo y haga clic en el botón **Enviar actualización**. La notificación se envía a los clientes del grupo que cumplan con los criterios de actualización.



### Nota

La ventana de actualización del cliente sólo está disponible si es admitida por la edición de IOS de su servidor de Cisco.

### Columna Tipo de Cliente

Indica el tipo de cliente para el cual se destina la revisión.

### Columna Revisiones

Muestra que revisiones están disponibles.

## Columna URL

Proporciona la ubicación de las revisiones.

## Botón Agregar

Haga clic para configurar una entrada nueva de actualización del cliente.

## Botón Editar

Haga clic para editar la entrada especificada de la actualización del cliente.

## Botón Eliminar

Haga clic para eliminar la entrada especificada de la actualización del cliente.

## Agregar o Editar Entrada de Actualización del Cliente

Esta ventana le permite configurar una entrada nueva de actualización del cliente.

## Tipo de Cliente

Introduzca un tipo de cliente o elija uno desde el menú desplegable. Los nombres del tipo de cliente son sensibles a mayúsculas y minúsculas.

Para los clientes de software, el tipo de cliente es normalmente el sistema operativo, por ejemplo, *Windows*. Para los clientes de hardware, el tipo de cliente es normalmente el número de modelo, por ejemplo, *vpn3002*.

Si usted está editando la entrada de actualización del cliente, el tipo de cliente será de sólo lectura.

## URL

Introduzca la URL que conduce a la última revisión del software o firmware. La URL deberá empezar con un protocolo apropiado, y puede incluir los nombres de los usuarios y contraseñas.

Los siguientes son ejemplos de URL para descargar un archivo de versión actualizada llamada *vpnclient-4-6.exe*:

- <http://username:password@www.cisco.com/go/vpn/vpnclient-4.6.exe>
- <https://username:password@www.cisco.com/go/vpn/vpnclient-4.6.exe>

- ftp://username:password@www.cisco.com/go/vpn/vpnclient-4.6.exe
- tftp://username:password@www.cisco.com/go/vpn/vpnclient-4.6.exe
- scp://username:password@www.cisco.com/go/vpn/vpnclient-4.6.exe
- rcp://username:password@www.cisco.com/go/vpn/vpnclient-4.6.exe
- cns:
- xmodem:
- ymodem:
- null:
- flash:vpnclient-4.6.exe
- nvram:vpnclient-4.6.exe
- usbtoken[0-9]:vpnclient-4.6.exe

El intervalo de números del puerto token USB es de 0 a 9. Por ejemplo, para un token USB conectado al puerto USB 0, la URL es `usbtoken0:vpnclient-4.6.exe`.

- usbflash[0-9]:vpnclient-4.6.exe

El intervalo de números del puerto flash USB es de 0 a 9. Por ejemplo, para un flash USB conectado al puerto USB 0, la URL es `usbflash0:vpnclient-4.6.exe`.

- disk[0-1]:vpnclient-4.6.exe

El número de disco es 0 o 1. Por ejemplo, para el número de disco 0, la URL es `disk0:vpnclient-4.6.exe`.

- archive:vpnclient-4.6.exe
- tar:vpnclient-4.6.exe
- system:vpnclient-4.6.exe

En estos ejemplos, *username* es el nombre del usuario del sitio y *password* es la contraseña del sitio.

## Revisiones

Especifique el número de revisión de la última actualización. Puede especificar múltiples números de revisión al separarlos con comas, por ejemplo, *4.3,4.4,4.5*. No use ningún espacio.

## Resumen

Esta ventana muestra la configuración del servidor Easy VPN que ha creado, y le permite guardarla. Puede revisar la configuración en esta ventana y hacer clic en el botón **Atrás** para cambiar cualquier parámetro.

Al hacer clic en el botón **Finalizar** se escribirá la información en la configuración actual del router. Si el túnel ha sido configurado para funcionar en el modo Automático, el router también trata de comunicarse con el servidor o concentrador VPN.

Si desea cambiar la configuración del servidor Easy VPN más adelante, puede realizar los cambios en el panel [Agregar o Editar el Servidor de la Easy VPN](#).

Para guardar esta configuración en la configuración actual del router y salir de este asistente, haga clic en **Finalizar**. Los cambios entrarán en efecto inmediatamente.

### Probar conectividad de la VPN después de la configuración

Haga clic para probar la conexión de la VPN que acaba de configurar. Los resultados del test aparecen en una ventana separada.

## Configuraciones del Proxy del Explorador

Esta ventana enumera las configuraciones del proxy del explorador, y muestra cómo se configuran. Usted puede agregar, editar, o eliminar las configuraciones del proxy del explorador. Use la configuración de las políticas del grupo para relacionar las configuraciones del proxy del explorador con los grupos del cliente.

### Nombre

El nombre de las configuraciones del proxy del explorador.

## Configuraciones

Muestra algo de lo siguiente:

- Sin Servidor Proxy

Los clientes no pueden usar ningún servidor proxy cuando se conecten a través del túnel de la VPN.

- Detección Automática de los Configuraciones

Los clientes intentan detectar automáticamente un servidor proxy.

- Configuración Proxy Manual

Las configuraciones se configuran manualmente.

## Detalles del Servidor

Muestra la dirección IP del servidor proxy y el número de puerto en uso.

## Desviar Direcciones Locales

Si se establece, evita que los clientes usen el servidor proxy para las direcciones locales (LAN).

## Lista de Excepciones

Lista de direcciones IP para las que *no* desea que los clientes usen el servidor proxy.

## Botón Agregar

Configura las nuevas configuraciones del proxy del explorador.

## Botón Editar

Edita las configuraciones del proxy especificadas del explorador.

## Botón Eliminar

Elimina las configuraciones del proxy especificadas del explorador. Las configuraciones del proxy del explorador asociadas con una o más políticas del grupo *no* pueden eliminarse antes de que se eliminen estas asociaciones.

# Agregar o Editar el Servidor de la Easy VPN

Esta ventana le permite ver y administrar las conexiones del servidor de la VPN Easy.

## Agregar

Haga clic en **Agregar** para agregar un nuevo servidor Easy VPN.

## Editar

Haga clic en **Editar** para editar una configuración de servidor Easy VPN existente.

## Eliminar

Haga clic en **Eliminar** para eliminar una configuración especificada.

## Columna Nombre

Nombre de la política IPsec asociada a esta conexión VPN.

## Columna Interfaz

Nombre de la interfaz utilizada en esta conexión.

## Columna Autorización de grupo

Nombre de la lista de métodos utilizado para la búsqueda de políticas de grupo.

## Columna Autenticación de usuario

Nombre de la lista de métodos utilizado para la autenticación de usuario.

## Configuración de modo

Muestra algo de lo siguiente:

- Iniciar

El router se configura para iniciar las conexiones con los clientes de Easy VPN remoto.

- Responder

El router se configura para esperar las solicitudes de los clientes de Easy VPN remoto antes de establecer las conexiones.

## Botón Probar servidor VPN

Haga clic para evaluar el túnel de la VPN elegido. Los resultados del test aparecen en una ventana separada.

## Botón Restringir Acceso

Haga clic en este botón para restringir el acceso del grupo para la conexión del Servidor de la Easy VPN especificada.

Este botón está activado sólo si se cumplen las siguientes dos condiciones:

- Hay más de una conexión del Servidor de la Easy VPN al usar la base de datos local para la autenticación del usuario.
- Hay al menos una política del grupo local configurada.

# Agregar o editar conexión de servidor Easy VPN

Esta ventana le permite agregar o editar una conexión del Servidor de la Easy VPN.

## Elija una interfaz

Si desea agregar una conexión, elija de esta lista la interfaz que va a utilizar. Si va a modificar la conexión, esta lista estará desactivada.



## Elegir una política IPSec

Si va a agregar una conexión, elija de esta lista la política IPSec que desea utilizar. Si va a modificar la conexión, esta lista estará desactivada.

## Lista de métodos para la búsqueda de políticas de grupo

En esta lista, elija la lista de métodos que desea utilizar para la búsqueda de políticas de grupo. Este tipo de listas se configuran haciendo clic en **Tareas adicionales** de la barra de tareas de Cisco SDM, a continuación, en el nodo AAA.

## Activar la autenticación de usuario

Marque esta casilla de verificación si usted desea que los usuarios se autenticuen por sí mismos.

## Lista de métodos para la autenticación de usuarios

En esta lista, elija la lista de métodos que desea utilizar para la autenticación de usuario. Este tipo de listas se configuran haciendo clic en **Tareas adicionales** de la barra de tareas de Cisco SDM, a continuación, en el nodo AAA.

## Configuración de modo

Marque la opción **Iniciar** si desea que el router inicie conexiones con los clientes de Easy VPN remoto.

Marque la opción **Responder** si desea que el router espere las solicitudes procedentes de los clientes de Easy VPN remoto antes de establecer conexiones.

## Restringir Acceso

Esta ventana le permite especificar qué políticas del grupo se permiten para usar la conexión de la Easy VPN.

Permite un acceso del grupo para la conexión del Servidor de la Easy VPN, al marcar su casilla de verificación. Niega un acceso del grupo para la conexión del Servidor de la Easy VPN, al desactivar su casilla de verificación.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Restringir una política de grupo a una conexión de servidor Easy VPN Server específico mientras que deniega todas las demás políticas de grupo a esa conexión.	Elija la conexión de servidor Easy VPN especificada y haga clic en el botón <b>Restringir Acceso</b> . Marque la casilla de verificación del grupo objetivo y desmarque la de los demás grupos. Deniegue el acceso al grupo objetivo en todas las demás conexiones de servidor Easy VPN. Para ello, desmarque las casillas de verificación de la ventana Restringir Acceso de cada una de las conexiones.

# Configuración de políticas de grupo

Esta ventana le permite ver, agregar, duplicar, y elegir las políticas del grupo para editar o eliminar. Las políticas del grupo se usan para identificar los recursos de los clientes de Easy VPN remoto.

## Botón Conjunto común

Haga clic para designar un conjunto existente como conjunto común para todas las políticas de grupo que se van a utilizar. Si no se ha configurado ningún conjunto local, este botón se desactivará. Los conjuntos pueden configurarse, al hacer clic en **Tareas adicionales > Conjuntos locales**, o cuando configure las conexiones de servidor Easy VPN.

## Botones Agregar/Editar/Clonar/Eliminar

Utilice estos botones para administrar políticas de grupo en el router. Si hace clic en **Clonar** aparecen las fichas de edición de políticas de grupo.

## Botón Enviar Actualización

Haga clic para enviar una notificación IKE de las actualizaciones del software o hardware para activar a los clientes del grupo elegido. Si se desactiva este botón, el grupo elegido no tendrá configurada la actualización del cliente.

Para configurar las notificaciones de actualización del cliente para el grupo elegido, haga clic en el botón **Editar** y, luego, haga clic en la ficha **Actualización del Cliente**.

## Columna Nombre del grupo

El nombre de la política de grupo.

## Columna Conjunto

El conjunto de direcciones IP utilizadas por los clientes de este grupo.

## Columna DNS

Los servidores DNS utilizados por los clientes de este grupo.

## Columna WINS

Los servidores WINS utilizados por los clientes de este grupo.

## Columna Nombre de dominio

El nombre de dominio utilizado por los clientes de este grupo.

## Columna ACL

Si para este grupo se especifica la división de la arquitectura de túneles, esta columna podrá contener el nombre de una lista de control de acceso que defina qué tráfico deberá cifrarse.

## Ventana de Detalles

La ventana Detalles es una lista de configuraciones de funciones y sus valores para la política de grupo elegida. Las configuraciones de las características sólo se muestran si son admitidas por la edición de IOS de su router Cisco, y se aplican solamente al grupo elegido. Las siguientes configuraciones de las funciones pueden aparecer en la lista:

- Autenticación  
Los valores indican una clave previamente compartida, si se configuró alguna, o un certificado digital, si no se configuró la clave previamente compartida.
- Conexiones Máximas Permitidas  
Muestra el número máximo de conexiones simultáneas permitidas. Cisco SDM admite un máximo de 5000 conexiones simultáneas por grupo.
- Restricción de Acceso  
Muestra la interfaz externa a la que se restringe el grupo especificado.
- Servidores de Respaldo  
Muestra la dirección IP de los servidores de respaldo que se han configurado.
- Firewall Are-U-There  
Restringe las conexiones a los dispositivos que activan a los firewalls Black Ice o Zone Alarm.
- Incluye la LAN Local  
Permite que una conexión que *no* use la división de la arquitectura de túneles pueda acceder a la subred local al mismo tiempo que el cliente.
- Confidencialidad Directa Perfecta (PFS, Perfect Forward Secrecy)  
PFS se requiere para IPsec.
- Configuración Push, URL, y Versión  
El servidor envía un archivo de configuración de la URL y con el número especificado de la versión para el cliente.
- Bloqueo del grupo  
Los clientes se restringen al grupo.

- Guardar Contraseña  
Las credenciales XAuth pueden guardarse en el cliente.
- Registros Máximos  
El número máximo de conexiones que un usuario puede establecer simultáneamente. Cisco SDM admite un máximo de 10 registros simultáneos por usuario.
- Anuncio XAuth  
El mensaje de texto mostrado a los clientes durante las solicitudes de XAuth.

## Conjuntos IP

En esta ventana se muestra una lista de los conjuntos de direcciones IP disponibles para las políticas de grupo en el router. De acuerdo con el área de Cisco SDM en la que esté trabajando, los botones **Agregar**, **Editar** y **Eliminar** pueden estar disponibles y el nombre de la ventana puede cambiar según el área de Cisco SDM en que está trabajando. Puede utilizar estos botones para administrar los conjuntos IP del router.

### Columna Nombre del conjunto

El nombre del conjunto de direcciones IP.

### Columna Intervalo de direcciones IP

El intervalo de direcciones IP para el conjunto seleccionado. Un intervalo de 2.2.2.0 a 2.2.2.254 proporciona 255 direcciones.

### Columna Tamaño caché

El tamaño de la caché de este conjunto.

### Columna Nombre del grupo

Si el conjunto local está configurado con la opción de grupo mediante el CLI, el nombre del grupo se mostrará en la columna de nombre del grupo. Esta columna no se muestra en todas las áreas de Cisco SDM.



#### Nota

No puede configurar conjuntos locales con la opción de grupo utilizando Cisco SDM.

## Agregar o editar conjunto local IP

Esta ventana le permite crear o editar un conjunto local de las direcciones IP.

### Nombre del conjunto

Si está creando un conjunto, especifique el nombre del conjunto. Si se está editando un conjunto, este campo estará desactivado.

### Intervalo de direcciones IP

Especifique o edite los intervalos de direcciones IP del conjunto en esta área. Un conjunto puede contener varios intervalos de direcciones IP. Utilice los botones Agregar, Editar y Eliminar para crear intervalos adicionales, editar intervalos y eliminar intervalos de direcciones IP.

### Tamaño caché

Especifique o edite el tamaño de la caché de este conjunto en este campo.

## Agregar intervalo de direcciones IP

Esta ventana le permite agregar el rango de una dirección IP a un conjunto existente.

### Dirección IP inicial

Especifique la dirección IP con el número más bajo del intervalo.

### Dirección IP final

Especifique la dirección IP con el número más alto del intervalo.



# CAPÍTULO 12

## Enhanced Easy VPN

---

Las siguientes secciones describen las pantallas de configuración de Administrador del dispositivo de seguridad de Cisco para Enhanced Easy VPN.

### Interfaz y Autenticación

Especifica la interfaz del router en la cual la interfaz de plantilla virtual no se va a numerar, y el método que se debe usar para autenticación en esta ventana.

#### Interfaz

No se debe numerar la interfaz de plantilla virtual en una interfaz del router para obtener una dirección IP.

Cisco recomienda no numerar la interfaz de plantilla virtual en una dirección de retrobucle para mayor flexibilidad. Para hacerlo, haga clic en **No numerado en la nueva interfaz de retrobucle** y especifique una dirección IP y una máscara de subred para la interfaz de retrobucle. Un ejemplo de dirección IP y máscara de subred de retrobucle es 127.0.0.1, 255.255.255.0.

Para no numerar la interfaz de plantilla virtual en otra interfaz, haga clic en **No numerado en** y elija la interfaz. Debe seleccionar la interfaz que finaliza el túnel en el router. Haga clic en **Detalles** para ver la dirección IP, autenticación, política y otra información acerca de la interfaz que está eligiendo.

## Autenticación

Seleccione el método que los clientes de Easy VPN usarán para autenticarse a sí mismos en el servidor de Easy VPN configurado en el router. Las claves compartidas previamente requieren que comunique la clave a los administradores de los clientes de Easy VPN. Los certificados digitales no requieren esto, pero cada cliente debe suscribirse a un certificado digital y recibirlo.

## Servidores RADIUS

Identifique los servidores [RADIUS](#) que el router usará para autorización y búsqueda de políticas de grupo, y los grupos VPN configurados en los servidores RADIUS de la ventana Servidores RADIUS.

## Origen de cliente RADIUS

Configurar el origen RADIUS le permite especificar la dirección IP del origen que se enviará en paquetes RADIUS con destino al servidor RADIUS. Para ver la dirección IP y otra información acerca de una interfaz, seleccione la interfaz y haga clic en el botón **Detalles**.

La dirección IP del origen en los paquetes RADIUS enviados desde el router debe configurarse como la dirección IP del NAD en la versión 3.3 o superior de Cisco Access Control Server ([ACS](#)).

Si selecciona **El router elige el origen**, la dirección IP del origen en los paquetes RADIUS será la dirección de la interfaz a través de la cual los paquetes RADIUS saldrán del router.

Si elige una interfaz de router específica, la dirección IP del origen en los paquetes RADIUS será la dirección de esa interfaz.



### Nota

---

El software Cisco IOS permite que una interfaz de origen RADIUS se configure en el router. Si el router ya tiene configurado un origen RADIUS y usted escoge un origen diferente a la dirección IP del origen colocada en los paquetes enviados al servidor RADIUS, se cambiará a la dirección IP del nuevo origen, y podrá no coincidir con la dirección IP del NAD configurada en Cisco ACS.

---



## Columnas de Servidor IP, Parámetros y Seleccionar

Estas columnas muestran la información clave acerca de los servidores RADIUS que utiliza el router. La columna IP del servidor enumera las direcciones IP de cada servidor configurado. La columna Parámetros enumera los puertos de autorización y de cuentas para cada servidor. La columna Seleccionar contiene una casilla de verificación para cada servidor configurado. Marque la casilla junto a cada servidor que desea usar. La siguiente tabla contiene un ejemplo de datos.

IP del servidor	Parámetros	Seleccionar
192.168.108.14	Puerto de autorización 1645; Puerto de cuentas 1646	Seleccionado
192.168.108.15	Puerto de autorización 3005; Puerto de cuentas 3006	

En esta configuración, el servidor RADIUS en 192.168.108.14 utiliza la autorización estándar y los puertos de cuentas 1645 y 1646, respectivamente. El router utilizará este servidor para autenticación y autorización. El servidor en 192.168.108.15 utiliza puertos de autenticación y autorización no estándar. El router no contactará a este servidor, porque la casilla Seleccionar no está marcada.

Haga clic en **Agregar** para crear una entrada para un servidor RADIUS. Seleccione una entrada del servidor y haga clic en **Editar** para cambiar la información que el router tiene para ese servidor. Seleccione una entrada del servidor y haga clic en **Enviar un ping** para probar la conexión entre el router y el servidor RADIUS.

## Grupos VPN en el Servidor RADIUS

Especifique los grupos VPN configurados en el servidor RADIUS a los cuales desea que esta conexión otorgue acceso. Utilice coma para separar las entradas. A continuación, se muestra un conjunto de entradas:

WGP-1, WGP-2, ACCTG, CSVG

Estos nombres deben coincidir con los nombres de los grupos configurados en el servidor RADIUS. Para facilitar la administración, éstos deben coincidir también con los nombres de los grupos que configura para los clientes de Easy VPN.

## Políticas de Grupo de usuarios y Autorización de grupos

Puede crear grupos de usuarios donde cada uno tenga su propio grupo de direcciones IP, configuración de actualización de clientes, configuración de división de arquitectura de túneles y otras configuraciones personalizadas. Estos atributos de grupos se descargan para el cliente en aquél grupo donde se conectan al servidor Easy VPN. El mismo nombre de grupo se debe configurar en los clientes que son miembros del grupo para asegurar que se descarguen los atributos de grupo correctos.

Si ya se han configurado políticas de grupo, éstas aparecen en la lista de esta ventana y puede seleccionarlas para esta conexión marcando la casilla Seleccionar a la izquierda del nombre del grupo.

En la lista se muestra el nombre del grupo, el nombre del grupo de direcciones IP, los nombres de los servidores DNS y WINS, y el nombre del dominio de cada grupo configurado. Cuando hace clic en **Agregar** para configurar los ajustes para un nuevo grupo o en **Editar** para cambiar los ajustes, los cambios aparecen en esta lista. Para usar los ajustes de un grupo existente como base de una nueva configuración de grupo, seleccione el grupo existente y haga clic en **Clonar**. Los botones Agregar, Editar y Clonar muestran cuadros de diálogo que permiten configurar ajustes de grupos.

### Configurar temporizador de inactividad

Marque **Configurar temporizador de inactividad** para especificar cuánto tiempo se debe mantener una conexión para clientes inactivos en el campo Temporizador de inactividad. Especifique valores de tiempo en el formato HH:MM:SS. Por ejemplo, para especificar 3 horas, 20 minutos y 32 segundos, especifique los siguientes valores en los campos:

03:20:32

El valor de límite de tiempo se aplicará a todos los grupos configurados para esta conexión.

## Agregar o Editar servidor Easy VPN: Ficha General

Especifique información general para la conexión del servidor Easy VPN en este cuadro de diálogo.

### Nombre de esta conexión

Especifique un nombre para identificar esta conexión. El nombre que introduce se muestra en la ventana Editar servidor Easy VPN.

### Dirección IP de la interfaz de túnel virtual

Haga clic en [Interfaz y Autenticación](#) para obtener una descripción de los campos de dirección IP del túnel virtual.

### Modo túnel

Seleccione **IPSec-IPV4** en el campo Modo túnel. La opción IPSec-IPV4 permite la creación de un túnel [IPSec](#), versión 4, de IP.

### Descripción

Puede especificar una descripción que sea de utilidad para los administradores de su red cuando cambian configuraciones o solucionan problemas de la red.

## Agregar o Editar servidor Easy VPN: Ficha IKE

El cuadro de diálogo [IKE](#) en el diálogo Agregar servidor Easy VPN le permite crear un [Perfil IKE](#) para esta conexión.

### Tipo de identidad de coincidencia

El perfil IKE incluye criterios de coincidencia que permiten al router identificar las conexiones entrantes y salientes a las cuales se aplicarán los parámetros de conexión IKE. Los criterios de coincidencia se pueden aplicar actualmente a los grupos VPN. El grupo se selecciona automáticamente en el campo Tipo de identidad de coincidencia.

Haga clic en **Agregar** para crear una lista de los grupos que desea incluir en los criterios de coincidencia.

Seleccione **Agregar nombre de grupo externo** para agregar el nombre a un grupo que no está configurado en el router y, a continuación, especifique el nombre en el diálogo que aparece.

Elija **Seleccionar entre los grupos locales** para agregar el nombre de un grupo que está configurado en el router. En el diálogo que aparece, seleccione la casilla al lado del grupo que desea agregar. Si todos los grupos locales se usan en otros perfiles IKE, SDM le informa que todos los grupos han sido seleccionados.

### Configuración de modo

Seleccione **Responder** en el campo Configuración de modo si el servidor Easy VPN responderá a solicitudes de configuración de modo.

Seleccione **Iniciar** si el servidor Easy VPN iniciará solicitudes de configuración de modo.

Seleccione **Ambos** si el servidor Easy VPN iniciará y responderá a solicitudes de configuración de modo.

### Política de autorización de búsqueda de políticas de grupo

Debe especificar una política de autorización que controle el acceso a información de políticas de grupo en el servidor AAA. Seleccione **por defecto** si desea otorgar acceso a información de búsqueda de políticas de grupo. Para especificar una política, seleccione una política existente en la lista o haga clic en **Agregar** para crear una política en el diálogo que aparece.

### Política de autenticación de usuario

Puede especificar una política de autenticación de usuario que se utilizará para conexiones a Xauth. Seleccione **por defecto** si desea permitir conexiones XAuth. Para especificar una política para controlar conexiones XAuth, seleccione una política existente en la lista o haga clic en **Agregar** para crear una política en el diálogo que aparece.

## Descubrimiento de par inactivo

Haga clic en **Descubrimiento de par inactivo** para que el router pueda enviar mensajes de descubrimiento de par inactivo (**DPD**) a los clientes de Easy VPN remoto. Si un cliente no responde a los mensajes DPD, se rechaza la conexión.

Especifique el número de segundos entre los mensajes PDP en el campo Intervalo “keepalive”. El intervalo oscila entre 10 y 3600 segundos.

En el campo Reintentos, especifique el número de segundos entre reintentos si fallan los mensajes PDP. El intervalo oscila entre 2 y 60 segundos.

El descubrimiento de par inactivo ayuda a administrar conexiones sin la intervención del administrador, pero genera paquetes adicionales que ambos pares deben procesar para mantener la conexión.

## Agregar o Editar servidor Easy VPN: Ficha IPSec

Especifique la información para crear un perfil IPSec en este diálogo. Un perfil **IPSec** especifica cuáles conjuntos de transformación se usarán, cómo se determinará el tiempo de vida de la asociación de seguridad (**SA**), y otra información.

### Columnas Conjunto de transformación

Use las dos columnas que se encuentran en la parte superior del diálogo para especificar los conjuntos de transformación que desea incluir en el perfil. La columna izquierda contiene los conjuntos de transformación configurados en el router. Para agregar un conjunto de transformación configurado al perfil, selecciónelo y haga clic en el botón >>. Si no hay conjuntos de transformación en la columna izquierda, o si necesita un conjunto de transformación que no ha sido creado, haga clic en **Agregar** y cree el conjunto de transformación en el diálogo que aparece.

### Tiempo de vida de SA de IPSec basado en tiempo

Haga clic en **Tiempo de vida de SA de IPSec basado en tiempo** si desea que se establezca una nueva SA después de transcurrido un período de tiempo establecido. Especifique el período de tiempo en los campos HH:MM:SS que se encuentran a la derecha. El intervalo oscila entre 0:2:0 (2 minutos) y 24:0:0 (24 horas).

## Tiempo de vida de SA de IPSec basado en volumen de tráfico

Haga clic en **Tiempo de vida de SA de IPSec basado en volumen de tráfico** si desea que se establezca una nueva SA después de que una cantidad de tráfico especificada haya pasado a través del túnel IPSec. Especifique el número de kilobytes que debe pasar por el túnel antes de quitar una SA existente y establecer otra nueva. El intervalo oscila entre 2560 KB y 536870912 KB.

## Tiempo de inactividad de SA de IPSec

Haga clic en Tiempo de inactividad de SA de IPSec si desea que se establezca un nuevo SA después de que el par haya estado inactivo durante un tiempo especificado. Especifique el período de tiempo de inactividad en los campos HH:MM:SS que se encuentran a la derecha. El intervalo oscila entre 0:1:0 (un minuto) y 24:0:0 (24 horas).

## Confidencialidad directa perfecta

Haga clic en **Confidencialidad directa perfecta** si IPSec debe requerir confidencialidad directa perfecta ([PFS](#)) al solicitar nuevas asociaciones de seguridad para esta interfaz de plantilla virtual, o si debe requerir PFS en solicitudes recibidas desde el par. Puede especificar los valores siguientes:

- grupo 1: el grupo de módulos principales Diffie-Hellman de 768 bits se usa para cifrar la solicitud PFS.
- grupo 2: el grupo de módulos principales Diffie-Hellman de 1024 bits se usa para cifrar la solicitud PFS.
- grupo 5: el grupo de módulos principales Diffie-Hellman de 1536 bits se usa para cifrar la solicitud PFS.

## Crear interfaz de túnel virtual

Especifique la información para una interfaz de túnel virtual en este cuadro de diálogo.

### Tipo de interfaz

Seleccione **por defecto** o **túnel** como el tipo de interfaz. Si está editando una interfaz de túnel virtual, se muestra el valor configurado y el campo es de sólo lectura.

## Configurar la dirección IP de la interfaz

La dirección IP de la interfaz de túnel virtual se puede no numerar en otra interfaz o puede no tener dirección IP. Seleccione **IP no numerada** y elija un nombre de interfaz en el campo No numerado en, o seleccione **Sin dirección IP**.

## Modo túnel

Cisco SDM actualmente admite el modo túnel IPsec-IPv4 y éste está seleccionado.

## Seleccionar zona

Este campo aparece cuando el router ejecuta una imagen de Cisco IOS que admite Firewall basado en política de zonas (**ZPF**), y una zona se ha configurado en el router. Si desea que esta interfaz de túnel virtual sea un miembro de la zona, haga clic en el botón a la derecha de este campo. Haga clic en **Seleccionar una zona** y seleccione la zona de la cual desea que la interfaz sea miembro, o haga clic en **Crear una zona** para crear una nueva zona para esta interfaz.



---

**Nota**

No es necesario que la interfaz de túnel virtual sea miembro de una zona. Sin embargo, el router no envía tráfico entre interfaces miembros de zonas e interfaces que no son miembros de zonas.

---







# CAPÍTULO 13

## DMVPN

---

Estos temas de ayuda ofrecen información sobre las pantallas de configuración de la red privada virtual multipunto dinámica (DMVPN).

## Red privada virtual multipunto dinámica (DMVPN)

Este asistente le ayudará a configurar el router como un hub de red privada virtual multipunto (**DMVPN**) o spoke DMVPN. Una conexión VPN es un túnel IPsec de punto a punto que conecta dos routers. DMVPN permite crear una red con un **hub** central que conecta otros routers remotos, denominados **spokes**, mediante un túnel GRE sobre IPsec. El tráfico IPsec se enruta a través del hub a los spokes de la red. Cisco SDM permite configurar el router como hub DMVPN principal o secundario, o bien como un router spoke en una red DMVPN.

El enlace siguiente contiene más información acerca de DMVPN (se requiere ID de conexión a CCO).

### [Redes privadas virtuales IPsec multipunto](#)

Cisco SDM admite la configuración de una red centro-radial (hub-and-spoke) DMVPN que utilice los perfiles de IPsec para definir el cifrado. Puede configurar una red DMVPN de malla completa y utilizar mapas criptográficos para definir el cifrado en la red DMVPN mediante el CLI. Las redes DMVPN de malla completa y redes DMVPN mediante mapas criptográficos se administran y modifican mediante el CLI. Cisco SDM admite la configuración de una red DMVPN a partir de la versión de IOS 12.2(13)T.

Cisco SDM admite la configuración de una **DMVPN única** en un router.

En esta pantalla, identifique el router como un [hub](#) o como un [spoke](#) en la red [DMVPN](#).

Es importante configurar el hub en primer lugar porque los spokes deben configurarse con la información acerca de éste. Si desea configurar uno, puede utilizar la función de configuración de spoke disponible en la ventana Resumen para generar un procedimiento que puede enviar a los administradores de spokes para que puedan configurar los spokes con la información de hub correcta. Si desea configurar un spoke, debe obtener los datos correctos acerca del hub antes de empezar.

### Crear un spoke (cliente) en una DMVPN

Seleccione esta opción si el router es un spoke de la red [DMVPN](#). Los spokes son los puntos finales lógicos de la red. Antes de empezar la configuración, debe efectuar un ping en el hub para asegurarse de que dispone de conectividad, así como tener a mano toda la información necesaria acerca de la configuración de hub que utilizará. Esta información se muestra en [Asistente para spokes de privada virtual multipunto dinámica](#).

### Crear un hub (servidor o extremo de transmisión) en una DMVPN

Seleccione esta opción si el router es un hub de la red [DMVPN](#). El hub es el punto central lógico de una red DMVPN, y está conectado a cada uno de los routers spoke por medio de una conexión IPsec de punto a punto. El hub puede enrutar el tráfico IPsec entre los routers spoke de la red.

## Asistente para hubs de red privada virtual multipunto dinámica

Este asistente puede ayudarle a configurar el router como un hub [DMVPN](#).

Es necesario configurar el hub antes de los spokes para que pueda facilitar a los administradores de spokes la información necesaria para configurar los routers spoke.

La ventana de aplicación explica los elementos que se configurarán. Una vez finalizada la configuración, deberá facilitar a los administradores de spokes la información siguiente acerca del hub:

- La dirección IP de la interfaz física del router hub.
- La dirección IP de la interfaz de túnel mGRE del hub.

- El protocolo de enrutamiento dinámico que se utilizará para enviar actualizaciones de enrutamiento a la red DMVPN, así como el número de sistema autónomo (AS) (para EIGRP) o ID de proceso (para OSPF) que se deberá utilizar.

La función de configuración de spoke de Cisco SDM permite crear un archivo de texto con la información que los administradores de spokes necesitan acerca de la configuración del hub. Esta función está disponible desde la ventana Resumen de este asistente.

También necesita indicar a los administradores de spokes la máscara de subred que se debe utilizar y asignar a cada spoke una dirección IP de la misma subred que el hub para que no se produzcan conflictos de direcciones.

## Tipo de hub

Las redes [DMVPN](#) pueden configurarse con un único hub, o bien con un hub principal y uno de reserva. Identifique el tipo de hub como el que desea configurar el router.

### Hub principal

Marque esta opción si el router es el [hub](#) principal de la red DMVPN.

### Hub de reserva

Marque este botón si el router es un hub de reserva en una red DMVPN de malla completa.

## Configurar la clave previamente compartida

Los pares DMVPN pueden utilizar una [clave previamente compartida](#) o certificados digitales para la [autenticación](#) de las conexiones entre sí. Si se utilizan claves previamente compartidas, cada router hub y router spoke de la red deberán utilizar la misma clave previamente compartida.

Las claves previamente compartidas deben intercambiarse con el administrador del sitio remoto mediante algún método cómodo y seguro como, por ejemplo, un mensaje de correo electrónico cifrado. Los signos de interrogación (?) y los espacios no pueden utilizarse en la clave previamente compartida. La clave previamente compartida puede contener un máximo de 128 caracteres.

## Clave previamente compartida

Especifique la clave previamente compartida utilizada en la red [DMVPN](#). Los signos de interrogación (?) y los espacios no pueden utilizarse en la clave previamente compartida. La clave previamente compartida puede contener un máximo de 128 caracteres.

## Certificados digitales

Seleccione este botón si el router utiliza certificados digitales para la autenticación. Los certificados digitales se configuran en Componentes VPN>Infraestructura de clave pública.

## Confirmar la clave previamente compartida

Vuelva a especificar la clave para confirmarla. Si los valores de este campo y el de Clave previamente compartida no coinciden, Cisco SDM le solicita que los especifique de nuevo.

## Configuración de la interfaz de túnel GRE de hub

La encapsulación genérica de enrutamiento multipunto ([mGRE](#)) se utiliza en una red [DMVPN](#) para permitir que una interfaz GRE única de un [hub](#) admita un túnel IPSec hacia cada uno de los routers [spoke](#). Este punto simplifica enormemente la configuración de DMVPN. [GRE](#) permite enviar actualizaciones de enrutamiento por las conexiones IPSec.

## Seleccione la interfaz que se conecta a Internet

Seleccione la interfaz de router que se conecta a Internet. El túnel GRE se origina a partir de esta interfaz.

Si selecciona una interfaz que utilice una conexión de marcación podría ocurrir que la conexión esté activa en todo momento. Puede examinar las interfaces admitidas en Interfaces y conexiones para determinar si existe una conexión de acceso telefónico. Normalmente, interfaces como ISDN (RDSI) o de serie asíncrona se configuran para una conexión de acceso telefónico a redes.

## Dirección IP

Especifique una dirección IP para la interfaz mGRE. Ésta debe ser una dirección privada y encontrarse en la misma subred que las interfaces GRE de los demás routers de la red. Por ejemplo, las interfaces GRE pueden compartir la subred 10.10.6.0 y que se les asigne las direcciones IP del intervalo 10.10.6.1 a 10.10.6.254.

## Máscara de subred

Especifique la máscara de la subred en la que se encuentran las interfaces GRE. Por ejemplo, la máscara de la subred 10.10.6.0 puede ser 255.255.255.0. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

## Botón Opciones avanzadas

Cisco SDM proporciona valores por defecto para la configuración de túnel avanzada. No obstante, el administrador de hubs debe decidir la configuración de túnel y remitirla al personal encargado de administrar los routers spoke para que puedan realizar configuraciones que coincidan.

## Configuración avanzada para la interfaz de túnel

Utilice esta ventana para configurar los parámetros de túnel [GRE](#). Cisco SDM proporciona valores por defecto, aunque el usuario debe obtener los valores correctos del administrador de hubs y especificarlos en esta ventana.

En este tema de ayuda se proporcionan los valores por defecto. Si los cambia y necesita restaurarlos, consulte este tema de ayuda.

## Cadena de autenticación NHRP

Especifique la cadena que deben utilizar los [DMVPN hubs](#) y [spokes](#) para autenticarse para las transacciones NHRP, la cual puede contener un máximo de 8 caracteres. No se permiten caracteres especiales como espacios o signos de interrogación (?). Todos los dispositivos de DMVPN deben configurarse con la misma cadena de autenticación.

Cisco SDM por defecto: DMVPN\_NW

## ID de red NHRP

Especifique el ID de red NHRP. El ID de red es un identificador de red de 32 bits exclusivo de forma global correspondiente a una red de multiacceso sin difusión (NBMA). El intervalo es de 1 a 4294967295.

Cisco SDM por defecto: 100000

## Tiempo de espera NHRP

Especifique los segundos durante los que los ID de red NHRP deben anunciarse como válidos.

Cisco SDM por defecto: 360

## Clave de túnel

Especifique la clave que se utilizará para este túnel. Debe ser la misma para todos los túneles mGRE de la red.

Cisco SDM por defecto: 100000

## Ancho de banda

Especifique el ancho de banda deseado, en kilobytes por segundo (kbps). Los valores de ancho de banda por defecto se configuran durante el inicio y se pueden mostrar mediante el comando para mostrar interfaces EXEC. 1000 es un valor de ancho de banda típico en las configuraciones DMVPN.

Cisco SDM por defecto: 1000

## MTU

Especifique la cantidad máxima de datos, expresada en bytes, que podrá contener un paquete que sea transferido a través del túnel.

Cisco SDM por defecto: 1400

## Retraso de rendimiento del túnel

Establezca un valor de retraso para una interfaz, expresado en decenas de microsegundos.

Cisco SDM por defecto: 1000

## Hub principal

Si el router que desea configurar es el **hub** de reserva de la red **DMVPN**, debe proporcionar las direcciones IP pública y privada del hub principal para identificarlo.

### Dirección IP pública

Especifique la dirección IP de la interfaz del hub principal que se utiliza para este túnel. Debe ser una dirección IP estática. Obtenga esta información del administrador de hubs.

### Dirección IP de la interfaz de túnel mGRE del hub

Especifique la dirección IP de la interfaz del túnel mGRE en el hub principal. Obtenga esta información del administrador de hubs.

## Seleccionar el protocolo de enrutamiento

Utilice esta ventana para especificar el modo en que otras redes detrás del router se anunciarán a los demás routers de la red. Seleccione uno de los siguientes:

- **EIGRP**: Extended Interior Gateway Routing Protocol.
- **OSPF**: Open Shortest Path First.
- **RIP**: Routing Internet Protocol.
- Enrutamiento estático: esta opción está activada cuando se configura un túnel GRE sobre IPsec.



#### Nota

---

RIP no se admite para la topología de spoke y hub DMVPN, pero está disponible para la topología de malla completa de DMVPN.

---

## Información de enrutamiento

Utilice esta ventana para agregar o editar la información de enrutamiento acerca de las redes detrás del router que desea anunciar a los demás routers de la red. Los campos de esta ventana varían en función del protocolo de enrutamiento especificado.

Si desea obtener más información acerca de los parámetros RIP, consulte [Agregar/Editar una ruta RIP](#).

Si desea obtener más información acerca de los parámetros EIGRP, consulte [Agregar o editar una ruta EIGRP](#).

Si desea obtener más información acerca de los parámetros OSPF, consulte [Agregar o editar una ruta OSPF](#).

### Seleccione la versión de RIP que debe activarse:

Especifique la versión 1 o versión 2 de RIP.

### Seleccione un ID de proceso OSPF/número EIGRP AS existente

Puede seleccionar un ID de proceso OSPF existente para OSPF o un número de AS para EIGRP si se ha configurado uno antes. Consulte [Recomendaciones para la configuración de protocolos de enrutamiento en DMVPN](#).

### Cree un ID de proceso OSPF/número EIGRP AS nuevo

Si no existe ningún ID de proceso, o bien si desea utilizar uno distinto, puede configurar un ID de proceso en este campo.

### ID de área OSPF para la red de túnel

Especifique un nuevo ID de área OSPF para la red. Este ID de área es para la red de túnel. Cisco SDM agrega automáticamente la red de túnel a este proceso mediante dicho ID.



## Redes privadas anunciadas mediante <nombre-protocolo>

Esta área muestra las redes anunciadas mediante el protocolo de enrutamiento seleccionado. Si ya ha configurado el protocolo de enrutamiento que ha especificado en este asistente, las redes que ha indicado que se anuncien figurarán en esta lista.

Agregue todas las redes privadas que desee anunciar a los homólogos DMVPN mediante este proceso de enrutamiento. El asistente para DMVPN agrega automáticamente la red de túnel a este proceso.

**Red:** una dirección de red. Puede especificar la dirección de una determinada red y utilizar la máscara inversa para generalizar la publicación.

**Máscara comodín:** (protocolos EIGRP y OSPF) una máscara de bit que especifica qué porción de la dirección de red debe coincidir con la dirección proporcionada en la columna de red. Esta máscara puede utilizarse para hacer que el router anuncie redes de un intervalo en particular, en función de la dirección proporcionada. Un bit 0 especifica que el bit de la dirección de red debe coincidir con el bit correspondiente de la dirección de red proporcionada.

Por ejemplo, si la dirección de red fuera 172.55.10.3 y la máscara inversa, 0.0.255.255, el router anunciaría todas las redes que empezaran por los números 172.55, no sólo la red 172.55.10.3.

**Área:** aparece cuando se selecciona OSPF; es el número del área OSPF de dicha red. Cada router de una determinada área OSPF mantiene una base de datos topológica de dicha área.

**Agregar:** haga clic para agregar una red, o un grupo de redes, para anunciar.

**Editar:** haga clic para editar los datos de una red o grupo de redes anunciadas. Este botón está activado para las entradas que haya creado durante la sesión actual de este asistente.

**Eliminar:** haga clic para eliminar los datos de la red o grupo de redes seleccionadas. Este botón está activado para las entradas que haya creado durante la sesión actual de este asistente.

## Asistente para spokes de privada virtual multipunto dinámica

Este asistente le ayuda a configurar el router como un spoke de una red [DMVPN](#). Antes de empezar la configuración, debe efectuar un ping en el hub para asegurarse de que el router puede enviarle tráfico. Por otra parte, antes de empezar debe tener a mano toda la información acerca del hub que necesita. Un administrador de hubs que utilice Cisco SDM para configurar el hub puede generar un archivo de texto que contenga la información de hub que necesitan los administradores de spokes.

Antes de empezar debe obtener la información siguiente:

- La dirección IP de la interfaz física del hub.
- La dirección IP de la interfaz de túnel mGRE del hub.
- La dirección IP y la máscara de subred que el administrador de hubs le indique que debe utilizar para el spoke. Dicho administrador debe asignar direcciones a cada uno de los spokes para asegurarse de que todos los routers de la red DMVPN se encuentran en la misma subred y de que cada uno de ellos utiliza una dirección exclusiva.
- El protocolo de enrutamiento que se debe emplear y el número de AS (EIGRP) o ID de proceso (OSPF) que se utilizará para enviar actualizaciones de enrutamiento en la red DMVPN.

### Topología de red DMVPN

Seleccione el tipo de red [DMVPN](#) a la cual pertenece este router.

#### Red centro-radial (hub and spoke)

Seleccione esta opción si desea configurar el router en una red en que cada router [spoke](#) tenga una conexión GRE sobre IPsec punto a punto al [hub](#) DMVPN y va a enviar tráfico destinado a otros spokes por medio del hub. Cuando se selecciona esta opción, el gráfico muestra enlaces de los spokes al hub.

## Red de malla completa

Seleccione esta opción si desea configurar el router como un spoke capaz de establecer un túnel IPsec directo a otros spokes de la red. Para admitir esta funcionalidad, se ha configurado un túnel GRE multipunto en el spoke. Cuando se selecciona esta opción, el gráfico muestra enlaces de los spokes al hub, así como enlaces entre ellos.

La pantalla del asistente muestra las imágenes del IOS necesarias para admitir la red DMVPN de malla completa.

## Especificar la información del hub

Utilice esta ventana para proporcionar la información necesaria acerca del [hub](#) de la red [DMVPN](#).

### Dirección IP de la interfaz física del hub

Especifique la dirección IP de la interfaz en el [hub](#), que podrá obtener del administrador de hubs. Se utilizará como el destino del túnel.

### Dirección IP de la interfaz de túnel mGRE del hub

Especifique la dirección IP de la interfaz de túnel [mGRE](#) del hub. Las direcciones de túnel mGRE del hub y spokes deben encontrarse en la misma subred.

## Configuración de la interfaz de túnel GRE de spoke

Se creará una conexión de punto a punto para este spoke mediante la información especificada en esta ventana.

### Seleccione la interfaz que se conecta a Internet

Seleccione la interfaz de router que se conecta a Internet. El túnel [GRE sobre IPsec](#) se origina desde la interfaz.

Si selecciona una interfaz que utilice una conexión de marcación podría ocurrir que la conexión esté activa en todo momento. Puede consultar las interfaces admitidas en Interfaces y conexiones para averiguar si para la interfaz física seleccionada se ha configurado una conexión de acceso telefónico a redes como, por ejemplo, una conexión ISDN (RDSI) o conexión asíncrona.

**Vuelva a registrarse en el hub cuando cambie la dirección IP de *nombre-interfaz*:** esta opción está disponible cuando la interfaz seleccionada recibe una dirección IP dinámica por medio de DHCP o IPCP. Especificar esta opción permitirá al spoke volver a registrarse con el hub cuando reciba una nueva dirección IP.

## Dirección IP

Especifique la dirección IP de la interfaz GRE a este hub. Ésta debe ser una dirección privada y encontrarse en la misma subred que las interfaces GRE de los demás routers de la red. Por ejemplo, las interfaces GRE pueden compartir la subred 10.10.6.0 y que se les asigne las direcciones IP del intervalo 10.10.6.1 a 10.10.6.254.

Si desea configurar un router spoke, debe utilizar la dirección IP que el administrador de hubs ha asignado al router. De no hacerlo, pueden ocasionarse conflictos de direcciones.

## Máscara de subred

Especifique la máscara de la subred en la que se encuentran las interfaces GRE. Esta máscara debe asignarla el administrador de hubs y debe ser la misma para todos los routers de la DMVPN. Por ejemplo, la máscara de la subred 10.10.6.0 podría ser 255.255.255.0. Para más información, consulte [Direcciones IP y máscaras de subred](#).

## Botón Opciones avanzadas

Haga clic en este botón para proporcionar parámetros de túnel y [NHRP](#) para esta conexión.

Cisco SDM proporciona valores por defecto para la configuración de túnel avanzada. No obstante, el administrador de hubs debe decidir la configuración de túnel y remitirla al personal encargado de administrar los routers spoke para que puedan realizar configuraciones que coincidan. Si desea configurar un router spoke, obtenga los parámetros de túnel del administrador de hubs, haga clic en este botón y especifique dichos parámetros en el cuadro de diálogo mostrado.

## Advertencia de Cisco SDM: DMVPN Dependency (Dependencia DMVPN)

Esta ventana aparece cuando la interfaz que ha elegido para el origen del túnel DMVPN presenta una configuración que impide su uso en la DMVPN. Cisco SDM informa al usuario del conflicto y le brinda la opción de permitir que Cisco SDM modifique la configuración para que se elimine el conflicto.

### Firewall

Si se ha aplicado un firewall a la interfaz que se designó como origen del túnel, Cisco SDM puede agregar entradas de regla de acceso a la configuración de modo que el tráfico GRE, IPSec e ISAKMP esté autorizado a pasar por el firewall.

### Ver detalles

Haga clic en este botón para ver las entradas de control de acceso que Cisco SDM agregará a la regla de acceso si selecciona **Permitir el tráfico GRE, IPSec e ISAKMP a través del firewall**.

Estas entradas autorizan ambos tipos de tráfico ([ISAKMP](#) y [GRE](#)), así como los protocolos [ESP](#) (Encapsulating Security Protocol) y [AHP](#) (Authentication Header Protocol).

## Editar VPN multipunto dinámica (DMVPN)

Esta ventana muestra las configuraciones de túnel [DMVPN](#) existentes. DMVPN permite crear una red con un [hub](#) central que conecta otros routers remotos, denominados [spokes](#). Cisco SDM admite topología de red centro-radial (hub-and-spoke), en la cual el tráfico GRE sobre IPSec se enruta a través del hub. Cisco SDM le permite configurar el router como hub DMVPN principal o secundario, o bien como un router spoke en una red DMVPN.

El enlace siguiente contiene más información acerca de DMVPN (se requiere ID de conexión a CCO). [Redes privadas virtuales IPSec multipunto](#)

Cisco SDM admite la configuración de una red centro-radial (hub-and-spoke) DMVPN que utilice los perfiles de IPSec para definir el cifrado. Puede configurar una red DMVPN de malla completa y utilizar mapas criptográficos para definir el cifrado en la red DMVPN mediante el CLI. Las redes DMVPN de malla completa y redes DMVPN mediante mapas criptográficos se administran y modifican mediante el CLI.

Cisco SDM admite la configuración de una [DMVPN única](#) en un router.

El hub debe configurarse en primer lugar, a fin de establecer las direcciones IP del mismo y los parámetros de enrutamiento con los que se deben configurar los *spokes*. Para consultar otras recomendaciones acerca de la configuración de los routers en una DMVPN, consulte [Recomendaciones para la configuración de DMVPN](#).

## Interfaz

La interfaz física desde la cual se origina este túnel.

## Perfil IPsec

El perfil IPsec que utiliza el túnel. Define los conjuntos de transformación que se utilizan para cifrar el tráfico en el túnel. Cisco SDM admite el uso de perfiles IPsec únicamente para definir el cifrado en una DMVPN. Si desea utilizar mapas criptográficos, configure la DMVPN mediante el CLI.

## Dirección IP

La dirección IP del túnel GRE. Este túnel se utiliza para enviar actualizaciones de enrutamiento a la DMVPN.

## Descripción

Una descripción de este túnel.

## Panel Detalles

El panel Detalles muestra los valores de toda la configuración del túnel DMVPN.

## ¿Por qué algunas interfaces de túnel son de sólo lectura?

Una interfaz de túnel es de sólo lectura si anteriormente se ha configurado con asociaciones de mapa criptográfico y parámetros de NHRP. Desde esta ventana podrá modificar los parámetros de NHRP y la información de enrutamiento, aunque la dirección IP, y el origen y destino del túnel deberán configurarse desde la ventana Interfaces y conexiones.

## Agregar

Haga clic en esta opción para agregar una nueva configuración de túnel DMVPN.

## Editar

Haga clic en esta opción para editar una determinada configuración de túnel DMVPN.

## Eliminar

Haga clic en esta opción para eliminar una configuración de túnel DMVPN.

# Panel General

En este panel podrá agregar o editar los parámetros de configuración generales del túnel DMVPN.

## Dirección IP

Especifique la dirección IP del túnel. Ésta debe ser una dirección privada y encontrarse en la misma subred que las demás direcciones de túnel de la DMVPN. Si desea configurar un spoke, debe utilizar la dirección que el administrador de hubs ha asignado al router a fin de evitar que se produzcan conflictos de direcciones.

## Máscara

Especifique la máscara de subred que el administrador de hubs ha asignado a la DMVPN. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

## Origen del túnel

Seleccione la interfaz que el túnel utilizará, o bien especifique la dirección IP de dicha interfaz. Consulte [Uso de interfaces con conexiones de acceso telefónico](#) antes de seleccionar una interfaz configurada para una conexión de acceso telefónico a redes.

## Destino del túnel

Haga clic en **Esto es un túnel GRE multipunto** si este es un túnel DMVPN en una red de malla completa. Haga clic en **IP/Nombre de host** y especifique una dirección IP o nombre de host si esta es una red centro-radial (hub-and-spoke).

## Perfil IPSec

Seleccione un perfil IPSec configurado para este túnel. Dicho perfil define los conjuntos de transformación que se utilizan para cifrar el tráfico en este túnel.

## MTU

Especifique la cantidad máxima de datos, expresada en bytes, que podrá contener un paquete que sea transferido a través del túnel.

## Ancho de banda

Especifique el ancho de banda deseado, en kilobytes por segundo (kbps). Los valores de ancho de banda por defecto se configuran durante el inicio y se pueden mostrar mediante el comando para mostrar interfaces EXEC. El valor 1000 es un parámetro de ancho de banda típico en las configuraciones DMVPN.

## Retraso

Establezca un valor de retraso para una interfaz, expresado en decenas de microsegundos. El valor 1000 es un parámetro de retraso típico en las configuraciones DMVPN.

## Clave de túnel

Especifique la clave que se utilizará para este túnel. Debe ser la misma para todos los túneles mGRE de la red.



## This is a multipoint GRE Tunnel (Esto es un túnel GRE multipunto)

Marque esta opción si va a utilizar una interfaz de túnel **mGRE**, esto es, una interfaz capaz de mantener las conexiones a varios homólogos. Si este router se va a configurar como un hub DMVPN, debe marcar esta casilla para permitir que el hub establezca conexiones con todos los spokes. Si el router se va a configurar como un spoke, marque esta casilla si desea configurar una DMVPN de malla completa. De este modo, un spoke puede establecer una conexión con el hub para enviar tráfico y recibir información de próximo salto (next hop) para conectarse directamente a todos los demás **spokes** de la DMVPN.

## Panel NHRP

Utilice este panel para indicar los parámetros de configuración NHRP.

### Cadena de autenticación

Especifique la cadena que deben utilizar los **DMVPN hubs** y **spokes** para autenticarse para las transacciones NHRP, la cual puede contener un máximo de 8 caracteres. Todas las estaciones NHRP de la DMVPN deben configurarse con la misma cadena de autenticación.

### Tiempo en espera

Especifique los segundos durante los que los ID de red NHRP deben anunciarse como válidos.

### ID de red

Especifique el ID de red NHRP. El ID de red es un identificador de red de 32 bits exclusivo de forma global correspondiente a una red de multiacceso sin difusión (NBMA). El intervalo va de 1 a 4294967295. Dicho ID debe ser exclusivo para cada estación NHRP.

## Servidores de próximo salto (next hop)

Esta área enumera las direcciones IP de los servidores de próximo salto (next hop) con los que este router puede establecer contacto. En ella debe constar la dirección IP del hub principal y del hub secundario si se trata de un router spoke. Si se trata de un hub, esta área debe contener las direcciones IP de los demás routers hub de la DMVPN.

Haga clic en **Agregar** para especificar la dirección IP del servidor de próximo salto (next hop). Seleccione un servidor y haga clic en **Eliminar** para eliminarlo de la lista.

## Mapa NHRP

Esta área enumera las asignaciones de dirección IP a NBMA disponibles. Haga clic en **Agregar** para crear un nuevo mapa. Una vez creado, se agregará a esta lista. Haga clic en **Editar** para modificar un determinado mapa. Haga clic en **Eliminar** para quitar una determinada configuración de mapa.

## Configuración del mapa NHRP

Utilice esta ventana para crear o editar una asignación entre direcciones IP y NBMA.

## Configure estáticamente la asignación de direcciones IP a NBMA de los destinos IP conectados a una red NBMA

Haga clic en este botón si desea configurar un spoke en una red de malla completa. Cisco SDM trata los hubs de reserva como spokes conectados a hubs principales, de modo que también deberá hacer clic en este botón si desea configurar un hub de reserva. En esta parte de la ventana indicará la información de dirección que el spoke o hub de reserva necesita para establecer contacto con el hub principal.

**Destino alcanzable a través de la red NBMA:** especifique la dirección IP del túnel mGRE configurado en el hub principal. Los spokes y hubs de reserva utilizan esta información de túnel para establecer contacto con el hub y crear un túnel mGRE hacia él. Los spokes utilizan el túnel para enviar datos cifrados al hub y consultar el hub para obtener información de próximo salto (next hop) a otros spokes.

**Dirección NBMA directamente alcanzable:** especifique la dirección IP estática de la interfaz del hub principal que admite el túnel mGRE.

## Configure las direcciones NBMA utilizadas como destinos para los paquetes de difusión o multidifusión que se enviarán a través de la red

Utilice esta área de la ventana para proporcionar la información utilizada por los protocolos de enrutamiento.

**Agregar dinámicamente las direcciones IP del spoke a la caché multidifusión del hub:** defina esta opción si desea configurar un hub principal o de reserva. El hub necesita esta opción para enviar actualizaciones de enrutamiento a todos los spokes DMVPN conectados.

**Dirección IP de la dirección NBMA directamente alcanzable:** si desea configurar un spoke en una DMVPN de malla completa, o un hub de reserva, marque esta casilla e indique la dirección IP estática de la interfaz en el hub principal que admite el túnel mGRE.

## Panel Enrutamiento

Utilice este panel para configurar la información de enrutamiento para la nube de la red DMVPN.

### Protocolo de enrutamiento

Seleccione el protocolo de enrutamiento dinámico que los routers hub y spoke de esta red DMVPN utilizan para realizar el enrutamiento. Tenga en cuenta que todos los routers de la red DMVPN deben configurarse para el protocolo de enrutamiento que seleccione.

- **RIP:** Routing Internet Protocol.
- **OSPF:** Open Shortest Path First.
- **EIGRP:** Extended Interior Gateway Routing Protocol.

### Campos RIP

Si ha seleccionado RIP como protocolo de enrutamiento dinámico, seleccione **Versión 1**, **Versión 2** o **Por defecto**. Si selecciona **Versión 2**, el router incluirá la máscara de subred en la actualización de enrutamiento. Si selecciona **Por defecto**, el router enviará actualizaciones de Versión 2, pero podrá recibir actualizaciones de RIP Versión 1 ó Versión 2.

**Desactivar el horizonte dividido (split horizon):** si éste es el router hub, marque esta casilla para desactivar el horizonte dividido (split horizon) en la interfaz del túnel mGRE. La desactivación del horizonte dividido (split horizon) permite al router anunciar las rutas que ha obtenido de la interfaz de túnel de la misma interfaz.

## Campos OSPF

Si ha seleccionado OSPF, deberán rellenarse los campos siguientes:

**ID de proceso OSPF:** especifique el ID de proceso. Este valor identifica el proceso OSPF para otros routers. Consulte [Recomendaciones para la configuración de protocolos de enrutamiento en DMVPN](#).

**Tipo de red OSPF: seleccione punto-a-multipunto o difusión. La primera opción hace que OSPF agregue rutas a la tabla de enrutamiento de routers spoke. Si desea evitarlo, puede seleccionar difusión.**

**Prioridad OSPF:** la prioridad OSPF identifica este router como un hub o un spoke. Si se trata de un router hub, especifique un valor de prioridad de 2. Si se trata de un router spoke, indique un valor de prioridad de 0.

## Campos EIGRP

Si ha seleccionado EIGRP, deberán rellenarse los campos siguientes:

**Número de sistema autónomo:** especifique el número de sistema autónomo para el grupo de routers que utiliza EIGRP. Los routers que compartan el mismo número de sistema autónomo EIGRP mantienen una base de datos de routers topológica en la región identificada por dicho número. Consulte [Recomendaciones para la configuración de protocolos de enrutamiento en DMVPN](#).

**Desactivar el horizonte dividido (split horizon):** si éste es el router hub, marque esta casilla para activar el horizonte dividido (split horizon) en la interfaz de túnel mGRE. Déjela sin marcar para desactivar el horizonte dividido (split horizon). La desactivación del horizonte dividido permite al router anunciar las rutas que ha obtenido de la interfaz de túnel de la misma interfaz.

**Utilizar próximo salto original (next hop router):** si se trata de un router hub DMVPN, EIGRP anunciará este router como el próximo salto (next hop). Marque esta casilla para que EIGRP utilice el próximo salto (next hop) IP original cuando se anuncien rutas a los routers spoke DMVPN.

# ¿Cómo se configura una red DMVPN manualmente?

Puede configurar el router como spoke o hub DMVPN mediante las ventanas Componentes VPN y la ventana Editar red privada virtual multipunto dinámica DMVPN. Para ello, debe realizar las tareas siguientes:

- Configure un perfil IPsec. No puede configurar una conexión DMVPN hasta que haya configurado al menos un perfil IPsec.
- Configure la conexión DMVPN.
- Especifique las redes que desee anunciar a la nube DMVPN.

A continuación, se describen los procedimientos para realizar estas tareas:

## Para configurar un perfil IPsec:

Debe configurar una política IPsec y, a continuación, un túnel DMVPN.

- 
- Paso 1** Haga clic en **VPN** en el panel izquierdo y, a continuación, haga clic en **Componentes VPN**.
  - Paso 2** Haga clic en la rama Perfiles IPsec y, a continuación, haga clic en **Agregar** en la ventana Perfiles IPsec.
  - Paso 3** Asigne un nombre al perfil y seleccione los conjuntos de transformación que va a contener en la ventana Agregar un perfil IPsec. Si lo desea, en este campo puede especificar una breve descripción.
  - Paso 4** Haga clic en **Aceptar**.
- 

## Para configurar una conexión DMVPN:

- 
- Paso 1** En el árbol VPN, haga clic en la rama **Red privada virtual multipunto dinámica**.
  - Paso 2** Haga clic en **Editar red privada multipunto dinámica (DMVPN)**.
  - Paso 3** Haga clic en **Agregar**.
  - Paso 4** En la ventana Configuración del túnel DMVPN, utilice las fichas General, NHRP y Enrutamiento para crear un túnel DMVPN. Consulte la ayuda en línea para obtener más información acerca de un campo en particular.
-

**Para especificar las redes que desea anunciar a la nube DMVPN:**

Si existen redes detrás del router que desea anunciar a la red DMVPN, agregue los números de red de las ventanas Enrutamiento.

- 
- Paso 1** En el panel izquierdo, haga clic en **Enrutamiento**.
- Paso 2** En la ventana Enrutamiento, seleccione el protocolo de enrutamiento que ha especificado en la configuración DMVPN y haga clic en **Editar**.
- Paso 3** Agregue los números de red que desea anunciar.
-



# CAPÍTULO 14

## Configuración VPN global

---

En estos temas de la ayuda se describen las ventanas de la Configuración VPN global.

### Configuración VPN global

En esta ventana se muestra la configuración VPN global del router.

#### Botón Editar

Haga clic en el botón **Editar** para agregar o cambiar la configuración VPN global.

#### Activar IKE

Este valor es “True” (Verdadero) si IKE está activado y “False” (Falso) si IKE está desactivado.



#### Nota

---

Si IKE está desactivado, la configuración de VPN no estará operativa.

---

#### Activar modo agresivo

Este valor es “True” (Verdadero) si el Modo agresivo está activado, y es “False” (Falso) si el Modo agresivo está desactivado. La función del Modo agresivo le permite especificar el túnel RADIUS para un par IPSec e iniciar una negociación en modo agresivo con los atributos del túnel.

## Límite de tiempo de XAuth

El número de segundos que el router esperará a que el sistema responda al desafío de Xauth.

## Identidad de IKE

El nombre de host del router o dirección IP que el router utilizará para identificarse en las negociaciones IKE.

## Detección del par muerto

La Detección del par muerto (DPD) le permite a un router detectar un par y, si se detecta, eliminar las asociaciones de seguridad IPSec y IKE con el par.

### Paquete “keep-alive” de IKE (Seg)

El valor es el número de segundos que el router espera entre cada envío de paquetes “keep-alive” de IKE.

### Reintento IKE (Seg)

El valor es el número de segundos que el router espera entre los distintos intentos de establecer una conexión IKE con el par remoto. Por defecto, aparece “2” segundos.

### Tipo de DPD

Puede ser **A petición** o **Periódico**.

Si se configura como **A petición**, se envían mensajes DPD en base a patrones de tráfico. Por ejemplo, si el router tiene que enviar tráfico saliente y la activación del par es cuestionable, el router envía un mensaje DPD para preguntar el estado del par. Si el router no tiene tráfico para enviar, jamás enviará un mensaje DPD.

Si se configura como **Periódico**, el router envía un mensaje DPD en el intervalo especificado por el valor “keep-alive” IKE.



### Longevidad (seg) de la asociación de seguridad (SA) por IPSec

El tiempo tras el que las asociaciones de seguridad (SA) por IPSec vencen y se regeneran. El valor por defecto es de 3.600 segundos (1 hora).

### Duración (Kilobytes) de la asociación de seguridad (SA) por IPSec

El número de kilobytes que el router puede enviar por la conexión VPN antes de que venza la SA por IPSec. La SA se renovará una vez llegada la longevidad inferior.

## Configuración VPN global: IKE

Esta ventana permite especificar la configuración global para IKE e IPSEC.

### Activar IKE

Deje esta casilla marcada si desea utilizar VPN.



#### Precaución

---

Si IKE está desactivado, la configuración de VPN no funcionará.

---

### Activar modo agresivo

La función de modo agresivo le permite especificar atributos de túnel RADIUS para un par IPSec e iniciar una negociación en modo agresivo IKE con los atributos de túnel.

### Identidad (de este router)

Este campo especifica el modo en que se identificará el router. Seleccione **Dirección IP** o **Nombre de host**.

### Límite de tiempo de XAuth

El número de segundos que el router debe esperar una respuesta del sistema que requiera autenticación XAuth.

## Activar Detección del par muerto (DPD)

La Detección del par muerto (DPD) le permite a un router detectar un par y, si se detecta, eliminar las asociaciones de seguridad IPsec y IKE con el par.

La casilla de verificación de Activar Detección del par muerto está desactivada cuando la imagen de Cisco IOS que el router está utilizando no admite DPD.

### Paquete “keepalive”

Especifique el número de segundos que el router debe mantener una conexión que no se está utilizando.

### Volver a intentar

Especifique el número de segundos que el router debe esperar entre los distintos intentos de establecer una conexión IKE con un par. El valor por defecto es de 2 segundos.

### Tipo de DPD

Seleccione **A petición** o **Periódico**.

Si se configura como **A petición**, se envían mensajes DPD en base a patrones de tráfico. Por ejemplo, si el router tiene que enviar tráfico saliente y la activación del par es cuestionable, el router envía un mensaje DPD para preguntar el estado del par. Si el router no tiene tráfico para enviar, jamás enviará un mensaje DPD.

Si se configura como **Periódico**, el router envía un mensaje DPD en el intervalo especificado por el valor “keep-alive” IKE.

## Configuración VPN global: IPsec

Puede editar la configuración IPsec global en esta ventana.

### Autenticar y generar una clave nueva cada

Marque esta casilla y especifique el intervalo de tiempo después del que el router debe autenticar y generar una nueva clave. Si no especifica ningún valor, el router autenticará y generará una clave nueva cada hora.

## Generar una clave nueva después de que la clave actual realice el cifrado de un volumen de

Marque esta casilla y especifique el número de kilobytes que debe cifrar la clave vigente antes de que el router autentique y genere una clave nueva. Si no especifica ningún valor, el router autenticará y generará una nueva clave una vez la clave vigente haya cifrado 4.608.000 kilobytes.

## Configuración del cifrado de la clave VPN

La ventana Configuración del cifrado de la clave VPN aparece si la imagen de IOS de Cisco de su router admite un cifrado del Tipo 6, también denominado *cifrado de clave VPN*. Esta ventana se puede utilizar para especificar una clave maestra para usar en el cifrado de claves VPN, como son claves previamente compartidas, claves Easy VPN y claves XAuth. Una vez cifradas, nadie que esté visualizando el archivo de configuración del router podrá leer estas claves.

### Activar el cifrado de claves VPN

Marque esta opción para activar el cifrado de estas claves.

### Clave maestra vigente

En este campo aparecen asteriscos (\*) cuando se ha configurado una clave maestra.

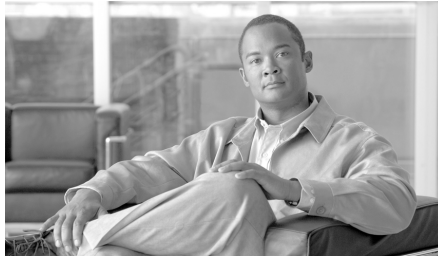
### Nueva clave maestra

Especifique una nueva clave maestra en este campo. Las claves maestras deben tener una longitud mínima de 8 caracteres y máxima de 128 caracteres.

### Confirmar clave maestra

Vuelva a escribir la clave maestra en este campo a modo de confirmación. Si los valores de este campo y del campo Nueva clave maestra no coinciden, Cisco SDM le solicitará que especifique de nuevo la clave.





# CAPÍTULO 15

## Seguridad IP

---

Seguridad IP (IPSec) es una infraestructura basada en estándares abiertos que brinda confidencialidad, integridad y autenticación de datos entre pares participantes. IPSec suministra estos servicios de seguridad en la capa IP; utiliza IKE para gestionar la negociación de protocolos y algoritmos basándose en la política local y para generar las claves de cifrado y de autenticación que utilizará.

Cisco SDM permite configurar conjuntos de transformación, reglas y políticas IPSec.

Utilice el árbol de IPSec para ir a las ventanas de configuración de IPSec que desee utilizar.

## Políticas IPSec

Esta ventana muestra las políticas IPSec configuradas en el router y los mapas criptográficos asociados a cada política. Las políticas IPSec se utilizan para definir conexiones VPN. Para informarse acerca de las relaciones entre las políticas IPSec, los mapas criptográficos y las conexiones VPN, consulte [Información adicional acerca de conexiones VPN y políticas IPSec](#).

### Icono



Si este icono aparece al lado de la política IPSec, esto indica que se trata de una política de sólo lectura que no puede editarse. Una política IPSec puede ser de sólo lectura si contiene comandos que Cisco SDM no admite.

**Nombre**

Nombre de esta política IPsec.

**Tipo**

Uno de los siguientes:

- **ISAKMP**: se utilizará **IKE** para establecer las asociaciones de seguridad IPsec de protección del tráfico especificadas por esta entrada del mapa criptográfico. Cisco SDM admite los mapas criptográficos de Protocolo de la asociación de seguridad en Internet y gestión de claves (ISAKMP).
- **Manual**: no se utilizará **IKE** para establecer las asociaciones de seguridad IPsec de protección del tráfico especificadas en esta entrada del mapa criptográfico. Cisco SDM no admite la creación de mapas criptográficos manuales. Cisco SDM trata como de sólo lectura a cualquier mapa criptográfico manual creado mediante la interfaz de línea de comandos (CLI).
- **Dinámico**: especifica que esta entrada del mapa criptográfico sirve para hacer referencia a un mapa criptográfico dinámico previamente existente. Los mapas criptográficos dinámicos son plantillas de políticas utilizadas para procesar las solicitudes de negociación de un dispositivo IPsec homólogo. Cisco SDM no admite la creación de mapas criptográficos dinámicos. Cisco SDM trata como de sólo lectura cualquier mapa criptográfico dinámico creado mediante la CLI.

**Mapas criptográficos en esta política IPsec****Nombre**

Nombre de la política IPsec de la que forma parte el mapa criptográfico.

**Núm. secuencia**

Cuando se utiliza una política IPsec en una conexión VPN, la combinación del número de secuencia y del nombre de la política IPsec identifica de forma exclusiva la conexión.

**Homólogos**

Esta columna muestra una lista de las direcciones IP o nombres de host de los dispositivos homólogos especificados en el mapa criptográfico. En caso de haber varios homólogos, éstos se separarán mediante comas.

**Conjunto de transformación**

Esta columna muestra una lista de los conjuntos de transformación utilizados en el mapa criptográfico.

**Mapas criptográficos dinámicos en esta política IPSec**

**Nombre del conjunto de mapas criptográficos dinámicos**

Nombre de este conjunto de mapas criptográficos dinámicos. Los nombres permiten a los administradores comprender cómo se utiliza el conjunto de mapas criptográficos.

**Número de secuencia**

Número de secuencia de este conjunto de mapas criptográficos dinámicos.

**Tipo**

El tipo siempre es Dinámico.

**¿Qué desea hacer?**

<b>Si desea:</b>	<b>Haga lo siguiente:</b>
Agregar una política IPSec a la configuración.	Haga clic en <b>Agregar</b> .
Editar una política IPSec existente.	Seleccione la política y haga clic en <b>Editar</b> .
Quitar una entrada de mapa criptográfico de una política.	Seleccione la política y haga clic en <b>Editar</b> . En la ventana, seleccione el mapa criptográfico que desee quitar y haga clic en <b>Eliminar</b> . A continuación, haga clic en <b>Aceptar</b> para regresar a esta ventana.
Quitar una política IPSec.	Seleccione la política y haga clic en <b>Eliminar</b> .

## Agregar una política IPsec/Editar la política IPsec

Utilice esta ventana para agregar o editar una política IPsec.

### Nombre

Nombre de esta política IPsec. Puede ser cualquier conjunto de caracteres alfanuméricos. Resulta útil incluir los nombres de los homólogos en el nombre de la política o bien incluir otra información representativa para el usuario.

### Mapas criptográficos en esta política IPsec

En este cuadro se muestra una lista de los mapas criptográficos de esta política IPsec. La lista incluye el nombre, el número de secuencia y el conjunto de transformación que forman este mapa criptográfico. En la política IPsec se puede seleccionar un mapa criptográfico y editarlo o eliminarlo.

Si desea agregar un mapa criptográfico, haga clic en **Agregar**. Si desea que Cisco SDM le guíe por todo el proceso, marque **Utilizar el asistente para agregar** y haga clic en **Agregar**.

### Icono




Si un mapa criptográfico es sólo de lectura, el icono de sólo lectura aparecerá en esta columna. Un mapa criptográfico puede ser de sólo lectura si contiene comandos que Cisco SDM no admite.

### Mapas criptográficos dinámicos en esta política IPsec

En este cuadro se muestra una lista de los conjuntos de mapas criptográficos dinámicos de esta política IPsec. Utilice el botón **Agregar** para agregar un conjunto de mapas criptográficos dinámicos a la política. Utilice el botón **Eliminar** para quitar de la política un conjunto de mapas criptográficos dinámicos seleccionado.



## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Agregar un mapa criptográfico a esta política.	Haga clic en <b>Agregar</b> y cree un mapa criptográfico en los paneles Agregar mapa criptográfico. O bien marque <b>Utilizar el asistente para agregar</b> y haga clic en <b>Agregar</b> .   <b>Nota</b> El asistente sólo le permitirá agregar un conjunto de transformación al mapa criptográfico. Si necesita varios conjuntos de transformación en el mapa criptográfico, no utilice el asistente.
Editar un mapa criptográfico en esta política.	Seleccione el mapa criptográfico, haga clic en <b>Editar</b> y edite el mapa criptográfico en los paneles Editar el mapa criptográfico.
Quitar un mapa criptográfico de esta política.	Seleccione el mapa criptográfico y haga clic en <b>Eliminar</b> .

## Agregar o editar el mapa criptográfico: General

En esta ventana puede cambiar los parámetros generales del mapa criptográfico. La ventana contiene los campos siguientes.

### Nombre de la política IPSec

Campo de sólo lectura que contiene el nombre de la política en la que se utiliza este mapa criptográfico. Este campo no aparece si está utilizando el Asistente para mapas criptográficos.

### Descripción

En este campo puede especificar o editar una descripción del mapa criptográfico. Esta descripción aparece en la lista de conexiones VPN y puede ser útil para distinguir este mapa criptográfico de los otros que se encuentran dentro de la misma política IPSec.

## Número de secuencia

Número que, junto con el nombre de la política IPsec, se utiliza para identificar una conexión. Cisco SDM genera automáticamente un número de secuencia. Si así se desea, se puede especificar un número de secuencia propio.

## Duración de la asociación de seguridad

Las asociaciones de seguridad de IPsec utilizan claves compartidas. Dichas claves, así como sus respectivas asociaciones de seguridad, tienen el mismo límite de tiempo. Existen dos duraciones: una duración determinada por un período de tiempo definido y otra determinada por el volumen de tráfico. La asociación de seguridad caduca cuando se alcanza la primera duración.

Puede utilizar este campo para especificar una longevidad de asociación de seguridad para este mapa criptográfico que no sea la longevidad especificada globalmente. En el campo Kilobytes, puede especificar la longevidad en número de kilobytes enviados, hasta un máximo de 4608000. En los campos HH:MM:SS, puede especificar la longevidad en horas, minutos y segundos. También puede especificar longevidades determinadas por un período de tiempo definido y determinadas por el volumen de tráfico. Si se especifican ambos, la longevidad caducará al cumplirse el primer criterio.

## Activar la confidencialidad directa perfecta

Cuando se derivan claves de seguridad de otras claves generadas anteriormente, se produce un problema de seguridad, ya que si se descubre una clave, las otras también se pueden descubrir. La confidencialidad directa perfecta (PFS) garantiza la derivación independiente de cada clave. De esta manera, es posible asegurar que si se descubre una clave, no se podrán descubrir las restantes. Si activa PFS, puede especificar que se utilice el método Diffie-Hellman group1, group2 o group5.



### Nota

---

Si el router no admite el grupo 5, no aparecerá en la lista.

---

## Activar inyección de ruta inversa

La inyección de ruta inversa (RRI) se usa para poblar la tabla de enrutamiento de un router interno que ejecute el protocolo OSPF (Open Shortest Path First) o RIP (Routing Information Protocol) para clientes VPN remotos o sesiones de LAN a LAN.

La inyección de ruta inversa agrega dinámicamente rutas estáticas a los clientes conectados al servidor Easy VPN.

## Agregar o editar el mapa criptográfico: Información del par

Un mapa criptográfico incluye los nombres de host o direcciones IP de los pares implicados en la asociación de seguridad. Esta pantalla permite agregar y quitar homólogos asociados a este mapa criptográfico. Varios pares proporcionan al router varias rutas para los datos cifrados.

Si desea:	Haga lo siguiente:
Agregar un par a la Lista actual.	Especifique la dirección IP o el nombre de host del par y haga clic en <b>Agregar</b> .
Quitar un par de la Lista actual.	Seleccione el homólogo y haga clic en <b>Quitar</b> .

## Agregar o editar el mapa criptográfico: Conjuntos de transformación

Utilice esta ventana para agregar y editar el conjunto de transformación utilizado en el mapa criptográfico. Un mapa criptográfico incluye los nombres de host o direcciones IP de los pares implicados en la asociación de seguridad. Varios pares proporcionan al router varias rutas para los datos cifrados. No obstante, los dispositivos situados a ambos extremos de la conexión VPN deben utilizar el mismo conjunto de transformación.

Utilice el Asistente para mapas criptográficos si es suficiente para el router ofrecer un mapa criptográfico con un conjunto de transformación.

Utilice **Agregar nuevo mapa criptográfico...** con la casilla de verificación **Utilizar el asistente para agregar** desactivada si desea configurar manualmente un mapa criptográfico con varios conjuntos de transformación (hasta seis) para asegurarse de que el router pueda ofrecer un conjunto de transformación que el par con el que está negociando pueda aceptar. Si ya se encuentra en el Asistente para mapas criptográficos, salga del asistente, desactive **Utilizar el asistente para agregar** y haga clic en **Agregar nuevo mapa criptográfico...**

También puede ordenar los conjuntos de transformación si configura manualmente un mapa criptográfico con varios conjuntos de transformación. Éste será el orden en que el router los utilizará para negociar el conjunto de transformación que se utilizará.

## Conjuntos de transformación disponibles

Conjuntos de transformación configurados disponibles para su utilización en mapas criptográficos. En el Asistente para mapas criptográficos, los conjuntos de transformación disponibles están incluidos en la lista desplegable **Seleccionar conjunto de transformación**.

Si no se ha configurado ningún conjunto de transformación en el router, esta lista sólo contendrá los conjuntos de transformación proporcionados por Cisco SDM.



### Nota

- No todos los routers admiten todos los conjuntos de transformación (tipos de cifrado). Los conjuntos de transformación no admitidos no aparecerán en la ventana.
- No todas las imágenes de IOS admiten todos los conjuntos de transformación que Cisco SDM admite. Los conjuntos de transformación que la imagen del IOS no admita no aparecerán en la ventana.
- Si el cifrado de hardware está activado, sólo aparecerán en la ventana los conjuntos de transformación admitidos tanto por el cifrado de hardware como por la imagen del IOS.

## Detalles del conjunto de transformación seleccionado (Asistente para mapas criptográficos únicamente)

Muestra el nombre, cifrado, características de autenticación y otros parámetros del mapa criptográfico seleccionado.



Si este icono aparece al lado del conjunto de transformación, dicho conjunto es de sólo lectura y no puede editarse.

## Conjuntos de transformación seleccionados en el orden de preferencia (Configuración manual del mapa criptográfico únicamente)

Los conjuntos de transformación seleccionados para este mapa criptográfico, en el orden en que se utilizarán. Durante las negociaciones con un par, el router ofrecerá los conjuntos de transformación en el orden indicado en la lista. Puede utilizar los botones de flecha hacia arriba y hacia abajo para cambiar el orden de la lista.

### ¿Qué desea hacer? (Asistente para mapas criptográficos únicamente)

Si desea:	Haga lo siguiente:
Utilizar el conjunto de transformación seleccionado para el mapa criptográfico.	Haga clic en <b>Siguiente</b> .
Utilizar otro conjunto de transformación existente.	Selecciónelo en la lista Seleccionar conjunto de transformación y haga clic en <b>Siguiente</b> .
Utilizar un conjunto de transformación nuevo.	Haga clic en <b>Agregar</b> y cree el conjunto de transformación en la ventana Agregar conjunto de transformación. A continuación, regrese a esta ventana y haga clic en <b>Siguiente</b> .
Editar el conjunto de transformación seleccionado.	Haga clic en <b>Editar</b> y edite el conjunto de transformación en la ventana Editar conjunto de transformación.
Agregar más conjuntos de transformación a este mapa criptográfico. Probablemente desee agregar más conjuntos de transformación para asegurarse de que el router pueda ofrecer un conjunto de transformación que el homólogo acepte utilizar.	Salga del Asistente para mapas criptográficos, desmarque <b>Utilizar el asistente para agregar</b> y haga clic en <b>Agregar mapa criptográfico</b> . La ficha Conjunto de transformación le permitirá agregar y ordenar conjuntos de transformación.

### ¿Qué desea hacer? (Configuración manual del mapa criptográfico únicamente)

Si desea:	Haga lo siguiente:
Agregar un conjunto de transformación al cuadro Conjuntos de transformación seleccionados.	Seleccione un conjunto de transformación en el cuadro Conjuntos de transformación disponibles y haga clic en el botón de flecha hacia la derecha.
Quitar un conjunto de transformación del cuadro Conjuntos de transformación seleccionados.	Seleccione el conjunto de transformación que desee quitar y haga clic en el botón de flecha hacia la izquierda.
Cambiar el orden de preferencia de los conjuntos de transformación seleccionados.	Seleccione un conjunto de transformación y haga clic en los botones de flecha hacia arriba o hacia abajo.

Si desea:	Haga lo siguiente:
Agregar un conjunto de transformación a la lista Conjuntos de transformación disponibles.	Haga clic en <b>Agregar</b> y configure el conjunto de transformación en la ventana Agregar conjunto de transformación.
Editar un conjunto de transformación en la lista Conjuntos de transformación disponibles.	Haga clic en <b>Editar</b> y configure el conjunto de transformación en la ventana Editar conjunto de transformación.

## Agregar o editar el mapa criptográfico: Tráfico de protección

Puede configurar el mapa criptográfico para proteger todo el tráfico (Asistente para mapas criptográficos únicamente) o seleccionar una regla IPSec para proteger el tráfico especificado.

### Proteger todo el tráfico entre las subredes siguientes (Asistente para mapas criptográficos únicamente)

Utilice esta opción para especificar una única subred de origen (una subred en la LAN) cuyo tráfico desee cifrar y una subred de destino admitida por el par especificado en la ventana Pares. No se cifrará el tráfico que fluya entre otras subredes de origen y de destino.

#### Origen

Especifique la dirección de subred cuyo tráfico saliente desee proteger e indique la máscara de subred. Puede seleccionar una máscara de subred en la lista o bien escribir una máscara personalizada. El número de subred y la máscara deben especificarse en formato de decimales con puntos. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

Se cifrará todo el tráfico que provenga de esta subred de origen y tenga una dirección IP de destino en la subred de destino.

#### Destino

Especifique la dirección de la subred de destino e indique la máscara de dicha subred. Puede seleccionar una máscara de subred en la lista o bien escribir una máscara personalizada. El número de subred y la máscara deben especificarse en formato de decimales con puntos.

Se cifrará todo el tráfico que se dirija a los hosts en esta subred.

## Regla IPSec (Crear o seleccionar una lista de acceso para el tráfico IPSec)

Puede agregar o cambiar la regla IPSec utilizada en este mapa criptográfico. Utilice esta opción si necesita especificar varios orígenes y destinos o tipos específicos de tráfico para cifrar. Una regla IPSec puede estar formada por varias entradas, cada una de ellas especificando diferentes tipos de tráfico y diferentes orígenes y destinos. Todos los paquetes que no coincidan con los criterios especificados en la regla IPSec se enviarán sin cifrar.



### Nota

---

Si va a agregar una regla IPSec para una conexión VPN que utiliza una interfaz de túnel, es preciso que la regla especifique los mismos origen y destino que la configuración del túnel.

---

Para agregar o cambiar la regla IPSec del mapa criptográfico, haga clic en el botón ... a la derecha del campo Regla IPSec y seleccione una de las siguientes opciones:

- **Seleccionar una regla existente (ACL):** si la regla que desea utilizar ya se ha creado, selecciónela y, a continuación, haga clic en **Aceptar**.
- **Cree una nueva regla (ACL) y seleccione:** si la regla que necesita no se ha creado, cree la regla y, a continuación, haga clic en **Aceptar**.
- **Ninguna:** si desea borrar una asociación de reglas. El campo Regla IPSec muestra el nombre de la regla IPSec que se utiliza, pero si selecciona **Ninguna**, el campo se queda en blanco.

Otra forma de agregar o cambiar la regla IPSec para este mapa criptográfico es introducir el número de la regla IPSec directamente en el campo Regla IPSec.



### Nota

---

Las reglas IPSec deberán ser reglas ampliadas y no reglas estándar. Si el número o el nombre especificado identifica una regla estándar, Cisco SDM mostrará un mensaje de alerta cuando haga clic en Aceptar.

---

# Conjuntos de mapas criptográficos dinámicos

En esta ventana se muestra una lista de los conjuntos de mapas criptográficos dinámicos configurados en el router.

## Botones Agregar/Editar/Eliminar

Utilice estos botones para gestionar los mapas criptográficos de la ventana. Si intenta eliminar un conjunto de mapas criptográficos asociados a una política IPsec, Cisco SDM se lo impedirá. Antes de eliminarlo, tendrá que disociar el mapa criptográfico de la política. Esta operación puede efectuarse en la ventana Políticas IPsec.

### Nombre

Nombre del mapa criptográfico dinámico.

### Tipo

Siempre Dinámico.

## Agregar un conjunto de mapas criptográficos dinámicos/Editar el conjunto de mapas criptográficos dinámicos

En esta ventana puede agregar o editar un conjunto de mapas criptográficos dinámicos.

### Nombre

Si va a agregar un mapa criptográfico dinámico, especifique el nombre en este campo. Por el contrario, si va a editarlo, este campo se desactivará y no podrá cambiar el nombre.

## Mapas criptográficos en esta política IPsec

En esta área se muestra una lista de los mapas criptográficos utilizados en este conjunto. Utilice los botones **Agregar**, **Editar** o **Eliminar** para agregar, quitar o modificar mapas criptográficos de la lista.



## Asociar mapas criptográficos a esta política IPsec

### Número de secuencia

Especifique un número de secuencia que permita identificar este conjunto de mapas criptográficos. El número de secuencia indicado es único y no lo puede utilizar otro conjunto de mapas criptográficos.

### Seleccione el conjunto de mapas criptográficos dinámicos

En esta lista, seleccione un conjunto de mapas criptográficos dinámicos que desee agregar.

### Mapas criptográficos en este conjunto de mapas criptográficos dinámicos

Esta área muestra una lista de nombres, números de secuencia y homólogos del conjunto de mapas criptográficos dinámicos seleccionado.

## Perfiles IPsec

Esta ventana muestra una lista de los perfiles IPsec configurados en el router. Los perfiles IPsec están formados por uno o varios conjuntos de transformación configurados y se aplican a túneles mGRE para definir cómo se cifra el tráfico en túnel.

### Nombre

Nombre del perfil IPsec.

### Conjunto de transformación

Conjunto de transformación utilizado en este perfil.

### Descripción

Descripción del perfil IPsec.

## Agregar

Haga clic para agregar un perfil IPsec nuevo.

## Editar

Seleccione un perfil existente y haga clic en **Editar** para cambiar la configuración del perfil.

## Eliminar

Haga clic en este botón para editar un perfil IPsec seleccionado. Si el perfil que va a eliminar se está utilizando actualmente en un túnel DMVPN, deberá configurar el túnel DMVPN para que utilice otro perfil IPsec.

## Detalles del perfil IPsec.

Esta área muestra la configuración del perfil IPsec seleccionado. Para obtener una descripción de la información que se muestra en esta área, consulte [Agregar o editar un perfil IPsec](#).

## Agregar o editar un perfil IPsec

Especifique la información para crear un perfil IPsec en este diálogo. Un perfil IPsec especifica cuáles conjuntos de transformación se usarán, cómo se determinará el tiempo de vida de la asociación de seguridad (SA) e información adicional.

## Columnas de conjunto de transformación

Use las dos columnas que se encuentran en la parte superior del diálogo para especificar los conjuntos de transformación que desea incluir en el perfil. La columna izquierda contiene los conjuntos de transformación configurados en el router. Para agregar al perfil un conjunto de transformación configurado, selecciónelo y haga clic en el botón >>. Si no hay conjuntos de transformación en la columna izquierda, o si necesita un conjunto de transformación que no se ha creado, haga clic en **Agregar** y cree el conjunto de transformación en el diálogo que aparece.

## Asociación del perfil IKE

Si desea asociar un perfil [IKE](#) con esta política IPsec, seleccione un perfil existente de la lista. Si ya se ha asociado un perfil IKE, este campo es de sólo lectura.

## Tiempo de vida de SA de IPsec basado en tiempo

Haga clic en **Tiempo de vida de SA de IPsec basado en tiempo** si desea que se establezca una nueva SA después de transcurrido un período de tiempo establecido. Especifique el período de tiempo en los campos HH:MM:SS que se encuentran a la derecha.

## Tiempo de vida de SA de IPsec basado en volumen de tráfico

Haga clic en **Tiempo de vida de SA de IPsec basado en volumen de tráfico** si desea que se establezca una nueva SA después de que una cantidad de tráfico especificada haya pasado a través del túnel IPsec. Especifique el número de kilobytes que debe pasar por el túnel antes de quitar una SA existente y establecer una nueva.

## Tiempo de inactividad de SA de IPsec

Haga clic en **Tiempo de inactividad de SA de IPsec** si desea que se establezca una nueva SA después de que el par haya estado inactivo durante un tiempo específico. Especifique el período de tiempo de inactividad en los campos HH:MM:SS que se encuentran a la derecha.

## Confidencialidad directa perfecta

Haga clic en **Confidencialidad directa perfecta** si IPsec debe requerir confidencialidad directa perfecta ([PFS](#)) al solicitar nuevas asociaciones de seguridad para esta interfaz de plantilla virtual, o si debe requerir PFS en solicitudes recibidas desde el par. Puede especificar los valores siguientes:

- grupo 1: el grupo de módulos principales Diffie-Hellman de 768 bits se usa para cifrar la solicitud PFS.
- grupo 2: el grupo de módulos principales Diffie-Hellman de 1024 bits se usa para cifrar la solicitud PFS.
- grupo 5: el grupo de módulos principales Diffie-Hellman de 1536 bits se usa para cifrar la solicitud PFS.

## Agregar un perfil IPsec/Editar el perfil IPsec y Agregar mapa criptográfico dinámico

Utilice esta ventana para agregar o editar un perfil IPsec o para agregar un mapa criptográfico dinámico.

### Nombre

Especifique un nombre para este perfil.

### Conjuntos de transformación disponibles

Esta columna muestra una lista de los conjuntos de transformación configurados en este router. Para agregar un conjunto de transformación de esta lista a la columna Conjuntos de transformación seleccionados, seleccione un conjunto de transformación y haga clic en el botón de flecha hacia la derecha (>>).

Si necesita configurar un conjunto de transformación nuevo, haga clic en el nodo **Grupos de transformación** del árbol de IPsec para ir a la ventana Grupos de transformación. En esta ventana, haga clic en **Agregar** para crear un conjunto de transformación nuevo.

### Conjuntos de transformación seleccionados

Esta columna muestra una lista de los conjuntos de transformación utilizados en este perfil. Puede seleccionar varios conjuntos de transformación para que el router que está configurando y el router del otro extremo del túnel puedan negociar acerca del conjunto que van a utilizar.

# Conjunto de transformación

Esta pantalla permite ver y transformar conjuntos de transformación, así como agregar conjuntos de transformación nuevos y editar o quitar los ya existentes. Un conjunto de transformación es una combinación particular de algoritmos y protocolos de seguridad. Durante la negociación de la asociación de seguridad IPSec, los homólogos acuerdan utilizar un conjunto de transformación determinado para proteger un flujo de datos concreto.

Se pueden crear varios conjuntos de transformación y, a continuación, especificar uno o varios de ellos en una entrada de mapa criptográfico. El conjunto de transformación definido en la entrada del mapa criptográfico se utilizará en la negociación de asociación de seguridad IPSec para proteger los flujos de datos especificados por la lista de acceso de la entrada de ese mapa criptográfico.

Durante las negociaciones de la asociación de seguridad IPSec con IKE, los homólogos buscan un conjunto de transformación que sea el mismo en ambos homólogos. Una vez encontrado el conjunto de transformación, éste se selecciona y se aplica en el tráfico protegido como parte de las asociaciones de seguridad IPSec de ambos homólogos.

## Nombre

Nombre del conjunto de transformación.

## Cifrado ESP

Cisco SDM reconoce los siguientes tipos de cifrado [ESP](#):

- **ESP\_DES**: ESP (Encapsulating Security Payload), DES (Data Encryption Standard). DES admite un cifrado de 56 bits.
- **ESP\_3DES**: ESP, Triple DES. Forma de cifrado más potente que DES que admite un cifrado de 168 bits.
- **ESP\_AES\_128**: ESP, AES (Advanced Encryption Standard). Cifrado con una clave de 128 bits. AES aporta mayor seguridad que DES y, desde un punto de vista computacional, es más eficiente que 3DES.
- **ESP\_AES\_192**: ESP, cifrado AES con una clave de 192 bits.
- **ESP\_AES\_256**: ESP, cifrado AES con una clave de 256 bits.

- **ESP\_NULL**: algoritmo de cifrado nulo, pero se utiliza una transformación de cifrado.
- **ESP\_SEAL**: ESP con el algoritmo de cifrado SEAL (Software Encryption Algorithm) de clave de cifrado de 160 bits. SEAL (Software Encryption Algorithm) es un algoritmo alternativo a DES (Data Encryption Standard), 3DES (Triple DES) y AES (Advanced Encryption Standard) basados en software. El cifrado SEAL utiliza una clave de cifrado de 160 bits y ejerce menor impacto sobre la CPU, si se compara con otros algoritmos basados en software.

## Integridad ESP

Indica el algoritmo de integridad que se utiliza. Esta columna contendrá un valor si se configura el conjunto de transformación para que suministre tanto integridad de datos como cifrado de los mismos. La columna puede contener uno de los valores siguientes:

- **ESP-MD5-HMAC**: Message Digest 5, Hash-based Message Authentication Code (HMAC).
- **ESP-SHA-HMAC**: algoritmo de hash seguro, HMAC.

## Integridad AH

Indica el algoritmo de integridad que se utiliza. Esta columna contendrá un valor si se configura el conjunto de transformación para que suministre integridad de datos, pero no cifrado. La columna puede contener uno de los valores siguientes:

- **AH-MD5-HMAC**: Message Digest 5.
- **AH-SHA-HMAC**: algoritmo de hash seguro.

## Compresión IP

Indica si se utiliza la compresión de datos IP.



### Nota

---

Si el router no admite la compresión IP, se desactivará este cuadro.

---

## Modo



Esta columna puede contener uno de los valores siguientes:

- Túnel: se cifran tanto los encabezados como los datos. Se trata del modo utilizado en las configuraciones VPN.
- Transporte: sólo se cifran los datos. Este modo se utiliza cuando los puntos finales del cifrado y los de la comunicación son los mismos.

## Tipo

Puede ser Definido por el usuario o bien Cisco SDM por defecto.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Agregar un conjunto de transformación nuevo a la configuración del router.	Haga clic en Agregar y cree el conjunto de transformación en la ventana Agregar conjunto de transformación.
Editar un conjunto de transformación existente.	<p>Seleccione el conjunto de transformación y haga clic en <b>Editar</b>. A continuación, edite el conjunto de transformación en la ventana Editar conjunto de transformación.</p> <p></p> <p><b>Nota</b> Los conjuntos de transformación de Cisco SDM por defecto son de sólo lectura y no se pueden editar.</p>
Eliminar un conjunto de transformación existente.	<p>Seleccione el conjunto de transformación y haga clic en <b>Eliminar</b>.</p> <p></p> <p><b>Nota</b> Los conjuntos de transformación de Cisco SDM por defecto son de sólo lectura y no se pueden eliminar.</p>

## Agregar/Editar conjunto de transformación

Utilice esta ventana para agregar o editar un conjunto de transformación.

Para obtener una descripción de las combinaciones de transformación permitidas y de las descripciones de las transformaciones, haga clic en [Combinaciones de transformación permitidas](#).



### Nota

- No todos los routers admiten todos los conjuntos de transformación (tipos de cifrado). Los conjuntos de transformación no admitidos no aparecerán en la pantalla.
- No todas las imágenes de IOS admiten todos los conjuntos de transformación que Cisco SDM admite. Los conjuntos de transformación que la imagen de IOS no admita no aparecerán en la pantalla.
- Si el cifrado de hardware está activado, sólo aparecerán en la pantalla los conjuntos de transformación admitidos tanto por el cifrado de hardware como por la imagen de IOS.
- Los servidores Easy VPN sólo admiten el modo de túnel. Los servidores Easy VPN no admiten el modo de transporte.
- Los servidores Easy VPN sólo admiten conjuntos de transformación con cifrado ESP. Los servidores Easy VPN no admiten el algoritmo AH.
- Los servidores Easy VPN no admiten el cifrado ESP-SEAL.

### Nombre de este conjunto de transformación

Puede ser cualquier nombre que desee. No es preciso que el nombre coincida con el nombre del conjunto de transformación que utiliza el homólogo, aunque puede ser útil dar a los conjuntos de transformación correspondientes el mismo nombre.



## Integridad de datos y cifrado (ESP)

Active este cuadro si desea proporcionar integridad de datos y cifrado ESP (Encapsulating Security Payload).

### Algoritmo de integridad

Seleccione uno de los siguientes:

- ESP\_MD5\_HMAC. Message Digest 5.
- ESP\_SHA\_HMAC. Algoritmo de hash seguro.

### Cifrado

Cisco SDM reconoce los siguientes tipos de cifrado [ESP](#):

- ESP\_DES. ESP (Encapsulating Security Payload), DES (Data Encryption Standard). DES admite un cifrado de 56 bits.
- ESP\_3DES. ESP, Triple DES. Forma de cifrado más potente que DES que admite un cifrado de 168 bits.
- ESP\_AES\_128. ESP, AES (Advanced Encryption Standard). Cifrado con una clave de 128 bits. AES aporta mayor seguridad que DES y, desde un punto de vista computacional, es más eficiente que 3DES.
- ESP\_AES\_192. ESP, cifrado AES con clave de 192 bits.
- ESP\_AES\_256. ESP, cifrado AES con clave de 256 bits.
- [ESP\\_SEAL](#): ESP con el algoritmo de cifrado SEAL (Software Encryption Algorithm) de clave de cifrado de 160 bits. SEAL (Software Encryption Algorithm) es un algoritmo alternativo a DES (Data Encryption Standard), 3DES (Triple DES) y AES (Advanced Encryption Standard) basados en software. El cifrado SEAL utiliza una clave de cifrado de 160 bits y ejerce menor impacto sobre la CPU, si se compara con otros algoritmos basados en software.
- ESP\_NULL. Algoritmo de cifrado nulo, pero se utiliza una transformación de cifrado.



#### Nota

---

Los tipos de cifrado ESP disponibles dependen del router. Según el tipo de router que se configure, es posible que uno o varios tipos de cifrado no estén disponibles.

---

## Integridad de datos y dirección sin cifrado (AH)

Esta casilla de verificación y los campos situados debajo de ella aparecen si hace clic en **Mostrar opciones avanzadas**.

Active este cuadro si desea que el router proporcione integridad de datos y dirección AH (encabezado de autenticación). El encabezado de autenticación no se cifrará.

### Algoritmo de integridad

Seleccione uno de los siguientes:

- AH\_MD5\_HMAC: Message Digest 5.
- AH\_SHA\_HMAC: algoritmo de hash seguro.

## Modo

Seleccione las partes del tráfico que desea cifrar:

- Transporte (cifrar datos solamente): el modo de transporte se utiliza cuando los dos puntos finales admiten IPSec. Este modo pone AH o ESP después del encabezado IP original; por consiguiente, sólo se cifrará la carga útil de IP. Este método permite a los usuarios aplicar servicios de red como controles de calidad de servicio (QoS) a paquetes cifrados. El modo de transporte sólo debe utilizarse cuando el destino de los datos es siempre el homólogo VPN remoto.
- Túnel (cifrar datos y encabezado IP): el modo de túnel proporciona una mayor protección que el modo de transporte. Dado que todo el paquete IP se encapsula en AH o ESP, se adjunta un encabezado IP nuevo y se puede cifrar el datagrama completo. El modo de túnel permite a los dispositivos de red, como un router por ejemplo, actuar como proxy IPSec para varios usuarios de VPN. En estas configuraciones debe utilizarse el modo de túnel.

## Compresión IP (COMP-LZS)

Active este cuadro si desea utilizar la compresión de datos.



### Nota

---

No todos los routers admiten la compresión IP. Si el router no admite la compresión IP, se desactivará este cuadro.

---

# Reglas IPSec

Esta ventana muestra las reglas IPSec configuradas para este router. Las reglas IPSec definen el tráfico IPSec que se cifrará. La parte superior de la ventana muestra una lista de las reglas de acceso definidas. La parte inferior muestra las entradas de la regla de acceso seleccionada en la lista de reglas.

Las reglas IPSec contienen información del tipo de servicio y de la dirección IP. Los paquetes que cumplen los criterios especificados en la regla se cifran. Los paquetes que no cumplen los criterios especificados se envían sin cifrar.

## Nombre/Número

Nombre o número de esta regla.

## Usado por

Mapas criptográficos en los que se utiliza esta regla.

## Tipo

Las reglas IPSec deben especificar el origen y el destino y deben poder especificar el tipo de tráfico que el paquete contiene. Por consiguiente, las reglas IPSec son reglas ampliadas.

## Descripción

Descripción textual de la regla, si está disponible.

## Acción

Puede ser **Permitir** o **Denegar**. **Permitir** significa que los paquetes que cumplen los criterios de estas reglas se protegen mediante cifrado. **Denegar** significa que los paquetes que cumplen los criterios se envían sin cifrar. Para obtener más información, consulte [Significados de las palabras clave “permit” y “deny”](#).

## Origen

Dirección IP o palabra clave que especifica el origen del tráfico. **Cualquiera** especifica que el origen puede ser cualquier dirección IP. La dirección IP de esta columna puede aparecer sola o seguida por una **máscara comodín**. En caso de haber una **máscara inversa**, ésta indica las porciones de la dirección IP que la dirección IP de origen debe respetar. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

## Destino

Dirección IP o palabra clave que especifica el destino del tráfico. **Cualquiera** especifica que el destino puede ser cualquier dirección IP. La dirección IP de esta columna puede aparecer sola o seguida por una **máscara comodín**. En caso de haber una **máscara inversa**, ésta indica las porciones de la dirección IP que la dirección IP de destino debe respetar.

## Servicio

Tipo de tráfico que el paquete debe contener.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Buscar en las entradas de la regla de acceso una regla determinada.	Seleccione la regla en la lista de reglas. Las entradas de la regla aparecerán en el cuadro inferior.
Agregar una regla IPSec.	Haga clic en <b>Agregar</b> y cree la regla en la ventana de regla que aparece.
Eliminar una regla IPSec.	Seleccione la regla en la lista de reglas y haga clic en <b>Eliminar</b> .
Eliminar una entrada de regla determinada.	Seleccione la regla en la lista de reglas y haga clic en <b>Editar</b> . Luego, elimine la entrada en la ventana de regla que aparece.
Aplicar una regla IPSec a una interfaz.	Aplique la regla en la ventana de configuración de la interfaz.



# CAPÍTULO 16

## Intercambio de claves por Internet

---

Los temas de ayuda en esta sección describen las pantallas de configuración del Intercambio de claves por Internet (IKE).

### Intercambio de claves por Internet (IKE)

El Intercambio de claves por Internet (IKE) es un método estándar para organizar comunicaciones seguras y autenticadas. IKE establece claves de sesión (y una configuración asociada criptográfica y de trabajo en red) entre dos hosts de la red.

Cisco SDM permite crear políticas IKE para proteger las identidades de pares durante la autenticación, Cisco SDM también permite crear claves previamente compartidas que los pares intercambiarán.

#### ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Obtener más información acerca de IKE.	Haga clic en <a href="#">Información adicional acerca de IKE</a> .
Activar IKE. Para utilizar las negociaciones IKE, es preciso activar IKE para conexiones VPN.	Haga clic en <b>Configuración global</b> y, a continuación, en <b>Editar</b> para activar IKE y efectuar configuraciones globales de IKE.

Si desea:	Haga lo siguiente:
<p>Crear una política IKE.</p> <p>Cisco SDM proporciona una política IKE por defecto, aunque no hay garantía de que la del par sea la misma. Es aconsejable configurar más políticas IKE a fin de que el router pueda ofrecer una política IKE que el par pueda aceptar.</p>	<p>Haga clic en el nodo <b>Política IKE</b> del árbol de VPN. Consulte el apartado <a href="#">Políticas IKE</a> para obtener más información.</p>
<p>Crear una clave previamente compartida.</p> <p>Si se utiliza IKE, los pares de los extremos deberán intercambiar una clave previamente compartida para autenticarse entre sí.</p>	<p>Haga clic en el nodo <b>Clave previamente compartida</b> del árbol de VPN. Consulte el apartado <a href="#">Claves previamente compartidas de IKE</a> para obtener más información.</p>
<p>Crear un perfil IKE.</p>	<p>Haga clic en el nodo <b>Perfil IKE</b> del árbol VPN. Consulte el apartado <a href="#">Perfiles IKE</a> para obtener más información.</p>

## Políticas IKE

Es preciso proteger las negociaciones IKE; por consiguiente, cada negociación IKE empieza con la configuración de una política IKE común (compartida) en ambos pares. Esta política indica qué parámetros de seguridad se utilizarán para proteger las negociaciones IKE posteriores. Esta ventana muestra las políticas IKE configuradas en el router y además permite agregar, editar y quitar políticas IKE de la configuración del router. Si no hay ninguna política IKE configurada en el router, esta ventana mostrará la política IKE por defecto.

Una vez que los dos pares hayan acordado el uso de una política común, una asociación de seguridad establecida en cada par identificará los parámetros de seguridad de la mencionada política. Estas asociaciones de seguridad se aplicarán durante la negociación a todo el tráfico IKE posterior.

Las políticas IKE de esta lista están disponibles para todas las conexiones VPN.

### Prioridad

Número entero que indica la prioridad de la política en relación con otras políticas IKE configuradas. Asigne los números más bajos a las políticas IKE que prefiera que utilice el router. Durante las negociaciones, el router ofrecerá primero dichas políticas.

## Cifrado

Tipo de cifrado que debe utilizarse para comunicarse con esta política IKE.

## Hash

Algoritmo de autenticación para negociación. Se puede elegir entre dos valores:

- Algoritmo de hash seguro (SHA)
- Message Digest 5 (MD5)

## Autenticación

Método de autenticación que se utilizará.

- Pre-SHARE. La autenticación se ejecutará mediante claves previamente compartidas.
- RSA\_SIG. La autenticación se ejecutará mediante firmas digitales.

## Tipo

Puede ser SDM\_DEFAULT o bien definido por el usuario. Las políticas SDM\_DEFAULT no se pueden editar.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Obtener más información acerca de las políticas IKE.	Consulte <a href="#">Información adicional acerca de las políticas IKE</a> .
Agregar una política IKE a la configuración del router.  Cisco SDM proporciona una política IKE por defecto, aunque no hay garantía de que la del par sea la misma. Es aconsejable configurar más políticas IKE a fin de que el router pueda ofrecer una política IKE que el par pueda aceptar.	Haga clic en <b>Agregar</b> y configure una política IKE nueva en la ventana Agregar una política IKE.

Si desea:	Haga lo siguiente:
Editar una política IKE existente.	<p>Seleccione la política IKE que desea modificar y haga clic en <b>Editar</b>. A continuación, edite la política IKE en la ventana Política IKE.</p> <p>Las políticas IKE por defecto son de sólo lectura. No se pueden editar.</p>
Quitar una política IKE de la configuración del router.	<p>Seleccione la política IKE que desee quitar y haga clic en <b>Quitar</b>.</p>

## Agregar o editar una política IKE

En esta ventana puede agregar o editar o una política IKE.



### Nota

- No todos los routers admiten todos los tipos de cifrado. Los tipos que no se admitan no aparecerán en la pantalla.
- No todas las imágenes de IOS admiten todos los tipos de cifrado que Cisco SDM admite. Los tipos que la imagen de IOS no admita no aparecerán en la pantalla.
- Si el cifrado de hardware está activado, sólo aparecerán en la pantalla los tipos de cifrado admitidos tanto por el cifrado de hardware como por la imagen de IOS.

## Prioridad

Número entero que indica la prioridad de la política en relación con otras políticas IKE configuradas. Asigne los números más bajos a las políticas IKE que prefiera que utilice el router. Durante las negociaciones, el router ofrecerá primero dichas políticas.



## Cifrado

Tipo de cifrado que debe utilizarse para comunicarse con esta política IKE. Cisco SDM admite varios tipos de cifrado, ordenados según su seguridad en una lista. Cuanto más seguro sea un tipo de cifrado, más tiempo de proceso necesitará.

**Nota**

---

Si el router no admite un tipo de cifrado, éste no aparecerá en la lista.

---

Cisco SDM admite los tipos de cifrado siguientes:

- DES (Data Encryption Standard): admite un cifrado de 56 bits.
- 3DES (Triple Data Encryption Standard): forma de cifrado más potente que DES; admite un cifrado de 168 bits.
- AES-128: cifrado AES con una clave de 128 bits. Aporta mayor seguridad que DES y, desde un punto de vista computacional, es más eficiente que 3DES.
- AES-192: cifrado AES con una clave de 192 bits.
- AES-256: cifrado AES con una clave de 256 bits.

## Hash

Algoritmo de autenticación que se utilizará para negociar. Existen dos opciones:

- Algoritmo de hash seguro (SHA)
- Message Digest 5 (MD5)

## Autenticación

Método de autenticación que se utilizará.

- Pre-SHARE. La autenticación se ejecutará mediante claves previamente compartidas.
- RSA\_SIG. La autenticación se ejecutará mediante firmas digitales.

## grupo D-H

Grupo Diffie-Hellman (D-H). Diffie-Hellman es un protocolo de criptografía de clave pública que permite a dos routers establecer un secreto compartido en un canal de comunicaciones que no es seguro. Las opciones son:

- group1: grupo D-H de 768 bits. Group D-H 1.
- group2: grupo D-H de 1.024 bits. Group D-H 2. Este grupo brinda más seguridad que el grupo 1, aunque necesita más tiempo de procesamiento.
- group5: grupo D-H de 1536 bits. Group D-H 5. Este grupo brinda más seguridad que el grupo 2, aunque necesita más tiempo de procesamiento.



### Nota

- Si el router no admite el grupo 5, no aparecerá en la lista.
- Los servidores Easy VPN no admiten el Grupo D-H 1.

## Duración

Duración de la asociación de seguridad, indicada en horas, minutos y segundos. El valor por defecto es un día o 24:00:00.

## Claves previamente compartidas de IKE

Esta ventana permite ver, agregar, editar y quitar claves previamente compartidas de IKE en la configuración del router. Durante la negociación IKE, se intercambia una clave previamente compartida con un par remoto. Ambos pares deben configurarse con la misma clave.

## Icono



Si una clave compartida previamente es de sólo lectura, aparecerá el icono correspondiente en esta columna. Una clave compartida previamente se marcará como de sólo lectura si se configura con la opción de CLI **no-Xauth** (sin Xauth)

## Nombre/IP del par

Nombre o dirección IP de un par con el que se comparte esta clave. Si se suministra una dirección IP, puede especificar todos los pares de una red o subred, o simplemente un host individual. Si, por el contrario, se especifica un nombre, la clave sólo se compartirá con el par indicado.

## Máscara de red

La **máscara de red** especifica qué porción de la dirección IP del par se utiliza para la dirección de red y qué parte se emplea para la dirección del host. Así, la máscara de red 255.255.255.255 indica que la dirección IP del par es una dirección de un host específico. Una máscara de red que contiene ceros en los bytes menos significativos indica que la dirección IP del par es una dirección de subred o de red. Así, por ejemplo, una máscara de red 255.255.248.0 indica que los primeros 22 bits de la dirección se utilizan para la dirección de red, mientras que los últimos 10 bits sirven para indicar la parte del host de la red.

## Clave previamente compartida

La clave previamente compartida no se puede leer en las ventanas de Cisco SDM. Si necesita examinar la clave previamente compartida, vaya a **Vista -> Configuración en ejecución**. Esto mostrará la configuración en ejecución. La clave está contenida en el comando **crypto isakmp key**.

Si desea:	Haga lo siguiente:
Agregar una clave previamente compartida a la configuración del router.	Haga clic en <b>Agregar</b> y agregue la clave previamente compartida en la ventana Agregar una nueva clave previamente compartida.
Editar una clave previamente compartida ya existente.	Seleccione la clave previamente compartida y haga clic en <b>Editar</b> . A continuación, edite la clave en la ventana Editar la clave previamente compartida.
Quitar una clave previamente compartida ya existente.	Seleccione la clave previamente compartida y haga clic en <b>Quitar</b> .

## Agregar una nueva clave previamente compartida/Editar la clave previamente compartida

Utilice esta ventana para agregar o editar una clave previamente compartida.

### Clave

Cadena alfanumérica que se intercambiará con el par remoto. Es preciso que la misma clave esté configurada en el par remoto. La clave proporcionada tiene que ser difícil de adivinar. Los signos de interrogación (?) y los espacios no pueden utilizarse en la clave previamente compartida.

### Vuelva a especificar la clave

A modo de confirmación, vuelva a introducir la cadena que ha especificado en el campo Clave.

### Par

Seleccione **Nombre de host** si desea que la clave se aplique a un host específico. Seleccione **Dirección IP** si desea especificar una red o subred o bien si desea introducir la dirección IP de un host específico debido a que no hay ningún servidor DNS para convertir los nombres de host en direcciones IP

### Nombre de host

Este campo aparece si ha seleccionado “**Nombre de host**” en el campo Par. Especifique el nombre de host del par. La red debe contar con un servidor DNS que pueda convertir el nombre de host en una dirección IP.

### Dirección IP/máscara de subred

Estos campos aparecen si ha seleccionado “Dirección IP” en el campo Par. Especifique la dirección IP de una red o subred en el campo Dirección IP. La clave previamente compartida se aplicará a todos los pares de la red o subred. Si desea obtener más información, consulte [Direcciones IP y máscaras de subred](#).

Especifique una máscara de subred si la dirección IP que ha indicado es una dirección de subred y no la dirección de un host específico.

## Autenticación de usuario [Xauth]

Marque esta casilla si los pares VPN de sitio a sitio utilizan Xauth para autenticarse a sí mismos. Si la autenticación de Xauth está activada en Configuración VPN global, estará activado tanto para pares de sitio a sitio como para conexiones Easy VPN.

## Perfiles IKE

Los perfiles **IKE**, también denominados perfiles **ISAKMP**, permiten definir un conjunto de parámetros IKE que puede asociar con uno o más túneles IPsec. Un perfil IKE aplica parámetros a una conexión IPsec entrante identificada exclusivamente a través de su concepto de comparar los criterios de identidad. Estos criterios se basan en la identidad IKE que se presenta mediante conexiones IKE entrantes e incluye una dirección IP, nombre de dominio completamente calificado (FQDN), y grupo (la agrupación de clientes remotos de la red privada virtual [VPN]).

Para obtener más información acerca de los perfiles ISAKMP y sobre cómo se configuran mediante el CLI de Cisco IOS, vaya a [Cisco.com](http://Cisco.com) y siga esta ruta:

**Productos y Servicios > Software Cisco IOS > Seguridad Cisco IOS > IPsec Cisco IOS > Documentación del Producto > Informes Técnicos > Aspectos generales ISAKMP Perfil ISAKMP**

## Perfiles IKE

El área de la pantalla Perfiles IKE incluye una lista de los perfiles IKE configurados e incluye el nombre del perfil, el perfil IPsec utilizado y una descripción del perfil si se ha proporcionado uno. Si ningún perfil IPsec utiliza el perfil IKE seleccionado, aparece el valor <ninguno> en la columna Usado por.

Cuando utiliza SDM para crear una configuración de servidor Easy VPN, los perfiles IKE se crean automáticamente, denominados por SDM, y se muestran en la lista.

## Detalles del perfil IKE

El área de detalles de la pantalla incluye una lista de los valores de configuración para el perfil seleccionado. Se puede utilizar para ver detalles sin hacer clic en el botón Editar ni mostrar un diálogo adicional. Si necesita realizar cambios, haga clic en Editar e introduzca los cambios que requiera en el diálogo que aparece. Haga clic en [Agregar o editar un perfil IKE](#) para conocer detalles sobre la información que se muestra en esta área.

## Agregar o editar un perfil IKE

Especifique la información y realice la configuración en este diálogo para crear un perfil IKE y asociarlo con una interfaz de túnel virtual.

### Nombre del perfil IKE

Especifique un nombre para este perfil IKE. Si se está editando un perfil, se activa este campo.

### Interfaz de túnel virtual

Seleccione la interfaz de túnel virtual a la cual desea asociar este perfil IKE en la lista de interfaces de túnel virtual. Si necesita crear una interfaz de túnel virtual, haga clic en **Agregar** y cree la interfaz en el diálogo que aparece.

### Tipo de identidad de coincidencia

El perfil IKE incluye criterios de coincidencia que permiten al router identificar las conexiones entrantes y salientes a las cuales se aplicarán los parámetros de conexión IKE. Los criterios de coincidencia se pueden aplicar actualmente a los grupos VPN. El grupo se selecciona automáticamente en el campo Tipo de identidad de coincidencia.

Haga clic en **Agregar** para crear una lista de los grupos que desea incluir en los criterios de coincidencia.

Seleccione **Agregar nombre de grupo externo** para agregar el nombre a un grupo que no está configurado en el router y, a continuación, especifique el nombre en el diálogo que aparece.

Elija **Seleccionar entre los grupos locales** para agregar el nombre de un grupo que está configurado en el router. En el diálogo que aparece, seleccione la casilla al lado del grupo que desea agregar. Si todos los grupos locales se usan en otros perfiles IKE, SDM le informa que todos los grupos han sido seleccionados.

## Configuración de modo

Seleccione **Responder** en el campo Configuración de modos si el router responderá a solicitudes de configuración de modos.

Seleccione **Iniciar** si el router iniciará solicitudes de configuración de modos.

Seleccione **Ambos** si el router iniciará y responderá a solicitudes de configuración de modos.

## Política de autorización de búsqueda de políticas de grupo

Debe especificar una política de autorización que controle el acceso a información de políticas de grupo en el servidor **AAA**. Seleccione **por defecto** si desea otorgar acceso a información de búsqueda de políticas de grupo. Para especificar una política, seleccione una política existente en la lista o haga clic en **Agregar** para crear una política en el diálogo que aparece.

## Política de autenticación de usuario

Puede especificar una política de autenticación de usuario que se utilizará para conexiones a **Xauth**. Seleccione **por defecto** si desea permitir conexiones XAuth. Para especificar una política para controlar conexiones XAuth, seleccione una política existente en la lista o haga clic en **Agregar** para crear una política en el diálogo que aparece.

## Descubrimiento de par inactivo

Haga clic en **Descubrimiento de par inactivo** para que el router pueda enviar mensajes de descubrimiento de par inactivo (**DPD**) a los pares. Si un par no responde a los mensajes DPD, se rechaza la conexión.

Especifique el número de segundos entre los mensajes PDP en el campo Intervalo “keepalive”. El intervalo oscila entre 1 y 3600 segundos.

En el campo Reintentos, especifique el número de segundos entre reintentos si fallan los mensajes PDP. El intervalo oscila entre 2 y 60 segundos.

El descubrimiento de par inactivo ayuda a administrar conexiones sin la intervención del administrador, pero genera paquetes que ambos pares deben procesar para mantener la conexión.

## Descripción

Puede agregar una descripción del perfil IKE que está agregando o editando.







# CAPÍTULO 17

## Infraestructura de clave pública

---

Las ventanas de PKI (Infraestructura de clave pública) permiten generar solicitudes de suscripción y claves RSA, así como gestionar claves y certificados. Puede utilizar el proceso SCEP (Simple Certificate Enrollment Process) para crear una solicitud de suscripción y un par de claves RSA y recibir certificados en línea, o crear una solicitud de suscripción que puede enviar a un servidor de CA (Autoridad certificadora) sin conexión.

Si desea utilizar SDP (Secure Device Provisioning) para suscribirse a los certificados, consulte [Secure Device Provisioning](#).

## Asistentes para certificados

Esta ventana permite seleccionar el tipo de suscripción que desea realizar. También indica las tareas de configuración que deben llevarse a cabo antes de comenzar la suscripción o las tareas que Cisco recomienda efectuar antes de la suscripción. Todo ello contribuye a la eliminación de posibles problemas.

Seleccione el método de suscripción que Cisco SDM utiliza para generar la solicitud de suscripción.

### Tareas previas

Si Cisco SDM identifica tareas de configuración que deben establecerse antes de comenzar el proceso de suscripción, le notificará de las mismas en este casillero. Se proporciona un enlace junto al texto de alerta para que pueda desplazarse hasta el área correspondiente de Cisco SDM y establecer la configuración. Si Cisco SDM no detecta la falta de configuraciones, esta casilla no aparece. Las posibles tareas previas se describen en [Tareas previas para configuraciones de PKI](#).

## SCEP

Haga clic en este botón si puede establecer una conexión directa entre el router y el servidor de una CA. Para ello, debe conocer la dirección URL de suscripción del servidor. El asistente realizará lo siguiente:

- Recopilar información del usuario para configurar un punto de confianza y transmitirlo al router.
- Iniciar una suscripción con el servidor de la CA especificado en el punto de confianza.
- Si el servidor de la CA está disponible, mostrar la “huella dactilar” del servidor de la CA para su aceptación.
- Si acepta la “huella dactilar” del servidor de la CA, finalice la suscripción.

## Cortar y pegar/Import from PC (Importar de PC)

Haga clic en este botón si el router no puede establecer una conexión directa con el servidor de la CA o si desea generar una solicitud de suscripción y enviarla a la CA en otro momento. Tras su generación, la solicitud de suscripción puede enviarse a una CA en otro momento. La suscripción mediante el proceso de cortar y pegar requiere la invocación del asistente para certificados digitales con el fin de generar una solicitud y, a continuación, su reinvocación después de haber obtenido los certificados para el servidor de la CA y el router.



### Nota

---

Cisco SDM sólo admite la suscripción mediante el proceso de cortar y pegar del tipo PKCS#10 codificado base 64. Cisco SDM no admite la importación de suscripciones de certificados del tipo PEM y PKCS#12.

---

## Botón Iniciar la tarea seleccionada

Haga clic en este botón para iniciar el asistente para el tipo de suscripción que ha seleccionado. Si Cisco SDM ha detectado una tarea requerida que debe realizarse antes de comenzar la suscripción, este botón estará desactivado. Cuando se haya completado la tarea, se activará el botón.

## Bienvenido al Asistente para SCEP

Esta pantalla indica que está utilizando el asistente para SCEP (Simple Certificate Enrollment Process). Si no desea emplear SCEP, haga clic en **Cancelar** para abandonar el asistente.

Cuando se haya finalizado el asistente y enviado los comandos al router, Cisco SDM intentará ponerse en contacto con el servidor de la CA. Si la conexión se establece, Cisco SDM mostrará una ventana de mensajes con el certificado digital del servidor.

## Información acerca de la Autoridad certificadora (CA)

En esta ventana, proporcione información que permita identificar el servidor de la CA. Además, especifique una contraseña de desafío que se enviará junto con la solicitud.



### Nota

---

La información que se especifique en esta pantalla se utiliza para generar un punto de confianza, el cual se crea mediante un método de comprobación de revocación por defecto de CRL. Si está utilizando el Asistente para SCEP con el fin de editar un punto de confianza existente y ya existe un método de revocación distinto de CRL (por ejemplo, OCSP) en este punto de confianza, Cisco SDM no lo modificará. Si necesita cambiar el método de revocación, diríjase a la ventana Certificados de router, seleccione el punto de confianza que ha configurado y haga clic en el botón **Comprobar revocación**.

---

### Apodo del servidor de la CA

El apodo del servidor de la CA es un identificador para el punto de confianza que se dispone a configurar. Especifique un nombre que le permita distinguir un punto de confianza de otro.

### URL de suscripción

Si está completando una suscripción SCEP, debe especificar en este campo la dirección URL de suscripción para el servidor de la CA. Por ejemplo,

`http://AutoridadC/suscripcion`

La dirección URL debe comenzar con los caracteres http://. Antes de comenzar el proceso de suscripción, asegúrese de que haya conectividad entre el router y el servidor de la CA.

Este campo no aparece si está llevando a cabo una suscripción mediante el proceso de cortar y pegar.

### **Contraseña de desafío y confirmar contraseña de desafío**

Una contraseña de desafío puede enviarse a la CA para que se pueda utilizar en el caso de tener que revocar el certificado. Es recomendable crear dicha contraseña, ya que algunos servidores de CA no emiten certificados si la contraseña de desafío se deja en blanco. Si desea utilizar dicha contraseña, especifíquela y, a continuación vuelva a introducirla en el campo de confirmación. La contraseña de desafío se enviará junto con la solicitud de suscripción. Por motivos de seguridad, esta contraseña se cifra en el archivo de configuración del router. Por lo tanto, deberá anotarla y guardarla en una ubicación que recordará.

Esta contraseña también se conoce como una contraseña de desafío.

### **Botón Opciones avanzadas**

Las opciones avanzadas permiten proporcionar información adicional para que el router pueda ponerse en contacto con el servidor de la CA.

### **Opciones avanzadas**

Utilice esta ventana para proporcionar información adicional con el fin de que el router pueda ponerse en contacto con el servidor de la CA.

### **Defina el origen de la solicitud de certificado en una interfaz específica**

Marque esta casilla si desea especificar una interfaz específica como origen del certificado.

### **Proxy HTTP y puerto HTTP**

Si la solicitud de suscripción se envía a través del servidor proxy, especifique en estos campos la dirección IP del mismo y el número de puerto que deberá utilizarse para las solicitudes proxy.

## Atributos del nombre de asunto del certificado

Especifique la información opcional que desee incluir en el certificado. Una vez incluida en el certificado, podrá verla todo usuario al que el router envíe el certificado.

### Incluir el FQDN del router en el certificado

Se recomienda que en el certificado se incluya el nombre de dominio completamente calificado del router. Marque esta casilla si desea que Cisco SDM lo incluya en la solicitud de certificado.

**Nota**

Si la imagen de Cisco IOS que se ejecuta en el router no admite esta función, esta casilla estará desmarcada.

**FQDN**

Si ha activado este campo, especifique en el mismo el FQDN del router. Un ejemplo de un FQDN es

```
sjrtr.miempresa.net
```

### Incluir la dirección IP del router

Marque esta opción cuando desee incluir en la solicitud de certificado una dirección IP válida configurada en el router. Si la marca, podrá especificar manualmente una dirección IP o bien seleccionar la interfaz cuya dirección IP desee utilizar.

**Dirección IP**

Haga clic si desea especificar una dirección IP y, en el campo que aparece, indique una dirección IP configurada en el router. Especifique una dirección IP que se haya configurado en el router o una dirección asignada al mismo.

**Interfaz**

Seleccione una interfaz de router cuya dirección IP desee incluir en la solicitud de certificado.

## Incluir el número de serie del router

Marque esta casilla cuando desee incluir el número de serie del router en el certificado.

## Otros atributos de asunto

La información que especifique en esta ventana se incluirá en la solicitud de suscripción. Las CA utilizan la norma X.500 para almacenar y mantener la información de los certificados digitales. Todos los campos son opcionales, pero es recomendable especificar la mayor cantidad de información posible.

### Common Name [Nombre común (cn)]

Especifique el nombre común que debe incluirse en este certificado. Éste sería el nombre utilizado para buscar el certificado en el directorio X.500.

### Organizational Unit (ou) [Unidad organizativa (ou)]

Especifique una unidad organizativa o nombre de departamento para su uso con este certificado. Por ejemplo: Desarrollo o Ingeniería podrían ser unidades organizativas

### Organización (o)

Especifique el nombre de la organización o empresa. Se trata del nombre de organización X.500.

### Estado (st)

Especifique la provincia o el estado en el que se encuentra el router o la organización.

### País (c)

Especifique el país en el que se encuentra el router o la organización.

## Correo electrónico (e)

Especifique la dirección de correo electrónico que debe incluirse en el certificado del router.

**Nota**

Si la imagen de Cisco IOS que se ejecuta en el router no admite este atributo, el campo estará desactivado.

# Claves RSA

Debe incluir una clave pública RSA en la solicitud de suscripción. Una vez concedido el certificado, la clave pública se incluirá en el mismo para que los homólogos la puedan utilizar con el fin de cifrar los datos que se envían al router. La clave privada se conserva en el router y se utiliza para descifrar los datos que envían los homólogos y para firmar digitalmente las transacciones durante las negociaciones con los mismos.

## Generar par de claves nuevas

Haga clic en este botón cuando desee generar una clave nueva para su uso en el certificado. Al generar un par de claves, debe especificar el módulo para determinar el tamaño de la clave. Esta nueva clave aparecerá en la ventana Claves RSA al finalizarse el asistente.

### Módulo

Especifique el valor del módulo de la clave. Si desea un valor de módulo de 512 a 1.024, especifique un valor entero que sea múltiple de 64. Si desea un valor mayor que 1.024, puede especificar 1.536 ó 2.048. Si especifica un valor mayor que 512, es posible que la generación de la clave tarde un minuto o más.

El módulo determina el tamaño de la clave. Cuanto mayor sea el módulo, más segura será la clave. Sin embargo, las claves con módulos grandes tardan más tiempo en generarse. Del mismo modo, las operaciones de cifrado y descifrado se prolongan si contienen claves grandes.

**Generate separate key pairs for encryption and signature (Generar pares de claves independientes para el cifrado y la firma)**

Por defecto, Cisco SDM crea un par de claves de objetivo general que se utiliza para el cifrado y la firma. Si desea que Cisco SDM genere pares de claves independientes para el cifrado y la firma de documentos, marque esta casilla. Cisco SDM generará claves de uso para el cifrado y la firma.

**Use existing RSA key pair (Utilizar par de claves RSA existente)**

Haga clic en este botón si desea utilizar un par de claves existente y seleccione la clave en la lista desplegable.

**Guardar en el Token USB**

Marque la casilla de verificación **Guardar claves y certificados en un token USB seguro** si desea guardar las claves y certificados RSA en un token conectado a su router. Esta opción solamente aparece si hay un token USB conectado a su router.

Seleccione el token USB del menú desplegable **Token USB**. Especifique el PIN requerido para iniciar sesión en el token USB deseado en **PIN**.

Después de elegir un token USB e introducir el PIN correspondiente, haga clic en **Inicio de sesión** para acceder al token USB.

## Resumen

En esta ventana se proporciona un resumen de la información que ha especificado. Estos datos se utilizan para configurar un punto de confianza en el router y comenzar el proceso de suscripción. Si activó **Obtener una vista previa de los comandos antes de enviarlos al router** en el cuadro de diálogo Preferencias, podrá obtener una vista previa del CLI que se envía al router.

**Si se dispone a realizar una suscripción SCEP**

Cuando los comandos se hayan enviado al router, Cisco SDM intentará ponerse en contacto con el servidor de la CA. Si la conexión se establece, Cisco SDM mostrará una ventana de mensajes con el certificado digital del servidor.



## Si se dispone a realizar una suscripción mediante el proceso de cortar y pegar

Después de que los comandos se hayan enviado al router, Cisco SDM genera una solicitud de suscripción y la muestra en otra ventana. Debe guardar dicha solicitud de suscripción y presentarla al administrador del servidor de la CA para obtener el certificado del servidor de la CA y el certificado para el router. La solicitud de suscripción tiene el formato PKCS#10 codificado Base 64.

Cuando haya obtenido los certificados del servidor de la CA, debe reiniciar el Cut and Paste Wizard (Asistente para cortar y pegar) y seleccionar **Reanudar suscripción sin terminar** para importar los certificados al router.

## Certificado de servidor de la CA

Cisco SDM muestra la “huella dactilar” digital del certificado del servidor de la CA. Si desea continuar con el proceso de suscripción, deberá aceptar este certificado. Si no acepta el certificado, la suscripción no avanzará

### La “huella dactilar” digital del certificado del servidor de la CA es:

Cisco SDM muestra el valor hexadecimal del certificado del servidor de la CA en mayúsculas. Por ejemplo:

```
E55725EC A389E81E 28C4BE48 12B905ACD
```

### Para aceptar el certificado del servidor de la CA y continuar con el proceso de suscripción

Haga clic en **Sí, acepto este certificado** y, a continuación, en **Siguiente**.

### Para rechazar el certificado del servidor de la CA y detener el proceso de suscripción

Haga clic en **No, no acepto este certificado** y haga clic en **Siguiente**.

## Estado de suscripción

Esta ventana indica el estado del proceso de suscripción. Si se han producido errores durante el proceso, Cisco SDM muestra la información correspondiente.

Una vez que haya revisado la información del estado, haga clic en **Finalizar**.

# Bienvenido al Asistente para cortar y pegar

El Asistente para cortar y pegar permite generar una solicitud de suscripción y guardarla en el PC para poder enviarla sin conexión a la Autoridad certificadora (CA). Puesto que la suscripción no se puede completar en una sola sesión, este asistente finaliza al generar y guardar en el PC el punto de confianza y la solicitud de suscripción.

Una vez que haya enviado manualmente la solicitud de suscripción al servidor de la CA y recibido el certificado para el router, debe volver a iniciar el Asistente para cortar y pegar con el fin de finalizar la suscripción e importar los certificados al router.

## Tarea de suscripción

Indique si está comenzando una suscripción nueva o si está reanudando una suscripción con una solicitud de suscripción que ha guardado en el PC.

### Comenzar suscripción nueva

Haga clic en **Comenzar suscripción nueva** para generar un punto de confianza, un par de claves RSA y una solicitud de suscripción que podrá guardar en el PC y enviar al servidor de la CA. El asistente finalizará después de que haya guardado la solicitud de suscripción. Para finalizar la suscripción tras haber recibido el certificado del servidor de la CA y el certificado para el router, vuelva a iniciar el Asistente para cortar y pegar y seleccione la opción **Reanudar suscripción sin terminar**.

### Reanudar una suscripción sin terminar

Haga clic en este botón para reanudar un proceso de suscripción. Puede importar los certificados que ha recibido del servidor de la CA y generar una nueva solicitud de suscripción para un punto de confianza, según sus necesidades.

# Solicitud de suscripción

En esta ventana se muestra la solicitud de suscripción de tipo PKCS#10 codificado Base 64 que el router ha generado. Guarde la solicitud de suscripción en el PC y, a continuación, envíela a la CA para obtener el certificado.

## Guardar:

Vaya hasta el directorio del PC en el que desea guardar el archivo de texto de la solicitud de suscripción, especifique un nombre para el archivo y haga clic en **Guardar**.

# Continuar con la suscripción sin terminar

Si se dispone a reanudar una suscripción sin terminar, debe seleccionar el punto de confianza asociado con la misma y, a continuación, especificar la parte del proceso de suscripción que necesita completar. Si está importando un certificado del servidor de la CA o un certificado de router, éstos deben estar disponibles en el PC.

## Seleccione el apodo del servidor de la CA (punto de confianza)

Seleccione el punto de confianza asociado con la suscripción que está llevando a cabo.

## Importar el o los certificados de la CA y del router

Seleccione esta opción cuando desee importar tanto el certificado del servidor de la CA como el certificado del router en una sola sesión. Ambos certificados deben estar disponibles en el PC.

Esta opción estará desactivada si ya se ha importado el certificado de la CA.

## Importar el certificado de la CA

Seleccione esta opción para importar un certificado del servidor de la CA que haya guardado en el PC. Después de importar el certificado, Cisco SDM mostrará la “huella dactilar” digital correspondiente. A continuación, podrá comprobar el certificado y aceptarlo o rechazarlo.

Esta opción estará desactivada si ya se ha importado el certificado de la CA.

## Importar el o los certificados de router

Seleccione esta opción para importar un certificado para el router que haya guardado en el PC. Después de esta operación, Cisco SDM mostrará el estado del proceso de suscripción.

**Nota**

Debe importar el certificado del servidor de la CA antes de importar el certificado del router.

## Generar solicitud de suscripción

Seleccione esta opción si necesita generar una solicitud de suscripción para el punto de confianza seleccionado. El router generará una solicitud de suscripción que se guardará en el PC y se enviará a la CA.

Cisco SDM genera una solicitud de suscripción de tipo PKCS#10 codificado base 64.

# Importar el certificado de la CA

Si dispone del certificado del servidor de la CA en el disco duro, puede buscarlo e importarlo al router mediante esta ventana. También puede copiar el texto del certificado y pegarlo en el área de texto de esta ventana.

## Botón Examinar

Haga clic en este botón para localizar el archivo de certificado en el PC.

# Importar el o los certificados de router

Si en el disco duro dispone de uno o varios certificados para el router concedidos por la CA, puede buscarlos e importarlos al router.

## Importar certificados adicionales

Si ha generado pares de claves RSA independientes para el cifrado y la firma, recibirá dos certificados para el router. Utilice este botón en el caso de disponer de más de un certificado de router para su importación.

## Quitar certificado

Haga clic en la ficha del certificado que desee quitar y, a continuación, en **Quitar**.

## Examinar

Localice el certificado para importarlo en el router.

# Certificados digitales

Esta ventana permite ver información acerca de los certificados digitales configurados en el router.

## Puntos de confianza

Esta área muestra información resumida para los puntos de confianza configurados en el router y permite ver los detalles de los puntos de confianza, editarlos y determinar si alguno de ellos ha sido revocado.

### Botón Detalles

La lista de puntos de confianza sólo muestra el nombre, la URL de suscripción y el tipo de suscripción de un punto de confianza. Haga clic en este botón para ver toda la información acerca del punto de confianza seleccionado.

### Botón Editar

Un punto de confianza puede editarse si es del tipo SCEP y si no se ha importado correctamente el certificado del servidor de la CA ni el certificado del router. Si el punto de confianza no es del tipo SCEP o si se ha enviado tanto el certificado del servidor de la CA como el del router asociados con un punto de confianza SCEP, este botón estará desactivado.

### Botón Eliminar

Haga clic en este botón para eliminar el punto de confianza seleccionado. Esta operación destruye todos los certificados que se hayan recibido de la CA asociada.

**Botón Comprobar revocación**

Haga clic en este botón para comprobar si el certificado seleccionado ha sido revocado. Cisco SDM muestra un cuadro de diálogo en el que se debe seleccionar el método que se utilizará para comprobar la revocación. Consulte [Comprobar revocación](#) y [Comprobar revocación de CRL únicamente](#) para obtener más información.

<b>Nombre</b>	Nombre del punto de confianza.
<b>Servidor de la CA</b>	Nombre o dirección IP del servidor de la CA.
<b>Tipo de suscripción</b>	<p>Uno de los siguientes:</p> <ul style="list-style-type: none"> <li>• SCEP (Simple Certificate Enrollment Protocol): la suscripción se ha realizado mediante una conexión directa al servidor de la CA.</li> <li>• Cortar y pegar: la solicitud de suscripción se ha importado desde un PC.</li> <li>• TFTP: la solicitud de suscripción se ha realizado mediante un servidor TFTP.</li> </ul>

**Certificate chain for trustpoint *name* (Nombre de la cadena de certificados para el punto de confianza)**

Esta área muestra los detalles de los certificados asociados con el punto de confianza seleccionado.

**Botón Detalles**

Haga clic en este botón para ver el certificado seleccionado.

**Botón Actualizar**

Haga clic en este botón para actualizar el área de cadena de certificados cuando seleccione otro punto de confianza en la lista de puntos de confianza.

<b>Tipo</b>	<p>Uno de los siguientes:</p> <ul style="list-style-type: none"> <li>• RA KeyEncipher Certificate: certificado de cifrado de Rivest Adelman.</li> <li>• RA Signature Certificate (Certificado de firma RA): certificado con la firma Rivest Adelman.</li> <li>• Certificado del servidor de la CA: el certificado de la organización de CA.</li> <li>• Certificate (Certificado): el certificado del router.</li> </ul>
<b>Uso</b>	<p>Uno de los siguientes:</p> <ul style="list-style-type: none"> <li>• Objetivo general: un certificado de objetivo general que el router utiliza para autenticarse en los homólogos remotos.</li> <li>• Firma: los certificados de CA son certificados de firma.</li> </ul>
<b>Número de serie</b>	Número de serie del certificado.
<b>Emisor</b>	Nombre de la CA que ha emitido el certificado.
<b>Estado</b>	<p>Uno de los siguientes:</p> <ul style="list-style-type: none"> <li>• Disponible: el certificado está disponible para su uso.</li> <li>• Pending (Pendiente): el certificado se ha solicitado pero no está disponible para su uso.</li> </ul>
<b>Vence al cabo de (días)</b>	Número de días durante los cuales puede utilizarse el certificado antes de su vencimiento.
<b>Fecha de vencimiento</b>	Fecha en la que caduca el certificado.

## Información acerca del punto de confianza

La lista de puntos de confianza de la ventana Certificados de router muestra información clave acerca de cada punto de confianza del router. Esta ventana ofrece todos los datos que se han proporcionado para crear el punto de confianza.

## Detalles del certificado

Esta ventana muestra los detalles del punto de confianza que no aparecen en la ventana Certificados.

## Comprobar revocación

Especifique en esta ventana cómo el router debe comprobar si el certificado ha sido revocado.

### Comprobar revocación

Configure cómo el router debe comprobar las revocaciones y disponga los métodos por orden de preferencia. El router puede utilizar varios métodos.

#### Usar/Método/Desplazar hacia arriba/Desplazar hacia abajo

Marque los métodos que desee emplear y utilice los botones **Desplazar hacia arriba** y **Desplazar hacia abajo** para colocarlos en el orden en que desea utilizarlos.

- OCSP: establecer conexión con un servidor OCSP (Online Certificate Status Protocol) para determinar el estado de un certificado.
- CRL: la revocación del certificado se comprueba mediante una lista de revocaciones de certificados.
- Ninguno: no realizar ninguna comprobación de revocación.

#### URL de consulta CRL

Se activa cuando se selecciona CRL. Especifique la URL en la que se encuentra la lista de revocaciones de certificados. Especifique la URL solamente si el certificado admite X.500 DN.

#### URL de OCSP

Se activa cuando se selecciona OCSP. Especifique la URL del servidor OCSP con el que desea ponerse en contacto.



## Comprobar revocación de CRL únicamente

Especifique en esta ventana cómo el router debe comprobar si el certificado ha sido revocado.

### Comprobación

Uno de los siguientes:

- Ninguna: comprobar el punto de distribución incorporado en el certificado de la Lista de revocación de certificados (CRL).
- Mejor esfuerzo: descargar la CRL del servidor de CRL, si está disponible. Si no lo está, se aceptará el certificado.
- Opcional: comprobar la CRL solamente si ya se ha descargado en el caché como resultado de una carga manual.

### CRL Query URL (URL de consulta CRL)

Especifique la URL en la que se encuentra la lista de revocaciones de certificados. Especifique la URL solamente si el certificado admite X.500 DN.

## Ventana Claves RSA

Las claves RSA proporcionan un sistema de cifrado y autenticación que utiliza un algoritmo desarrollado por Ron Rivest, Adi Shamir y Leonard Adelman. El sistema RSA es el algoritmo de cifrado y autenticación que se utiliza con mayor frecuencia y se incluye con IOS de Cisco. Para utilizar este sistema, un host de red genera un par de claves; una se denomina *clave pública* y la otra *clave privada*. La clave pública se entrega a cualquier usuario que desee enviar datos cifrados al host. La clave privada nunca se comparte. Cuando un host remoto desea enviar datos, éste los cifra utilizando la clave pública que comparte con el host local, el cual, a su vez, recurre a la clave privada para descifrar los datos enviados.

## Claves RSA configuradas en el router

<b>Nombre</b>	El nombre de la clave. Cisco SDM asigna automáticamente los nombres de claves. Las claves “HTTPS_SS_CERT_KEYPAIR” y “HTTPS_SS_CERT_KEYPAIR.server” se mostrarán como de sólo lectura. De manera similar, toda clave bloqueada o cifrada en el router aparecerá con iconos que indican su estado.
<b>Uso</b>	De uso u objetivo general. Las claves de objetivo general se utilizan para cifrar datos y firmar el certificado. Si se configuran claves independientes para cifrar datos y firmar certificados, dichas claves se denominan claves de uso.
<b>Exportable</b>	Si esta columna contiene una marca de verificación, la clave puede exportarse a otro router si éste debe asumir el papel del router local.

### Key Data (Datos de la clave)

Haga clic en este botón para ver la clave RSA seleccionada.

### Botón Save Key to PC (Guardar clave en PC)

Haga clic en este botón para guardar los datos de la clave seleccionada en el PC.

## Generar par de claves RSA

Utilice esta ventana para generar un nuevo par de claves RSA.

### Etiqueta

Especifique la etiqueta de la clave en este campo.

## Módulo

Especifique el valor del módulo de la clave. Si desea un valor de módulo de 512 a 1.024, especifique un valor entero que sea múltiple de 64. Si desea un valor mayor que 1.024, puede especificar 1.536 ó 2.048. Si especifica un valor mayor que 512, es posible que la generación de la clave tarde un minuto o más.

Cuanto mayor sea el módulo, más segura será la clave. Sin embargo, las claves con módulos grandes tardan más tiempo en generarse y su procesamiento durante el intercambio es también más largo.

## Tipo

Seleccione el tipo de clave que debe generarse, **Objetivo general** o **Uso**. Las claves de objetivo general se utilizan tanto para el cifrado como para la firma de los certificados. Si genera claves de tipo **Uso**, un conjunto de claves se empleará para el cifrado y otro conjunto independiente para la firma de certificados.

## Casilla de verificación La clave se puede exportar

Marque esta casilla si desea que la clave se pueda exportar. Un par de claves exportable puede enviarse a un router remoto si este último necesita asumir las funciones del router local.

## Guardar en el Token USB

Marque la casilla de verificación **Guardar claves y certificados en un token USB seguro** si desea guardar las claves y certificados RSA en un token conectado a su router. Esta opción solamente aparece si hay un token USB conectado a su router.

Seleccione el token USB del menú desplegable **Token USB**. Especifique el PIN requerido para iniciar sesión en el token USB deseado en **PIN**.

Después de elegir un token USB e introducir el PIN correspondiente, haga clic en **Inicio de sesión** para acceder al token USB.

## Credenciales del token USB

Esta ventana aparece cuando se agregan o eliminan credenciales, como por ejemplo un par de claves RSA o certificados digitales, que han sido guardadas en un token USB. Para que la eliminación surta efecto, se debe proporcionar el nombre del token USB y el PIN.

Seleccione el token USB del menú desplegable **Token USB**. Especifique el PIN requerido para iniciar sesión en el token USB deseado en **PIN**.

## Tokens USB

Esta ventana permite configurar el acceso a tokens USB. Esta ventana también muestra una lista de los registros de acceso al token USB configurados. Al conectar un token USB al router Cisco, Cisco SDM utiliza el registro de acceso correspondiente para acceder al token.

### Agregar

Haga clic en **Agregar** para agregar una nueva conexión al token USB.

### Editar

Haga clic en **Editar** para editar una conexión al token USB existente. Especifique la conexión a editar seleccionándola de la lista.

### Eliminar

Haga clic en **Eliminar** para eliminar una conexión al token USB existente. Especifique la conexión a eliminar seleccionándola de la lista.

### Nombre del token

Muestra el nombre utilizado para ingresar al token USB.

### PIN de usuario

Muestra el PIN utilizado para acceder al token USB.

## Máximo de reintentos del PIN

Muestra el máximo de intentos de Cisco SDM para acceder al token USB con el PIN proporcionado. Si después de intentar el número de veces indicado Cisco SDM no tiene éxito, dejará de intentar acceder al token USB.

## Tiempo máximo de desinserción

Muestra el máximo de segundos que Cisco SDM seguirá usando las credenciales de Intercambio de claves por Internet (IKE) obtenidas del token USB una vez que el token se desconecta del router.

Si la opción Tiempo Máximo de desinserción está vacía, se utiliza el tiempo máximo por defecto. El tiempo máximo por defecto se activa al realizar un nuevo intento de acceder las credenciales IKE.

## Archivo secundario de configuración

Muestra el archivo de configuración que Cisco SDM intenta encontrar en el token USB. El archivo de configuración puede ser un archivo CCCD o un archivo .cfg. CCCD se refiere a un archivo de configuración del arranque. En el caso de los tokens USB, el archivo CCCD se carga usando un software TMS.

# Agregar o Editar un token USB

Esta ventana permite agregar o editar registros de ingreso al token USB.

## Nombre del token

Si está agregando un registro de acceso al token USB, especifique el nombre del token USB. Este nombre debe coincidir con el nombre del token al cual desea acceder.

El nombre del token viene definido de fábrica. Por ejemplo, los tokens fabricados por Aladdin Knowledge Systems tienen como nombre eToken.

También puede utilizar el nombre “usbtoken $x$ ”, donde  $x$  es el número de puerto USB donde se conecta el token USB. Por ejemplo, un token conectado al puerto USB 0 se llamará usbtoken0.

Si está editando un registro de ingreso al token USB no se puede cambiar el campo Nombre del Token.

## **PIN actual**

Si está agregando una conexión al token USB o si está editando una conexión a un token USB que no posee PIN, el campo PIN Actual muestra la palabra <Ninguno>. Si está editando un registro de acceso a un token USB que posee PIN, el campo PIN Actual muestra \*\*\*\*\*.

## **Especifique nuevo PIN**

Especifique un nuevo PIN para el token USB. El nuevo PIN debe contener al menos cuatro dígitos y debe coincidir con el nombre del token al cual se quiere acceder. Si está editando un registro de acceso a un token USB el PIN Actual será reemplazado por el nuevo PIN.

## **Reintroduzca el nuevo PIN**

Reintroduzca el nuevo PIN para confirmarlo.

## **Máximo de reintentos del PIN**

Seleccione el máximo de intentos de Cisco SDM para acceder al token USB con el PIN proporcionado. Si después de intentar el número de veces indicado Cisco SDM no tiene éxito, dejará de intentar acceder al token USB.

## **Tiempo máximo de desinserción**

Introduzca el máximo de segundos que Cisco SDM seguirá usando las credenciales de Intercambio de Claves por Internet (IKE) obtenidas del token USB una vez que el token desconecta del router. El número de segundos debe estar en el rango de 0 a 480.

Si no especifica un número, se utilizará el tiempo máximo por defecto. El tiempo máximo por defecto se activa al realizar un nuevo intento de acceder las credenciales IKE.

## **Archivo secundario de configuración**

Especifica un archivo de configuración existente en el token USB. El archivo puede ser un archivo de configuración parcial o completo. La extensión del archivo debe ser .cfg.

Si Cisco SDM logra acceder al token USB, fusionará el archivo de configuración especificado con la configuración en ejecución del router.

# Abrir Firewall

Esta pantalla aparece cuando Cisco SDM detecta algún firewall en las interfaces que pueda bloquear el tráfico de vuelta que el router debe recibir. Existen dos situaciones en las que dicha ventana podrá aparecer: cuando un firewall bloquee tráfico DNS o cuando bloquee tráfico PKI e impide que el router reciba dicho tráfico desde los servidores. Cisco SDM puede modificar estos firewalls para que los servidores se puedan comunicar con el router.

## Modificar el firewall

Esta área proporciona una lista de las interfaces de salida y los nombres de la ACL. Además, permite seleccionar los firewalls que desea que Cisco SDM modifique. Seleccione los firewalls que desea que Cisco SDM modifique en la columna Acción. Cisco SDM los modificará para permitir el tráfico SCEP o DNS desde el servidor al router.

Tenga en cuenta lo siguiente respecto al tráfico SCEP:

- Cisco SDM no modificará el firewall para los servidores CRL/OCSP si éstos no se han configurado explícitamente en el router. Para permitir la comunicación con servidores CRL/OCSP, obtenga la información correspondiente del administrador del servidor de la CA y modifique el firewall utilizando la ventana de Editar Política de Firewall Policy/ACL.
- Cisco SDM supone que el tráfico que se envía desde el servidor de la CA hacia el router accederá mediante las mismas interfaces a través de las cuales se ha enviado el tráfico desde el router hacia el servidor de la CA. Si cree que el tráfico de vuelta desde el servidor de la CA accederá al router a través de una interfaz distinta de la que indica Cisco SDM, deberá abrir el firewall mediante la ventana Editar política de firewall / ACL. Esto podrá suceder cuando se utiliza un enrutamiento asimétrico, en el que el tráfico sale desde el router hacia el servidor de la CA a través de una interfaz y el tráfico de vuelta accede al mismo a través de una interfaz distinta.

- Cisco SDM determina las interfaces de salida del router en el momento en que se agrega la ACE de paso. Si se utiliza un protocolo de enrutamiento dinámico para obtener las rutas hacia el servidor de la CA y la ruta cambia (la interfaz de salida cambia para el tráfico SCEP con destino al servidor de la CA), debe agregar explícitamente una ACE de paso para las interfaces mediante la ventana Editar política de firewall / Lista de control de acceso.
- Cisco SDM agrega ACE de paso para el tráfico SCEP, pero no ocurre lo mismo para el tráfico de revocación como, por ejemplo, el tráfico CRL y OCSP. Debe agregar explícitamente ACE de paso para este tipo de tráfico mediante la ventana Editar política de firewall / Lista de control de acceso.

### Botón Detalles

Haga clic en este botón para ver la entrada de control de acceso que Cisco SDM agregará al firewall si permite la modificación.

## Abrir detalles del firewall

Esta ventana muestra la entrada de control de acceso (ACE) que Cisco SDM agregaría a un firewall para permitir que varios tipos de tráfico lleguen al router. Esta entrada no se agrega si no se activa la casilla **Modificar** de la ventana Abrir Firewall y se completa el asistente.





# CAPÍTULO 18

## Servidor de la autoridad certificadora

---

Puede configurar un router de Cisco IOS para que cumpla la función de servidor de la Autoridad certificadora (CA). Un servidor de la CA maneja las solicitudes de suscripción de certificados de los clientes, y puede emitir y revocar certificados digitales.

Para crear, respaldar, restaurar o editar un servidor de la CA, vaya a **Configurar > VPN > Infraestructura de clave pública > Autoridad certificadora > Crear servidor de la CA**.

Para administrar certificados en un servidor de la CA existente, vaya a **Configurar > VPN > Infraestructura de clave pública > Autoridad certificadora > Administrar servidor de la CA**.

Para supervisar un servidor de la CA, vaya a **Supervisar > Estado de la red VPN > Servidor de la CA**.

## Crear servidor de la CA

Esta ventana le permite iniciar un asistente para crear un servidor de Autoridad certificadora (CA) o un asistente para restaurar un servidor de la CA. Sólo se puede configurar un servidor de la CA en un router de Cisco IOS.

El servidor de la CA se debe utilizar para emitir certificados a hosts en la red privada, de modo que puedan usar los certificados para autenticarse entre ellos

## Tareas previas

Si Cisco SDM identifica tareas de configuración que deben establecerse antes de comenzar el proceso de configuración del servidor de la CA, le notificará de las mismas en esta casilla. Se proporciona un enlace junto al texto de alerta para que pueda desplazarse hasta el área correspondiente de Cisco SDM y establecer dicha configuración. Si Cisco SDM no detecta la falta de configuraciones, este cuadro no aparece. Las posibles tareas previas se describen en [Tareas previas para configuraciones de PKI](#).

### Crear servidor de la autoridad certificadora (CA)

Haga clic en este botón para crear un servidor de CA en el router. Puesto que sólo se puede configurar un servidor de la CA en el router, este botón está desactivado si ya se configuró un servidor de la CA.

**Nota**

---

El servidor de la CA que configura con SDM le permite otorgar y revocar certificados. Aunque el router no guarda los números de serie ni otra información de identificación acerca de los certificados que otorga, no guarda los certificados. El servidor de la CA se debe configurar con una URL en un servidor de Autoridad de registro (RA) que pueda guardar certificados otorgados por el servidor de la CA.

---

### Restaurar servidor de la autoridad certificadora (CA)

Si un servidor de la CA ya opera en el router, puede restaurar su configuración y la información. Si no se ha configurado un servidor de la CA en el router, esta opción estará desactivada.

## Tareas previas para configuraciones de PKI

Antes de comenzar una suscripción de certificados o configuración del servidor de CA, puede ser necesario completar antes las tareas de configuración de soporte. SDM revisa la configuración en ejecución antes de permitirle comenzar, le advierte de las configuraciones que debe completar, y proporciona enlaces que lo llevan a las áreas de SDM que le permiten completar estas configuraciones.

SDM puede generar alertas acerca de las siguientes tareas de configuración:

- **Credenciales SSH no verificadas:** Cisco SDM requiere que proporcione credenciales para SSH antes de comenzar.
- **NTP/SNTP sin configurar:** la hora del router debe ser exacta para que funcione la suscripción de certificados. La identificación de un servidor NTP (Network Time Protocol) a partir del cual el router puede obtener la hora exacta ofrece una fuente de hora que no se verá afectada en el caso de que deba reiniciarse el router. Si su organización no dispone de ningún servidor NTP, tiene la opción de utilizar un servidor disponible públicamente como, por ejemplo, el servidor que se describe en la dirección URL siguiente:  
`http://www.eecis.udel.edu/~mills/ntp/clock2a.html`
- **DNS sin configurar:** la especificación de servidores DNS contribuye a garantizar que el router podrá ponerse en contacto con el servidor de certificados. La configuración DNS se requiere para ponerse en contacto con el servidor de la CA y con cualquier otro servidor relacionado con la suscripción de certificados como, por ejemplo, servidores OCSP o repositorios CRL en el caso de que dichos servidores se especifiquen como nombres y no como direcciones IP.
- **Dominio o nombre de host sin especificar:** se recomienda configurar un dominio y nombre de host antes de comenzar la suscripción.

## Asistente para el servidor de la CA: Bienvenido

El asistente para el servidor de la Autoridad certificadora (CA) le guía en la configuración de un servidor de la CA. Antes de empezar asegúrese de tener la información siguiente:

- **Información general acerca del servidor de la CA:** el nombre que desea dar al servidor, el nombre del emisor del certificado que desea usar, y el nombre de usuario y la contraseña que se solicitará ingresar a los suscritos cuando envíen una solicitud de suscripción al servidor.
- **Información más detallada sobre el servidor:** si el servidor opera en modo Autoridad de registro (RA) o Autoridad certificadora (CA), el nivel de información acerca de cada certificado que el servidor guardará, si el servidor debe otorgar certificados automáticamente, y la duración de los certificados otorgados, y solicitudes de suscripción abiertas.
- **Información de soporte:** enlaza al servidor RA que guardará los certificados y al servidor de Punto de distribución de la lista de revocaciones de certificados (CDP).

## Asistente para el servidor de la CA: Información acerca de la Autoridad certificadora

Especifique información básica acerca del servidor de CA que está configurando en esta ventana.

### Nombre del servidor de la CA

Proporcione un nombre que permita identificar el servidor en el campo Nombre del servidor de la CA. Puede ser el nombre de host del router u otro nombre que especifique.

### Otorgar

Seleccione **Manual** si desea otorgar certificados de forma manual. Seleccione **Auto** si desea que el servidor otorgue certificados de forma automática. Auto, utilizado principalmente para depuración, no se recomienda porque emitirá certificados a cualquier solicitante sin exigirles la información de suscripción.



¡Advertencia!

---

**No defina Otorgar en Auto si el router está conectado a Internet. Otorgar se debe definir en Auto sólo para propósitos internos, como, por ejemplo, cuando se ejecutan procedimientos de depuración.**

---

### URL de CDP

Especifique la URL para un servidor de Punto de distribución de la Lista de revocación de certificados (CDP) en el campo URL de CDP. La URL debe ser una URL de HTTP. La siguiente es una URL de ejemplo:

```
http://172.18.108.26/cisco1cdp.cisco1.crl
```

CRL es la lista de certificados revocados. Los dispositivos que necesitan comprobar la validez del certificado de otro dispositivo, buscarán en la CRL del servidor de la CA. Puesto que muchos dispositivos pueden intentar buscar en la CRL, descargarla en un dispositivo remoto, de preferencia un servidor HTTP, reducirá el impacto del rendimiento en el router de Cisco IOS que aloja al servidor de la CA. Si el dispositivo que se comprueba no se conecta al CDP, como reserva utilizará SCEP para buscar en la CRL desde el servidor de la CA.

## Atributos de nombre de emisor

### **Common Name [Nombre común (cn)]**

Especifique el nombre común que desea utilizar para el certificado. Puede ser el nombre del servidor de la CA, el nombre de host del router u otro nombre que especifique.

### **Organizational Unit (ou) [Unidad organizativa (ou)]**

Especifique una unidad organizativa o nombre de departamento para su uso con este certificado. Por ejemplo, Soporte de TI o Ingeniería podrían ser unidades organizativas.

### **Organización (o)**

Especifique el nombre de la organización o empresa.

### **Estado (st)**

Especifique la provincia o el estado en el que se encuentra la organización.

### **País (c)**

Especifique el país en el que se encuentra la organización.

### **Correo electrónico (e)**

Especifique la dirección de correo electrónico que debe incluirse en el certificado del router.

## Opciones avanzadas

Haga clic en este botón para especificar opciones avanzadas para el servidor de la CA.

## Opciones avanzadas

La pantalla Opciones avanzadas le permite cambiar valores por defecto para la configuración del servidor y especificar la URL para la base de datos que va a contener la información del certificado.

## Base de datos

Configure el nivel, la URL y el formato de la base de datos en esta sección del cuadro de diálogo.

### Nivel de la base de datos

Seleccione el tipo de datos que se guardará en la base de datos de suscripción de certificados:

- **mínimo:** se guarda información suficiente para continuar emitiendo nuevos certificados sin conflicto. Este es el valor por defecto.
- **nombres:** además de la información proporcionada por la opción mínima, esta opción incluye el número de serie y el nombre del asunto de cada certificado.
- **completo:** además de la información proporcionada por las opciones mínimo y nombres, cada certificado emitido se copia en la base de datos.

### URL de la base de datos

Especifique la ubicación en la cual el servidor de la CA escribirá datos de suscripción de certificados. Si no se especifica una ubicación, los datos de suscripción de certificados se escribirán por defecto en la memoria flash.

Por ejemplo, para escribir datos de suscripción de certificados en un servidor tftp, especifique tftp://mytftp. Para restablecer la URL de la base de datos en la memoria flash, escriba nvram.

### Archivo de base de datos

Seleccione **pem** para crear el archivo en formato pem, o **pkcs12** para crear el archivo en formato pkcs12.

### Nombre de usuario de base de datos

Especifique un nombre de usuario para el archivo de la base de datos en el campo Nombre de usuario de base de datos. El nombre de usuario y la contraseña se usarán para autenticar el servidor en la base de datos.

### Contraseña de la base de datos y confirmar contraseña

Especifique una contraseña en el campo Contraseña de la base de datos y vuelva a especificarla en el campo Confirmar contraseña.

## Duraciones

Defina la duración, o el tiempo antes del vencimiento, de los elementos asociados con el servidor de la CA. Para definir la duración de un elemento específico, selecciónelo desde la lista desplegable Duración y especifique un valor en el campo Duración.

Puede definir duraciones para los siguientes elementos:

- **Certificado:** certificados emitidos por el servidor de la CA. La duración se especifica en días, en el intervalo 1–1825. Si no se especifica un valor, un certificado vence después de un año. Si se especifica un nuevo valor, éste afecta a los certificados que se crean sólo después de que se aplica ese valor.
- **CRL:** Lista de revocación de certificados para certificados emitidos por el servidor de la CA. La duración se especifica en horas, en el intervalo 1–336. Si no se especifica un valor, una CRL vence después de 168 horas (una semana).
- **Solicitud de suscripción:** solicitudes de certificados abiertas que existen en la base de datos de suscripciones, pero que no incluyen solicitudes recibidas mediante SCEP. La duración se especifica en horas, en el intervalo 1–1.000. Si no se especifica un valor, una solicitud de suscripción abierta vence después de 168 horas (una semana).

## Asistente para el servidor de la CA: Claves RSA

El servidor de la CA utiliza [claves RSA](#) públicas y privadas para cifrar datos y firmar certificados. SDM genera automáticamente un nuevo par de claves y le da el nombre del servidor de la CA. Puede cambiar el módulo y tipo de la clave, y puede hacer que la clave se pueda exportar. Especifique una frase de contraseña para utilizar cuando restaure el servidor de la CA.

### Etiqueta

Este campo es de sólo lectura. SDM utiliza el nombre del servidor de la CA como el nombre del par de claves.

## Módulo

Especifique el valor del módulo de la clave. Si desea un valor de módulo de 512 a 1.024, especifique un valor entero que sea múltiplo de 64. Si desea un valor mayor que 1.024, puede especificar 1.536 ó 2.048. Si especifica un valor mayor que 512, es posible que la generación de la clave tarde un minuto o más.

El módulo determina el tamaño de la clave. Cuanto mayor sea el módulo, más segura será la clave. Sin embargo, las claves con módulos grandes tardan más tiempo en generarse. Del mismo modo, las operaciones de cifrado y descifrado se prolongan si contienen claves grandes.

## Tipo

Por defecto, Cisco SDM crea un par de claves de objetivo general que se utilizará para el cifrado y la firma. Si desea que Cisco SDM genere pares de claves independientes para el cifrado y la firma de documentos, seleccione **Claves de uso**. Cisco SDM generará claves de uso para el cifrado y la firma.

## La clave se puede exportar

Marque **La clave se puede exportar** si desea que la clave del servidor de la CA se pueda exportar.

## Frase de contraseña y confirmar frase de contraseña

En el campo Frase de contraseña, especifique una frase de contraseña para utilizar cuando restaure el servidor de la CA de reserva. En el campo Confirmar frase de contraseña, vuelva a especificar la misma frase de contraseña.

## Abrir Firewall

La ventana Abrir firewall aparece cuando es necesario modificar una configuración de firewall para permitir la comunicación entre el servidor de [CDP](#) y [servidor de la CA](#). Seleccione la interfaz y marque la casilla **Modificar** para que SDM pueda modificar el firewall para permitir este tráfico. Haga clic en **Detalles** para ver la [ACE](#) que se agregaría al firewall.



## Asistente para el servidor de la CA: Resumen

La ventana Resumen muestra la información que ha especificado en las pantallas del asistente para que pueda revisar la información antes de enviarla al router. A continuación, se muestra un ejemplo del resumen:

```
-----  
Configuración del servidor de la CA  
-----
```

```
Nombre del servidor de la CA: CASvr-a  
Otorgamiento:Manual  
URL de CDP:http://192.27.108.92/snrs.com  
Nombre común (cn):CS1841  
Unidad organizativa (ou): IT Support  
Organización (o):Acme Enterprises  
Estado (st): CA  
País (c): EE.UU.
```

```
-----  
Configuración avanzada del servidor de la CA  
-----
```

```
URL de la base de datos: nvram:  
Archivo de base de datos:pem  
Nombre de usuario de base de datos:bjones  
Contraseña de la base de datos:*****
```

```
-----  
Claves RSA:  
-----
```

El servidor de la CA genera automáticamente un par de claves de RSA con los siguientes valores por defecto:

```
Módulo:1024  
Tipo de clave:Objectivo general  
Clave exportable:No  
Frase de contraseña configurada:*****
```

```
-----  
ACE de paso en firewall para interfaces:  
-----
```

```
FastEthernet0/0  
  permit tcp host 192.27.108.92 eq www host 192.27.108.91 gt 1024
```

La pantalla de resumen contiene cuatro secciones: sección Configuración del servidor de la CA, sección Configuración avanzada del servidor de la CA, sección Claves de RSA y sección Paso de firewall. El nombre de este servidor de la CA es CASvr-a. Los certificados se otorgarán manualmente. La información del certificado se guarda en nvram, en formato [PEM](#). SDM generará un par de claves de objetivo general con el módulo por defecto, 1024. La clave no se podrá exportar. Se configurará una ACE para permitir el tráfico entre el router y el host de [CDP](#) con la dirección IP 192.27.108.92.

## Administrar servidor de la CA

Puede iniciar y detener el servidor de la CA desde esta ventana, otorgar y rechazar solicitudes de certificados, y revocar certificados. Si necesita cambiar la configuración del servidor de la CA, puede desinstalar el servidor desde esta ventana y volver a la ventana Crear servidor de la CA para crear la configuración de servidor que necesita.

### Nombre

Muestra el nombre del servidor. El nombre del servidor se creó cuando se creó el servidor.

### Icono de estado

Si el servidor de la CA está en ejecución, se muestra la palabra En ejecución y un icono verde. Si el servidor de la CA no está en ejecución, se muestra la palabra Detenido y un icono rojo.

### Iniciar servidor

El botón Iniciar servidor se muestra si se detiene el servidor. Haga clic en **Iniciar servidor** para iniciar el servidor de la CA.

### Detener servidor

El botón Detener servidor se muestra si el servidor está en ejecución. Haga clic en **Detener servidor** si necesita detener el servidor de la CA.

## Servidor de reserva

Haga clic en **Servidor de reserva** para respaldar la información de configuración del servidor en el equipo. Especifique la ubicación de reserva en el cuadro de diálogo que se muestra.

## Desinstalar servidor

Haga clic para desinstalar el servidor de la CA desde el router de Cisco IOS. Se eliminará toda la configuración y los datos del servidor de la CA. Si respaldó el servidor de la CA antes de desinstalarlo, puede restaurar sus datos sólo después de crear un nuevo servidor de la CA. Consulte [Crear servidor de la CA](#).

## Detalles del servidor de la CA

La tabla Detalles del servidor de la CA proporciona una instantánea de la configuración del servidor de la CA. La tabla siguiente muestra un ejemplo de información.

Nombre de elemento	Valor de elemento
Duración del certificado de la CA	1.095 días
URL de CDP	http://192.168.7.5
Duración de CRL	168 horas
Duración del certificado	365 días
Nivel de la base de datos	mínimo
URL de la base de datos	nvrám:
Duración de la solicitud de suscripción	168 horas
Otorgamiento	manual
Nombre del emisor	CN=CertSvr
Modo	Autoridad certificadora
Nombre	CertSvr

Consulte [Asistente para el servidor de la CA: Información acerca de la Autoridad certificadora](#) y [Opciones avanzadas](#) para ver descripciones de estos elementos.

## Servidor de la CA de reserva

Puede respaldar los archivos que contienen la información del [servidor de la CA](#) en su equipo. La ventana Servidor de la CA de reserva enumera los archivos que se respaldarán. Los archivos que se listan deben estar presentes en la NVRAM del router para que el respaldo sea satisfactorio.

Haga clic en **Examinar** y especifique una carpeta del equipo en la cual se deben respaldar los archivos del servidor de la CA.

## Administrar servidor de la CA: Restaurar ventana

Si ha respaldado y desinstalado un [servidor de la CA](#), puede restaurar la configuración del servidor en el router, haciendo clic en el botón **Restaurar servidor de la CA**. Debe ser capaz de proporcionar el nombre del servidor de la CA, completar la URL de la base de datos y la frase de contraseña de reserva que se usó durante la configuración inicial. Cuando restaura el servidor de la CA, se le da la oportunidad de cambiar los ajustes de la configuración.

## Restaurar servidor de la CA

Si ha respaldado la configuración de un [servidor de la CA](#) que se desinstaló, puede restaurarla proporcionando la información acerca de él en la ventana Restaurar servidor de la CA. Puede editar la configuración del servidor haciendo clic en **Editar configuración del servidor de la CA antes de la restauración**. Debe proporcionar el nombre, el formato de archivo, la URL a la base de datos y la frase de contraseña para respaldar el servidor o editar su configuración.

### Nombre del servidor de la CA

Especifique el nombre del servidor de la CA que respaldó.

### Formato de archivo

Seleccione el formato de archivo que especificó en la configuración del servidor: [PEM](#) o [PKCS12](#).

## Completar la URL

Especifique la URL de la base de datos del router que se proporcionó cuando se configuró el servidor de la CA. Ésta es la ubicación en la cual el servidor de la CA escribe datos de suscripción de certificados. A continuación se entregan dos ejemplos de URL:

```
nvrnm:/mycs_06.p12  
tftp://192.168.3.2/mycs_06.pem
```

## Frase de contraseña

Especifique la frase de contraseña que se proporcionó cuando se configuró el servidor de la CA.

## Copiar archivos del servidor de la CA del equipo

Marque la casilla de verificación **Copiar archivos del servidor de la CA del equipo** para copiar la información del servidor que respaldó en el PC para la nvrnm del router.

## Editar configuración del servidor de la CA antes de la restauración

Haga clic en **Editar configuración del servidor de la CA antes de la restauración** para cambiar la configuración del servidor de la CA antes de restaurar el servidor. Consulte [Asistente para el servidor de la CA: Información acerca de la Autoridad certificadora](#) y [Asistente para el servidor de la CA: Claves RSA](#) para obtener información acerca de las configuraciones que puede cambiar.

## Editar configuración del servidor de la CA: Ficha General

Edite la configuración del servidor de la CA en esta ventana. No puede cambiar el nombre del servidor de la CA. Para obtener información sobre las configuraciones que puede cambiar, consulte [Asistente para el servidor de la CA: Información acerca de la Autoridad certificadora](#).

## Editar configuración del servidor de la CA: Ficha Avanzado

Puede cambiar cualquier configuración del servidor de la CA avanzado en esta ventana. Para obtener información sobre estas configuraciones, consulte [Opciones avanzadas](#).

# Administrar servidor de la CA: Servidor de la CA no configurado

Esta ventana aparece cuando hace clic en **Administrar servidor de la CA**, pero no se ha configurado ningún servidor de la CA. Haga clic en **Crear servidor de la CA** y complete el asistente para configurar un servidor de la CA en el router.

## Administrar certificados

Al hacer clic en VPN > Infraestructura de clave pública > Autoridad certificadora > Administrar certificados, se muestra la ficha Solicitudes pendientes y la ficha Certificados revocados. Para ir a los temas de ayuda para estas fichas, haga clic en los siguientes enlaces:

- [Solicitudes pendientes](#)
- [Certificados revocados](#)

## Solicitudes pendientes

Esta ventana muestra una lista de solicitudes de suscripción de certificados recibidas por el servidor de la CA de los clientes. La parte superior de la ventana contiene información y controles del servidor de la CA. Para obtener información sobre la detención, el inicio y la desinstalación del servidor de la CA, consulte [Administrar servidor de la CA](#).

Puede seleccionar una solicitud de suscripción de certificados en la lista y luego emitirla (aceptarla), rechazarla o eliminarla. Las acciones disponibles dependen del estado de la solicitud de suscripción de certificados seleccionada.

### Seleccionar todo

Haga clic en **Seleccionar todo** para seleccionar todas las solicitudes de certificados pendientes. Cuando se seleccionan todas las solicitudes de certificados, al hacer clic en **Otorgar** se otorgan todas las solicitudes. Cuando se seleccionan todas las solicitudes de certificados, al hacer clic en **Rechazar** se rechazan todas las solicitudes.

## Otorgar

Haga clic en **Otorgar** para emitir el certificado al cliente que lo solicita.



### Nota

Las ventanas del servidor de la CA no muestran los ID de los certificados que otorgan. En caso en que sea necesario revocar un certificado, debe solicitar el ID del certificado al administrador del cliente, que indique el propósito para el cual se emitió el certificado. El administrador del cliente puede determinar el ID del certificado especificando el comando de Cisco IOS, `sh crypto pki cert`.

## Eliminar

Haga clic en **Eliminar** para eliminar la solicitud de suscripción de certificados en la base de datos.

## Rechazar

Haga clic en **Rechazar** para denegar la solicitud de suscripción de certificados.

## Actualizar

Haga clic en **Actualizar** para actualizar las solicitudes de suscripción de certificados con los últimos cambios.

## Área de solicitudes de suscripción de certificados

El área de solicitudes de suscripción de certificados tiene las siguientes columnas:

**ID de solicitud:** número único asignado a la solicitud de suscripción de certificados.

**Estado:** estado actual de la solicitud de suscripción de certificados. El estado puede ser Pendiente (sin decisión), Otorgado (certificado emitido), Rechazado (solicitud denegada).

**Huella dactilar:** identificador de cliente digital único.

**Nombre del asunto:** nombre del asunto en la solicitud de suscripción.

El siguiente es un ejemplo de una solicitud de suscripción:

ID de solicitud	Estado	Huella dactilar	Nombre del asunto
1	pendiente	serialNumber=FTX0850Z0GT +hostname=c1841.snrsprp.com	B398385E6BB6604E9E98B8FD BBB5E8BA

## Revocar certificado

Haga clic en **Revocar certificado** para mostrar un cuadro de diálogo que le permite especificar el ID del certificado que desea revocar.



### Nota

El ID del certificado no siempre coincide con el ID de la solicitud que se muestra en las ventanas del servidor de la CA. Puede ser necesario solicitar el ID del certificado que se va a revocar al administrador del cliente, a quien se otorgó el certificado. Para obtener información sobre cómo el administrador del cliente puede determinar el ID del certificado, consulte [Solicitudes pendientes](#).

## Certificados revocados

Esta ventana muestra una lista de los certificados emitidos y revocados. Sólo los certificados emitidos se pueden revocar. La parte superior de la ventana contiene información y controles del servidor de la CA. Para obtener información sobre la detención, el inicio y la desinstalación del servidor de la CA, consulte [Administrar servidor de la CA](#).

La lista de certificados tiene las siguientes columnas:

- **Número de serie del certificado:** número único asignado al certificado. Este número se muestra en formato hexadecimal. Por ejemplo, el número de serie decimal 1 se muestra como 0x01.
- **Fecha de revocación:** hora y fecha en que se revocó el certificado. Si un certificado se revocó a 41 minutos y 20 segundos después de la medianoche del día 6 de febrero de 2007, la fecha de revocación se muestra como 00:41:20 UTC Feb 6 2007.



## Revocar certificado

Haga clic en **Revocar certificado** para mostrar un cuadro de diálogo que le permite especificar el ID del certificado que desea revocar.



### Nota

El ID del certificado no siempre coincide con el ID de la solicitud que se muestra en las ventanas del servidor de la CA. Puede ser necesario solicitar el ID del certificado que se va a revocar al administrador del cliente, a quien se otorgó el certificado. Para obtener información sobre cómo el administrador del cliente puede determinar el ID del certificado, consulte [Solicitudes pendientes](#).

## Revocar certificado

En esta ventana puede revocar certificados otorgados por este servidor de la CA.

### ID del certificado

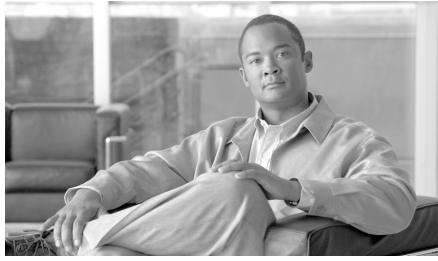
Especifique el ID del certificado que está revocando.



### Nota

El ID del certificado no siempre coincide con el ID de la solicitud que se muestra en las ventanas del servidor de la CA. Puede ser necesario solicitar el ID del certificado que se va a revocar al administrador del cliente, a quien se otorgó el certificado. Para obtener información sobre cómo el administrador del cliente puede determinar el ID del certificado, consulte [Solicitudes pendientes](#).





# CAPÍTULO 19

## VPN con SSL de Cisco IOS

---

VPN con SSL de Cisco IOS proporciona conectividad de acceso remoto Secure Socket Layer (SSL) VPN desde prácticamente cualquier ubicación que disponga de conexión a Internet con sólo un explorador Web y su cifrado SSL nativo. Esto permite a las empresas ampliar sus redes empresariales seguras a cualquier usuario autorizado ofreciendo conectividad de acceso remoto a los recursos corporativos desde cualquier equipo con acceso a Internet.

VPN con SSL de Cisco IOS también permite el acceso desde máquinas que no pertenecen a la empresa, incluidos equipos domésticos, cabinas de Internet y puntos de acceso inalámbrico, en los que la gestión y la implementación del software cliente VPN necesario para las conexiones VPN IPsec no son tarea sencilla para el departamento de TI.

Existen tres modos de acceso VPN SSL: Sin cliente, Cliente ligero y Cliente de túnel completo. Cisco SDM admite los tres modos que se describen a continuación:

- **Sin cliente SSL VPN:** el modo Sin cliente (sin software en estaciones cliente) ofrece acceso seguro a los recursos privados de la red y proporciona acceso al contenido Web. Este modo resulta útil para acceder a la mayoría del contenido que se prevé que se utilizará en un explorador Web como, por ejemplo, acceso a la intranet y a las herramientas en línea que utilicen una interfaz Web.

- **Cliente ligero SSL VPN** (subprograma Java con mapeo de puertos): el modo Cliente ligero amplía la capacidad de las funciones criptográficas del explorador Web para permitir el acceso remoto a aplicaciones basadas en TCP como, por ejemplo, POP3, SMTP, IMAP, Telnet y SSH.
- **Cliente de túnel completo SSL VPN**: el modo Cliente de túnel completo proporciona soporte extendido de aplicaciones mediante el software cliente SSL VPN descargado dinámicamente para Cisco IOS SSL VPN. Con el Cliente de túnel completo para VPN con SSL de Cisco IOS, Cisco proporciona un cliente de arquitectura de túneles SSL VPN ligero, configurado centralmente y de fácil soporte que permite el acceso de conectividad de nivel de red a prácticamente cualquier aplicación.

[Contextos, gateways y políticas VPN con SSL de Cisco IOS](#) describe el modo en el que los componentes de una configuración de VPN con SSL de Cisco IOS funcionan conjuntamente.

Haga clic en [Enlaces de VPN con SSL de Cisco IOS en Cisco.com](#) para ver enlaces a documentos de VPN con SSL de Cisco IOS.

## Enlaces de VPN con SSL de Cisco IOS en Cisco.com

En este tema de ayuda se enumeran los enlaces actuales que proporcionan la información más útil sobre VPN con SSL de Cisco IOS.

El enlace siguiente ofrece acceso a documentos que describen VPN con SSL de Cisco IOS. Vuelva a este enlace de vez en cuando para obtener la información más reciente.

[www.cisco.com/go/iosSSLVPN](http://www.cisco.com/go/iosSSLVPN)

En el enlace siguiente se describe cómo configurar un servidor AAA con el protocolo RADIUS para VPN con SSL de Cisco IOS.

[http://www.cisco.com/en/US/products/ps6441/products\\_feature\\_guide09186a00805eeaea.html#wp1396461](http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00805eeaea.html#wp1396461)

# Crear SSL VPN

Es posible utilizar asistentes de VPN con SSL de Cisco IOS para crear un nuevo VPN con SSL de Cisco IOS o para añadir nuevas políticas o funciones a un VPN con SSL de Cisco IOS existente.

Haga clic en [VPN con SSL de Cisco IOS](#) para ver los aspectos generales de las funciones que admite Cisco SDM. En [Contextos, gateways y políticas VPN con SSL de Cisco IOS](#) se describe el modo en el que los componentes de una configuración de VPN con SSL de Cisco IOS funcionan conjuntamente.

Haga clic en [Enlaces de VPN con SSL de Cisco IOS en Cisco.com](#) para ver enlaces a documentos de VPN con SSL de Cisco IOS.

## Tareas previas

Para poder iniciar una configuración de Cisco IOS SSL VPN, es necesario que AAA y los certificados se hayan configurado en el router. Si falta alguna de estas configuraciones, aparecerá una notificación en esta área de la ventana y también un enlace que le permitirá completar la configuración que falta. Cuando se hayan realizado todas las configuraciones previas requeridas, será posible volver a esta ventana e iniciar la configuración de VPN con SSL de Cisco IOS.

Cisco SDM activa AAA sin la intervención del usuario. Cisco SDM puede ayudarle a generar claves públicas y privadas para el router y a suscribirlas con una autoridad certificadora para obtener certificados digitales. Consulte el apartado [Infraestructura de clave pública](#) para obtener más información. Como opción alternativa, puede configurar un certificado con firma automática permanente que no requiere la aprobación de una CA. Para obtener información más detallada sobre la función de certificado con firma automática permanente, consulte el enlace siguiente:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products\\_feature\\_guide09186a008040adf0.html#wp1066623](http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008040adf0.html#wp1066623)

Asegúrese de que en el campo del enlace del explorador aparece la URL completa.

## Crear una nueva SSL VPN

Seleccione esta opción para crear una nueva configuración de Cisco IOS SSL VPN. Este asistente permite la creación de Cisco IOS SSL VPN con una política de usuario y una cantidad limitada de funciones. Tras finalizar el asistente, se pueden utilizar otros asistentes para configurar funciones y políticas adicionales de Cisco IOS SSL VPN. Es posible volver a este asistente para crear configuraciones adicionales de Cisco IOS SSL VPN.

Si utiliza Cisco SDM para crear la primera configuración de Cisco IOS SSL VPN en un router, creará un contexto de Cisco IOS SSL VPN, configurará un gateway y creará una política de grupo. Cuando haya finalizado el asistente, haga clic en **Editar SSL VPN** para ver la configuración y familiarizarse con el modo en el que los componentes de Cisco IOS SSL VPN funcionan conjuntamente. Si desea obtener información que le ayude a comprender lo que ve, haga clic en [Contextos, gateways y políticas VPN con SSL de Cisco IOS](#).

## Agregar una nueva política a una SSL VPN existente para un nuevo grupo de usuarios

Seleccione esta opción si desea añadir una nueva política a una configuración de Cisco IOS SSL VPN existente para un nuevo grupo de usuarios. Gracias a la existencia de varias políticas podrá definir conjuntos distintos de funciones para diferentes grupos de usuarios. Por ejemplo, se puede definir una política para ingeniería y otra distinta para ventas.

## Configurar funciones avanzadas para una SSL VPN existente

Seleccione esta opción si desea configurar funciones adicionales para una política de Cisco IOS SSL VPN existente. Es necesario especificar el contexto en el que se configura la política.

## Botón Iniciar la tarea seleccionada

Haga clic para iniciar la configuración seleccionada. Si no se puede completar la tarea elegida, aparecerá un mensaje de advertencia. Si es necesario realizar algún requerimiento previo, se le informará de la tarea de la que se trata y de cómo llevarla a cabo.

## Certificado con firma automática permanente

En este cuadro de diálogo se puede especificar la información para un certificado con firma automática permanente. Con la información proporcionada, el servidor HTTPS generará un certificado que se utilizará en el protocolo de intercambio SSL. Los certificados con firma automática permanente permanecen en la configuración incluso en el caso de que se vuelva a cargar el router, y se presentan durante el protocolo de intercambio SSL. Los nuevos usuarios deben aceptar manualmente estos certificados, pero los usuarios que ya lo hayan hecho previamente no deberán volverlos a aceptar cuando se realice una recarga del router.

Para obtener más información sobre la función de certificado con firma automática permanente, consulte la información de este enlace:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products\\_feature\\_guide09186a008040adf0.html#wp1066623](http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008040adf0.html#wp1066623)

Asegúrese de que en el campo del enlace del explorador aparece la URL completa.

### Nombre

Cisco SDM coloca el nombre Router\_Certificate en este campo. Es posible cambiar el nombre si se desea. Este nombre corresponde al del asunto que se utilizaría en una solicitud de certificado.

### Longitud de la clave RSA

Cisco SDM coloca el valor 512 en este campo. Si se desea, se puede especificar una clave más larga como, por ejemplo, 1024. La longitud de la clave debe ser un múltiplo de 64.

### Asunto

Escriba la información para los campos en el área Asunto. Para obtener más información acerca de estos campos, consulte la información de la sección [Otros atributos de asunto](#).

### Botón Generar

Tras proporcionar la información en esta ventana, haga clic en **Generar** para que el router cree el certificado con firma automática permanente.

## Bienvenido

En la pantalla de bienvenida de cada asistente se enumeran las tareas que se pueden realizar con ese asistente. Utilice esta información para asegurarse de que está utilizando el asistente adecuado. En caso contrario, haga clic en **Cancelar** para volver a la ventana Crear SSL VPN y seleccione el asistente que desea utilizar.

Cuando haya escrito la información que le solicita el asistente, la ventana Resumen mostrará la información introducida. Si desea ver los comandos del CLI de Cisco IOS que se envían al router, haga clic en **Cancelar** para salir del asistente, vaya a **Editar > Preferencias** y seleccione **Obtener una vista previa de los comandos antes de enviarlos al router**. A continuación, reinicie el asistente y escriba la información que le sea solicitada. Al enviar la configuración al router, aparecerá una ventana adicional en la que podrá ver los comandos del CLI de Cisco IOS que está enviando.

## Gateways SSL VPN

El gateway de Cisco IOS SSL VPN proporciona la dirección IP y el certificado digital para todo [Contexto SSL VPN](#) que lo utiliza. En esta ventana se puede introducir la información para un gateway, así como la información que permitirá a los usuarios acceder a un portal.

### Campos Dirección IP y Nombre

Utilice estos campos para crear la URL que utilizarán los usuarios para acceder al portal de Cisco IOS SSL VPN. La lista de direcciones IP contiene las direcciones IP de todas las interfaces del router configuradas y de todos los gateways de Cisco IOS SSL VPN existentes. Se puede utilizar la dirección IP de una interfaz del router si se trata de una dirección pública a la que los clientes que se desea tienen acceso, o bien se puede utilizar otra dirección IP pública a la que los clientes tienen acceso.

Si se utiliza una dirección IP que aún no se ha utilizado para un gateway, se crea un nuevo gateway.



## Permitir acceso a Cisco SDM a través de la casilla de verificación *Dirección IP*

Seleccione esta casilla si desea seguir accediendo a Cisco SDM desde esta dirección IP. Esta casilla de verificación aparece si se ha especificado la dirección IP que se está utilizando actualmente para acceder a Cisco SDM.



### Nota

Si marca esta casilla de verificación, la URL que debe utilizar para acceder a Cisco SDM cambiará cuando haya enviado la configuración al router. Revise el área de información en la parte inferior de la ventana para saber cuál URL se debe usar. Cisco SDM coloca un acceso directo a esta URL en el escritorio de su equipo, el cual puede usar para acceder a Cisco SDM en el futuro.

## Certificado digital

Si está creando un nuevo gateway, seleccione el certificado digital que desea que el router presente a los clientes cuando se conecten al gateway. Si selecciona la dirección IP de un gateway existente, el router utilizará el certificado digital configurado para dicho gateway y se desactivará este campo.

## Área de Información

Cuando escriba la información en los campos Dirección IP y Nombre, esta área contendrá la URL que introducirán los usuarios. Es necesario proporcionar esta URL a los usuarios para los que se crea esta Cisco IOS SSL VPN.

Si seleccionó **Permitir Cisco SDM acceso a través de dirección IP**, la URL que debe usar en el futuro para acceder a Cisco SDM se muestra en esta área. Cisco SDM coloca un acceso directo a esta URL en el escritorio de su equipo después de enviar la configuración de VPN con SSL de Cisco IOS al router.

## Autenticación del Usuario

Utilice esta ventana para especificar el modo en el que el router debe realizar la autenticación del usuario. El router puede autenticar los usuarios de Cisco IOS SSL VPN localmente, o bien puede enviar peticiones de autenticación a servidores AAA remotos.

### Botón Servidor AAA externo

Haga clic en este botón si desea que el router utilice un servidor AAA para autenticar los usuarios de Cisco IOS SSL VPN. El router utilizará los servidores AAA enumerados en esta ventana. Si no existen servidores AAA configurados, podrá configurarlos en esta ventana. Para usar esta opción, debe haber al menos un servidor AAA configurado en el router.

### Botón Localmente en este router

Haga clic si desea que el router autentique los usuarios por sí mismo. El router autenticará todos los usuarios que aparezcan en esta ventana. Si no hay usuarios configurados en el router, se pueden añadir usuarios en esta ventana.

### Botón Primero en un servidor AAA externo y, a continuación, localmente en este router

Haga clic si desea que el router realice primero la autenticación utilizando un servidor AAA y, en el caso de que ésta falle, intente después una autenticación local. Si el usuario no se ha configurado ni en un servidor AAA configurado ni localmente en el router, la autenticación de ese usuario fallará.

### Botón Utilizar la lista de métodos para autenticación AAA

Haga clic si desea que el router utilice una lista de métodos para la autenticación. Una lista de métodos contiene los métodos de autenticación que deben utilizarse. El router probará el primer método de autenticación de la lista. Si la autenticación falla, el router probará el siguiente método de la lista y seguirá así hasta que autentique el usuario o hasta que llegue al final de la lista.

### Lista Servidores AAA configurados para este router

Esta lista contiene los servidores AAA que utiliza el router para autenticar usuarios. Si elige la opción de autenticar usuarios con servidores AAA, esta lista deberá contener el nombre o la dirección IP de al menos un servidor. Utilice el botón **Agregar** para añadir la información para un nuevo servidor. Para gestionar las configuraciones de AAA en el router, salga del asistente, haga clic en **Tareas adicionales** y, a continuación, haga clic en el nodo de AAA del árbol Tareas adicionales. Esta lista no aparecerá si se ha seleccionado **Localmente en este router**.

## Crear cuentas de usuario localmente en este router

Escriba en esta lista los usuarios que desea que autentique el router. Utilice los botones **Agregar y Editar** para gestionar los usuarios en el router. La lista no aparecerá si se selecciona **Servidor AAA externo**.

## Configurar sitios Web de la intranet

Configure en esta ventana grupos de sitios Web de la intranet a los que desea que los usuarios tengan acceso. Estos enlaces aparecerán en el portal que verán los usuarios de esta Cisco IOS SSL VPN al iniciar la sesión.

### Columnas Acción y Lista de URL

Si se agrega una política a un contexto de Cisco IOS SSL VPN existente, puede haber listas de direcciones URL en la tabla que aparece. Marque la opción **Seleccionar** si desea utilizar una lista de URL mostrada para la política.

Para crear una nueva lista, haga clic en **Agregar** y especifique la información necesaria en el cuadro de diálogo que aparecerá. Utilice los botones **Editar** y **Eliminar** para cambiar o eliminar las listas de direcciones URL de esta tabla.

## Agregar o editar URL

Agregue o edite la información de un enlace de Cisco IOS SSL VPN en esta ventana.

### Etiqueta

La etiqueta se muestra en el portal que aparece cuando los usuarios inician sesión en Cisco IOS SSL VPN. Por ejemplo, se puede utilizar la etiqueta Calendario de pagos para un enlace al calendario en el que aparecen los días de vacaciones pagados y los días de pago.

### Enlace de URL

Especifique o edite la URL al sitio Web de la intranet corporativa que desea que puedan visitar los usuarios.

## Personalizar el portal SSL VPN

Los ajustes realizados en este portal determinan el aspecto que tendrá el portal. Se puede seleccionar uno de los temas predefinidos de la lista y obtener una vista previa del portal para comprobar el aspecto que tendría si se utilizara ese tema.

### Tema

Seleccione el nombre de un tema predefinido.

### Vista previa

En esta área se muestra el aspecto del portal con el tema seleccionado. Se puede obtener la vista previa de varios temas para que el usuario elija el que desea utilizar.

## Configuración de paso por SSL VPN

Para que los usuarios puedan conectarse a la intranet, se deben añadir entradas de control de acceso (ACE) al firewall y a las configuraciones del control de acceso a la red (NAC) para permitir que el tráfico SSL pueda llegar a la intranet. La configuración de las ACE puede realizarla Cisco SDM, o bien puede optar por realizarla usted mismo yendo a **Firewall y ACL > Editar Política de firewall/ACL**, donde podrá realizar las modificaciones necesarias.

Si está trabajando en el asistente para Cisco IOS SSL VPN, haga clic en **Permitir que SSL VPN funcione con NAC y firewall** si desea que Cisco SDM configure estas ACE. Haga clic en **Ver detalles** para ver las ACE que creará Cisco SDM. Las entradas que agrega Cisco SDM son similares a las del ejemplo siguiente:

```
permit tcp any host 172.16.5.5 eq 443
```

Si está editando un contexto de Cisco IOS SSL VPN, Cisco SDM mostrará la interfaz afectada y la ACL que se le aplica. Haga clic en **Modificar** para que Cisco SDM pueda agregar entradas a la ACL para permitir el paso del tráfico SSL por el firewall. Haga clic en **Detalles** para ver la entrada que agrega Cisco SDM. La entrada será similar a la mostrada anteriormente.

## Política de usuarios

En esta ventana se puede seleccionar una Cisco IOS SSL VPN existente y agregarle una nueva política. Por ejemplo, supongamos que se ha creado una Cisco IOS SSL VPN denominada Corporativa y se desea definir un acceso a la intranet para un nuevo grupo de usuarios denominado Ingeniería.

### Seleccionar SSL VPN existente

Seleccione la Cisco IOS SSL VPN para la que desea crear un nuevo grupo de usuarios. Las políticas ya configuradas para esa Cisco IOS SSL VPN se mostrarán en un cuadro debajo de la lista. Se puede hacer clic en cualquiera de ellas para ver sus detalles. Consulte el apartado [Detalles de la política de grupo de SSL VPN: Policyname](#) para obtener más información.

### Nombre de la nueva política

Especifique el nombre que desea asignar al nuevo grupo de usuarios. En el área inferior a este campo aparecerá una lista con las políticas de grupo que ya existen para esta Cisco IOS SSL VPN.

## Detalles de la política de grupo de SSL VPN: Policyname

En esta ventana se muestran los detalles de una política de Cisco IOS SSL VPN existente.

### Servicios

En esta área aparecen enumerados los servicios para los que se ha configurado esta política como, por ejemplo, manipulación de URL o Cisco Secure Desktop.

### URL mostradas a los usuarios

En esta área se enumeran las URL de la intranet mostradas a los usuarios regidos por esta política.

## Servidores mostrados a los usuarios

En esta área se muestran las direcciones IP de los servidores con mapeo de puertos que debe utilizar esta política según se indica en su configuración.

## Servidores WINS

En esta área se muestran las direcciones IP de los servidores WINS que debe utilizar esta política según se indica en su configuración.

# Seleccionar el grupo de usuarios de SSL VPN

Seleccione en esta ventana la Cisco IOS SSL VPN y el grupo de usuarios asociado para el que desea configurar servicios avanzados.

## SSL VPN

Seleccione la Cisco IOS SSL VPN a la que está asociado el grupo de usuarios desde esta lista.

## Grupo de usuarios

Seleccione el grupo de usuarios para el que desea configurar funciones avanzadas. El contenido de esta lista se basa en la Cisco IOS SSL VPN seleccionada.

# Seleccionar funciones avanzadas

Seleccione en esta ventana las funciones que desea configurar. El asistente mostrará ventanas que le permitirán configurar las funciones seleccionadas.

Por ejemplo, al hacer clic en Cliente ligero (mapeo de puertos), Cisco Secure Desktop y Sistema de archivos de Internet común (CIFS), el asistente mostrará ventanas de configuración para estas funciones.

Debe seleccionar al menos una función para configurarla.

## Cliente ligero (mapeo de puertos)

En ocasiones, las estaciones de trabajo remotas deben ejecutar aplicaciones cliente para poder comunicarse con los servidores de la intranet. Por ejemplo, los servidores IMAP (Internet Mail Access Protocol) o SMTP (Simple Mail Transfer Protocol) pueden requerir que las estaciones de trabajo ejecuten aplicaciones cliente para poder enviar y recibir correo electrónico. La función Cliente ligero, también conocida como mapeo de puertos, permite que se descargue un pequeño subprograma junto con el portal para que la estación de trabajo remota pueda comunicarse con el servidor de la intranet.

Esta ventana contiene una lista de los servidores y los números de puerto configurados para la intranet. Utilice el botón **Agregar** para añadir el número de puerto y la dirección IP de un servidor. Utilice los botones **Editar** y **Eliminar** para realizar modificaciones en la información de la lista y para eliminar la información de un servidor.

La lista creada aparecerá en el portal que ven los clientes cuando inician sesión.

### Agregar o editar un servidor

Agregue o edite información de un servidor en esta ventana.

#### Dirección IP del servidor

Especifique la dirección IP o el nombre de host del servidor.

#### Puerto del servidor en el que escucha el servicio

Especifique el puerto por el que escucha el servidor para este servicio. Se puede tratar de un número de puerto estándar para el servicio como, por ejemplo, el número de puerto 23 para Telnet, o bien se puede tratar de un número de puerto no estándar para el que se haya creado una Asignación de puerto a aplicación (PAM). Por ejemplo, si se ha cambiado el número de puerto de Telnet en el servidor por 2323 y se ha creado una entrada PAM para ese puerto en el servidor, se deberá especificar 2323 en esta ventana.

## Puerto en PC cliente

En este campo, Cisco SDM introduce un número empezando por 3000. Cada vez que se añade una entrada, Cisco SDM incrementa el número en 1. Utilice las entradas que ha colocado Cisco SDM en este campo.

## Descripción

Escriba una descripción para la entrada. Por ejemplo, si se está añadiendo una entrada que permite a los usuarios realizar una conexión mediante Telnet con el servidor en 10.10.11.2, se puede escribir “Telnet a 10.10.11.2”. La descripción aparecerá en el portal.

## Más información

Haga clic en este enlace para obtener más información. Puede ver la información ahora haciendo clic en [Más detalles acerca de los servidores de mapeo de puertos](#).

## Más detalles acerca de los servidores de mapeo de puertos

El mapeo de puertos permite a un usuario remoto de Cisco IOS SSL VPN conectarse con puertos estáticos de servidores con direcciones IP privadas en la intranet corporativa. Por ejemplo, es posible configurar el mapeo de puertos en un router de modo que se ofrezca a los usuarios remotos acceso Telnet a un servidor de la intranet corporativa. Para configurar el mapeo de puertos, se requiere la información siguiente:

- La dirección IP del servidor.
- El número de puerto estático del servidor.
- El número de puerto remoto del PC cliente. En el cuadro de diálogo, Cisco SDM muestra un número de puerto de uso seguro.

Por ejemplo, para que los usuarios puedan utilizar Telnet para conectarse a un servidor con la dirección IP 10.0.0.100 (puerto 23), se debería crear una entrada de asignación de puerto con la información siguiente:

Dirección IP del servidor: 10.0.0.100

Puerto del servidor al que se está conectando el usuario: 23

Puerto en el PC cliente: valor suministrado por Cisco SDM. 3001 para este ejemplo.



Descripción: acceso Telnet de SSL VPN al servidor-a. En el portal aparecerá esta descripción.

Cuando el explorador del cliente se conecta con el router del gateway, se descarga un subprograma del portal en el PC cliente. Este subprograma contiene el número de puerto estático y la dirección IP del servidor, así como el número de puerto que va a utilizar el PC cliente. El subprograma realiza las acciones siguientes:

- Crea una asignación en el PC cliente que asigna el tráfico para el puerto 23 en 10.0.0.100 a la dirección IP de retrobucle del PC 127.0.0.1, puerto 3001.
- Escucha por el puerto 3001, dirección IP 127.0.0.1

Cuando el usuario ejecuta una aplicación que se conecta con el puerto 23 en 10.0.0.100, la solicitud se envía a 127.0.0.1, puerto 3001. El subprograma del portal que escucha ese puerto y la dirección IP reciben esta petición y la envían al gateway a través del túnel de Cisco IOS SSL VPN. El router del gateway la reenvía al servidor a 10.0.0.100 y devuelve de nuevo el tráfico de vuelta al PC.

## Túnel completo

Los clientes de túnel completo deben descargar el software de túnel completo y obtener una dirección IP del router. Utilice esta ventana para configurar el conjunto de direcciones IP que obtendrán los clientes de túnel completo cuando inicien sesión y para especificar la ubicación del paquete de instalación de túnel completo.



### Nota

---

Si el paquete de instalación del software aún no está instalado, debe haber suficiente memoria en la memoria flash del router para que Cisco SDM pueda instalarlo tras la finalización de este asistente.

---

### Casilla de verificación Activar túnel completo

Marque esta casilla para permitir que el router descargue el software de cliente de túnel completo en el PC del usuario y para activar los demás campos de esta ventana.

## Conjunto de direcciones IP

Especifique el conjunto de direcciones IP que obtendrán los clientes de túnel completo. Puede especificar el nombre de un conjunto existente en el campo, o bien puede hacer clic en el botón que encontrará a la derecha del campo y seleccionar **Seleccionar un conjunto IP existente** para examinar la lista de conjuntos. Seleccione **Crear un conjunto nuevo** y rellene el cuadro de diálogo que aparecerá para crear un conjunto nuevo. El conjunto de direcciones seleccionado o creado debe contener direcciones en la intranet corporativa.

## Casilla de verificación Mantener instalado el software de cliente de túnel completo en el PC cliente

Marque esta casilla si desea que el software Túnel completo permanezca en el PC del cliente cuando éste finalice la sesión. Si no marca esta casilla de verificación, los clientes deberán descargar el software cada vez que establezcan comunicación con el gateway.

## Casilla de verificación Instalar el cliente de túnel completo

Marque esta casilla si desea instalar el software de cliente de túnel completo en este momento. También puede instalar el software cliente al editar esta Cisco IOS SSL VPN.

El software de cliente de túnel completo debe estar instalado en el router para que los clientes puedan descargarlo para establecer una conectividad de túnel completo. Si se ha instalado el software Túnel completo con Cisco SDM, la ruta al software aparecerá automáticamente en el campo Ubicación, tal como se muestra en el [Ejemplo 19-1](#).

### *Ejemplo 19-1 Paquete Túnel completo instalado en el router*

```
flash:sslclient-win-1.0.2.127.pkg
```

En el [Ejemplo 19-1](#), el paquete de instalación Túnel completo está cargado en la memoria flash del router. Si el dispositivo principal del router es un disco o una ranura, la ruta que aparecerá empezará por `diskn` o `slotn`.

Si este campo está vacío, deberá buscar el paquete de instalación para que Cisco SDM pueda cargarlo en el dispositivo principal del router, o bien descargar el paquete de instalación del software en Cisco.com haciendo clic en el enlace Descargue el paquete de instalación más reciente de... que encontrará en la parte inferior de la ventana. Este enlace le llevará a la página Web siguiente:

<http://www.cisco.com/cgi-bin/tablebuild.pl/sslvpnclient>

**Nota**

Es posible que necesite un nombre de usuario y una contraseña de CCO para poder obtener el software en un sitio de descarga de Cisco. Para obtener estas credenciales, haga clic en **Registro** que encontrará en la parte superior de cualquier página Web de Cisco.com y proporcione la información solicitada. Recibirá por correo electrónico el ID de usuario y la contraseña.

Haga clic en [Buscar el paquete de instalación de Cisco SDM](#) para obtener más información acerca de cómo buscar el paquete de instalación del software Túnel completo y proporcionar una ruta para que Cisco SDM pueda encontrarlo.

### Botón Opciones avanzadas

Haga clic en este botón para configurar las opciones avanzadas como, por ejemplo, la división de la arquitectura de túneles, la división de DNS y los ajustes de Microsoft Internet Explorer.

## Buscar el paquete de instalación de Cisco SDM

Utilice el procedimiento siguiente para buscar paquetes de instalación de software para Cisco SDM, de modo que el sistema pueda utilizar esta ubicación en la configuración de VPN con SSL de Cisco IOS o, si fuera necesario, cargar el software en el router.

**Nota**

Es posible que necesite un nombre de usuario y una contraseña de CCO para poder obtener el software en un sitio de descarga de Cisco. Para obtener estas credenciales, haga clic en **Registro** que encontrará en la parte superior de cualquier página Web de Cisco.com y proporcione la información solicitada. Recibirá por correo electrónico el ID de usuario y la contraseña.

- Paso 1** Observe el campo **Ubicación**. Si la ruta al paquete de instalación se encuentra en este campo, no necesitará emprender ninguna otra acción. Cisco SDM configurará el router para que descargue el software desde esta ubicación. El [Ejemplo 19-2](#) muestra una ruta a un paquete de instalación de software.

**Ejemplo 19-2 Paquete Túnel completo instalado en el router**

```
flash:sslclient-win-1.0.2.127.pkg
```

- Paso 2** Si el campo Ubicación está vacío, haga clic en el botón ... que encontrará a la derecha del campo para especificar la ubicación del software.
- Paso 3** Si el software está instalado en el router, seleccione **Sistema de archivos del router** y, a continuación, busque el archivo.
- Si el software se encuentra en su PC; seleccione **Mi PC** y busque el archivo.
- Cisco SDM colocará el sistema de archivos del router o la ruta del PC especificada en el campo Ubicación.
- Paso 4** Si el software no se encuentra en el router ni en el PC, deberá descargarlo en el PC y, a continuación, especificar la ruta al archivo en este campo.
- Haga clic en el enlace [Descargue el paquete de instalación más reciente de...](#) de la ventana. Se conectará a la página de descarga del software que desea.
  - Es posible que en la página Web que aparezca haya paquetes de software disponibles para plataformas de Cisco IOS y otras plataformas. Haga doble clic en la versión más reciente del software que desea descargar para plataformas de Cisco IOS y especifique el nombre de usuario y la contraseña de CCO cuando le sea solicitado.
  - Descargue el paquete en el PC.
  - En el asistente para Cisco IOS SSL VPN, haga clic en el botón ... que encontrará a la derecha del campo Ubicación, seleccione **Mi PC** en la ventana Seleccionar ubicación (Select Location) que aparecerá y navegue hasta el directorio en el que ha colocado el archivo.
  - Seleccione el archivo del paquete de instalación y haga clic en **Aceptar** en la ventana Seleccionar ubicación. Cisco SDM colocará esa ruta en el campo Ubicación. El ejemplo siguiente muestra un paquete de instalación ubicado en el escritorio del PC.

### *Ejemplo 19-3 Paquete Túnel completo instalado en el router*

```
C:\Documents and Settings\username\Desktop\sslclient-win-1.1.0.154.pkg
```

Cisco SDM instalará el software en el router desde el directorio del PC especificado al enviar la configuración al router cuando haga clic en **Finalizar**.

---

## Activar Cisco Secure Desktop

El router puede instalar Cisco Secure Desktop en el PC del usuario cuando éste se conecta a la Cisco IOS SSL VPN. Las transacciones de Internet pueden dejar cookies, archivos del historial del explorador, documentos adjuntos de correo electrónico y otros archivos en el PC una vez finalizada la conexión. Cisco Secure Desktop crea una partición segura en el escritorio y utiliza un algoritmo del Departamento de Defensa de los EE.UU. para eliminar los archivos cuando finaliza la sesión.

### Instale Cisco Secure Desktop

Los clientes deben descargar el paquete de instalación del software Cisco Secure Desktop desde el router. Si este software se ha instalado con Cisco SDM, la ruta al mismo aparecerá automáticamente en el campo **Ubicación**, tal como se muestra en el [Ejemplo 19-4](#).

### *Ejemplo 19-4 Paquete Cisco Secure Desktop instalado en el router*

```
flash:/securedesktop-ios-3.1.0.29-k9.pkg
```

En el [Ejemplo 19-4](#), el paquete de instalación de Cisco Secure Desktop está cargado en la memoria flash del router. Si el dispositivo principal del router es un disco o una ranura, la ruta que aparecerá empezará por `diskn O slotn`.

Si este campo está vacío, deberá buscar el paquete de instalación para que Cisco SDM pueda cargarlo en el dispositivo principal del router, o bien descargar el paquete de instalación del software en Cisco.com haciendo clic en el enlace **Descargue el paquete de instalación más reciente de...** que encontrará en la parte inferior de la ventana. Este enlace conduce a la siguiente página Web:

<http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop>



#### Nota

Es posible que necesite un nombre de usuario y una contraseña de CCO para poder obtener el software de un sitio de descarga de Cisco. Para obtener estas credenciales, haga clic en **Registro** que encontrará en la parte superior de cualquier página Web de Cisco.com y proporcione la información solicitada. Recibirá por correo electrónico el ID de usuario y la contraseña.

Haga clic en [Buscar el paquete de instalación de Cisco SDM](#) para obtener más información acerca de cómo buscar el paquete de instalación del software Cisco Secure Desktop y especificar una ruta que pueda utilizar Cisco SDM.

## Sistema de archivos de Internet común

Sistema de archivos de Internet común (CIFS) permite a los clientes explorar, acceder y crear archivos de forma remota en servidores de archivos basados en Microsoft Windows mediante una interfaz de explorador Web.

### Servidores WINS

Los servidores Microsoft Windows Internet Naming Service (WINS) mantienen la base de datos que asigna direcciones IP cliente a sus correspondientes nombres de NetBIOS. Especifique en este cuadro las direcciones IP de los servidores WINS de su red. Utilice un punto y coma (;) para separar las direcciones.

Por ejemplo, para introducir las direcciones IP 10.0.0.18 y 10.10.10.2, escriba 10.0.0.18;10.10.10.2 en este cuadro.

### Permisos

Especifique los permisos que desea otorgar a los usuarios.

## Activar Citrix sin cliente

Citrix sin cliente permite a los usuarios ejecutar aplicaciones como, por ejemplo, Microsoft Word o Excel en servidores remotos del mismo modo en el que lo harían localmente, sin necesidad de que el cliente disponga del software en el PC. El software de Citrix debe estar instalado en uno o varios de los servidores de una red a la que el router tenga acceso.

### Servidor Citrix

Para crear una nueva lista, haga clic en **Agregar** y especifique la información necesaria en el cuadro de diálogo que aparecerá. Utilice las teclas **Editar** y **Eliminar** para cambiar o eliminar listas de URL de esta tabla.

## Resumen

Esta ventana muestra un resumen de la configuración de Cisco IOS SSL VPN que ha creado. Haga clic en **Finalizar** para enviar la configuración al router o haga clic en **Atrás** para volver a la ventana del asistente a realizar cambios.

Para ver los comandos del CLI que se envían al router, vaya a **Editar > Preferencias** y marque la opción **Obtenga una vista previa de los comandos antes de enviarlos al router**.

## Editar SSL VPN

La ventana Editar SSL VPN permite modificar o crear configuraciones de VPN con SSL de Cisco IOS. En la parte superior de la ficha aparece una lista de los contextos VPN con SSL de Cisco IOS configurados. En la parte inferior se muestran los detalles de ese contexto.

Haga clic en [VPN con SSL de Cisco IOS](#) para obtener una visión general de las funciones de VPN con SSL de Cisco IOS admitidas por Cisco SDM.

Haga clic en [Enlaces de VPN con SSL de Cisco IOS en Cisco.com](#) para ver enlaces a documentos de VPN con SSL de Cisco IOS.

Haga clic en [Contextos, gateways y políticas VPN con SSL de Cisco IOS](#) para obtener una descripción del modo en el que los componentes de una configuración de VPN con SSL de Cisco IOS funcionan conjuntamente.

## Contextos de SSL VPN

En esta área se muestran los contextos de VPN con SSL de Cisco IOS configurados en el router. Haga clic en un contexto de esta área para ver su información detallada en la parte inferior de la ventana. Para añadir un nuevo contexto, haga clic en **Agregar** y especifique la información en el cuadro de diálogo que aparecerá. Si desea editar un contexto, selecciónelo y haga clic en **Editar**. Para eliminar un contexto y sus políticas de grupo asociadas, selecciónelo y haga clic en **Eliminar**.

Es posible activar un contexto que no esté en funcionamiento seleccionándolo y haciendo clic en **Activar**. Para que un contexto deje de funcionar, selecciónelo y haga clic en **Desactivar**.

Se mostrará la información siguiente para cada contexto.

### Nombre

El nombre del contexto de VPN con SSL de Cisco IOS. Si el contexto se ha creado en el asistente para VPN con SSL de Cisco IOS, el nombre será la cadena especificada en la ventana Dirección IP y nombre.

### Gateway

El gateway que utiliza el contexto contiene la dirección IP y el certificado digital que utilizará el contexto de VPN con SSL de Cisco IOS.

### Dominio

Si se ha configurado un dominio para el contexto, se mostrará en esta columna. Si se ha configurado un dominio, los usuarios deberán indicarlo en el explorador Web para poder acceder al portal.

### Estado

Contiene iconos para una identificación rápida del estado.

### Estado administrativo

Descripción textual del estado.

- En servicio: el contexto está en funcionamiento. Los usuarios especificados en las políticas configuradas del contexto podrán acceder a su portal de VPN con SSL de Cisco IOS.



- Fuera de servicio: el contexto no está en funcionamiento. Los usuarios especificados en las políticas configuradas del contexto no podrán acceder a su portal de VPN con SSL de Cisco IOS.

### Pantalla de ejemplo

En la tabla siguiente se muestra una pantalla de ejemplo de contextos de VPN con SSL de Cisco IOS.

Nombre	Gateway	Dominio	Estado	Estado administrativo
WorldTravel	Gateway1	wtravel.net		En servicio
A+Insurance	Gateway2	aplus.com		Fuera de servicio

### Detalles del contexto SSL VPN: *Nombre*

En esta área se muestran los detalles del contexto con el *nombre* seleccionado en la parte superior de la ventana. Puede modificar los ajustes visualizados haciendo clic en **Editar** en la parte superior de la ventana.

## Contexto de SSL VPN

Utilice esta ventana para agregar o editar un contexto de VPN con SSL de Cisco IOS.

### Nombre

Especifique el nombre de un contexto nuevo, o bien seleccione el nombre de un contexto existente para editarlo.

### Gateway asociado

Seleccione un gateway existente, o bien haga clic en **Crear gateway** para configurar un nuevo gateway para el contexto. El gateway contiene la dirección IP y el certificado digital utilizados en este contexto. Cada gateway requiere una dirección IP pública exclusiva.

## Dominio

Si dispone de un dominio para este contexto, indíquelo en este campo. Los usuarios de VPN con SSL de Cisco IOS podrán utilizar este nombre de dominio en lugar de una dirección IP para acceder al portal. Por ejemplo, miempresa.com.

## Lista de autenticación

Seleccione la lista de métodos AAA que desea utilizar para autenticar usuarios para este contexto.

## Dominio de autenticación

Indique el nombre del dominio que debe anexarse al nombre de usuario antes de enviarlo para su autenticación. Este dominio debe coincidir con el utilizado en el servidor AAA en los usuarios autenticados para este contexto.

## Casilla de verificación Activar contexto

Marque esta casilla si desea que el contexto se active una vez configurado. Si lo activa aquí, no necesitará volver a esta ventana para desactivarlo. Es posible activar y desactivar contextos individuales en la ficha Editar SSL VPN.

## Número máximo de usuarios

Especifique el número máximo de usuarios que pueden utilizar simultáneamente este contexto.

## Nombre de VRF

Especifique el nombre de enrutamiento y redireccionamiento de VPN (VRF) para este contexto. Este nombre de VRF ya debe haberse configurado en el router.

## Política de grupo por defecto

Seleccione la política que desea utilizar como política de grupo por defecto. La política de grupo por defecto se utilizará para los usuarios que no se hayan incluido en ninguna política configurada en el servidor AAA.

## Designar interfaces como internas o externas

Una ACL que se aplica a una interfaz en la cual se configura una conexión VPN con SSL de Cisco IOS puede bloquear el tráfico SSL. Cisco SDM puede modificar automáticamente la ACL para permitir este tráfico a través del firewall. Sin embargo, es necesario indicar cuál es la interfaz interna (fiable) y cuál la externa (no fiable) para que Cisco SDM pueda crear la entrada de control de acceso (ACE) que permitirá que el tráfico adecuado pase por el firewall.

Marque la opción **Interna** si la interfaz de la lista es fiable, y **Externa** si se trata de una interfaz no fiable.

## Seleccionar un gateway

Seleccione un gateway existente en esta ventana. Esta ventana proporciona información necesaria para determinar cuál gateway seleccionar. Muestra los nombres y las direcciones IP de todos los gateways, el número de contextos al que cada uno está asociado y si el gateway está activado o no.

## Contexto: Políticas de grupo

En esta ventana se muestran las políticas de grupo configuradas para el contexto de VPN con SSL de Cisco IOS seleccionado. Utilice los botones **Agregar**, **Editar** y **Eliminar** para gestionar estas políticas de grupo.

En esta ventana se muestra el nombre de la política y si se trata de la política de grupo por defecto. La política de grupo por defecto es la política asignada a un usuario que no se ha incluido en ninguna política. Es posible cambiar la política de grupo volviendo a la ventana Contexto y seleccionando otra política como política por defecto.

Haga clic en una política de la lista para ver sus detalles en la parte inferior de la ventana. Para obtener una descripción de estos detalles, haga clic en los enlaces siguientes

[Política de grupo: Ficha General](#)

[Política de grupo: Ficha Sin clientes](#)

[Política de grupo: Ficha Cliente ligero](#)

[Política de grupo: Ficha Cliente VPN con SSL \(túnel completo\)](#)

## Haga clic aquí para obtener más información

Haga clic en el enlace de la ventana para obtener información importante. Para obtener esta información desde esta página de ayuda, haga clic en [Más detalles acerca de las políticas de grupo](#).

## Más detalles acerca de las políticas de grupo

Las políticas de grupo de VPN con SSL de Cisco IOS definen el portal y los enlaces para los usuarios incluidos en dichas políticas. Cuando un usuario remoto entra en la URL de VPN con SSL de Cisco IOS que se le ha proporcionado, el router debe determinar de qué política es miembro el usuario para poder mostrar el portal configurado para esa política. Si en el router sólo se ha configurado una política de VPN con SSL de Cisco IOS, éste podrá autenticar los usuarios localmente o mediante el servidor AAA y, a continuación, mostrar el portal.

Sin embargo, si se han configurado varias políticas, el router deberá confiar en un servidor AAA para determinar qué política debe utilizar cada vez que un usuario remoto intenta iniciar sesión. Si se ha configurado más de una política de grupo de VPN con SSL de Cisco IOS, es necesario configurar al menos un servidor AAA para el router, así como una política en ese servidor para cada grupo de usuarios para el que se ha creado una política de VPN con SSL de Cisco IOS. Los nombres de políticas del servidor AAA deben ser idénticos a los nombres de las políticas de grupo configuradas en el router, y deben configurarse con las credenciales de los usuarios que son miembros del grupo.

Por ejemplo, si un router se ha configurado con autenticación local para Bob Smith y sólo se ha configurado la política de grupo Ventas, sólo se podrá visualizar un portal cuando Bob Smith intente iniciar sesión. Sin embargo, si se han configurado tres políticas de grupo de VPN con SSL de Cisco IOS, Ventas, Campo y Fabricación, el router no podrá determinar por sí mismo a qué grupo de política pertenece Bob Smith. Si se ha configurado un servidor AAA con la información adecuada para estas políticas, el router podrá ponerse en contacto con el servidor y recibir la información de que Bob Smith es un miembro del grupo Ventas. A continuación, el router podrá mostrar el portal correcto para el grupo Ventas.

Para obtener información acerca de cómo configurar el servidor AAA, consulte la sección “Configuring RADIUS Attribute Support for SSL VPN” del documento *SSL VPN Enhancements* en el enlace siguiente:

[http://www.cisco.com/en/US/products/ps6441/products\\_feature\\_guide09186a00805eeaea.html#wp1396461](http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00805eeaea.html#wp1396461)

## Política de grupo: Ficha General

Al crear una nueva política de grupo, se debe especificar información en todos los campos de la ficha General.

### Nombre

Escriba un nombre para la política de grupo como, por ejemplo, Ingeniería, Recursos Humanos o Marketing.

### Límites de tiempo

En Límite de tiempo de inactividad, especifique cuántos segundos puede permanecer inactivo el cliente antes de que se finalice la sesión.

En Límite de tiempo de sesión, especifique la cantidad máxima de segundos de una sesión, independientemente de la actividad que tenga.

### Casilla de verificación Establecer esta política de grupo como la predeterminada para el contexto

Marque esta casilla si desea que ésta sea la política de grupo por defecto. La política de grupo por defecto es la política asignada a un usuario que no está incluido en ninguna política. Si se marca esta casilla de verificación, esta política aparecerá como la política por defecto en la ventana Política de grupo.

## Política de grupo: Ficha Sin clientes

Citrix sin cliente permite a los usuarios ejecutar aplicaciones en servidores remotos del mismo modo en el que lo harían localmente, sin necesidad de que el software cliente esté instalado en los sistemas remotos que utilizan estas aplicaciones. El software de Citrix debe estar instalado en uno o varios de los servidores de una red a la que el router tenga acceso.

Escriba la información en esta ficha si desea que los clientes de VPN con SSL de Cisco IOS puedan utilizar Citrix sin cliente.

## Navegación Web sin cliente

Seleccione una o varias listas de direcciones URL que desea que puedan ver en el portal los usuarios de este grupo. Si desea examinar una lista de direcciones URL, seleccione un nombre de la lista y haga clic en **Ver**. Las URL de la lista especificada aparecerán en el portal.

Si desea restringir el acceso de los usuarios a las URL de la lista e impedir que puedan acceder a otras URL, haga clic en **Ocultar la barra de URL en la página del portal**.

## Activar CIFS

Seleccione esta opción si desea que los miembros del grupo puedan explorar archivos en servidores de MS Windows de la red corporativa. Es necesario especificar la lista de servidores WINS que activará los archivos correspondientes que se mostrarán a estos usuarios. Para verificar el contenido de una lista de servidores WINS, seleccione la lista y haga clic en **Ver**.

Haga clic en **Lectura** para permitir que los miembros del grupo puedan leer los archivos. Haga clic en **Escritura** para permitir que los miembros del grupo puedan realizar cambios en los archivos.

Para que esta función esté disponible, configure al menos una lista de servidores WINS para este contexto de VPN con SSL de Cisco IOS.

## Política de grupo: Ficha Cliente ligero

Realice los ajustes en esta ficha si desea configurar Cliente ligero, también denominado mapeo de puertos, para los miembros de este grupo.

Haga clic en **Activar cliente ligero (mapeo de puertos)** y especifique una lista de mapeo de puertos para activar esta función. Debe haber al menos una lista de mapeo de puertos configurada para el contexto de VPN con SSL de Cisco IOS en el que se ha configurado esta política de grupo. Haga clic en **Ver** para examinar la lista de mapeo de puertos seleccionada.

## Política de grupo: Ficha Cliente VPN con SSL (túnel completo)

Realice los ajustes en esta ficha si desea que los miembros del grupo puedan descargar y utilizar el software de cliente de túnel completo.



### Nota

Es necesario especificar la ubicación del software de cliente de túnel completo. Para ello, haga clic en **Paquetes** en el árbol de SSL VPN, especifique la ubicación del paquete de instalación y, a continuación, haga clic en **Instalar**.

Active las conexiones Túnel completo seleccionando **Activar** en la lista. Si desea que las conexiones Túnel completo sean obligatorias, seleccione **Requerido**. Si se selecciona **Requerido**, la comunicación Sin cliente y Cliente ligero sólo funcionará si el software cliente VPN con SSL de Cisco IOS se ha instalado correctamente en el PC cliente.

### Conjunto de direcciones IP desde la que se asignará una dirección IP a los clientes

El router asignará direcciones IP a los clientes que establezcan una comunicación Túnel completo. Especifique el nombre del conjunto o bien haga clic en el botón ... para crear un nuevo conjunto desde el que el router pueda asignar direcciones.

### Casilla de verificación Mantener instalado el software de cliente de túnel completo en el PC cliente

Marque esta casilla si desea que el software Túnel completo permanezca en el PC del cliente cuando éste finalice la sesión. Si no marca esta casilla de verificación, los clientes deberán descargar el software cada vez que establezcan comunicación con el gateway.

### Campo Renegociar clave

Especifique cuántos segundos deben transcurrir para que el túnel quede fuera de servicio y se pueda negociar una nueva clave SSL y restablecer el túnel.

### ACL para restringir el acceso de los usuarios de este grupo a los recursos corporativos

Es posible seleccionar o crear una lista de acceso (ACL) que especifique los recursos de la red corporativa restringidos para los miembros del grupo.

## La página de inicio de cliente aparecerá al abrir un explorador Web con el software de túnel completo instalado

Escriba la dirección URL a la página de inicio que deben visualizar los clientes Túnel completo de este grupo.

### Límites de tiempo de detección de par inactivo

La Detección de par muerto (DPD) permite al sistema detectar un par que ya no responde. Es posible definir límites de tiempo distintos que el router puede utilizar para detectar clientes y servidores que ya no responden. El intervalo oscila en ambos casos entre 0 y 3600 segundos.

### Botón Configurar servidores DNS y WINS

Haga clic para ver el cuadro de diálogo Servidores DNS y WINS, que permite especificar las direcciones IP de los servidores DNS y WINS en la intranet corporativa que deben utilizar los clientes para acceder a los servicios y hosts de la intranet.

### Botón Configuración de opciones avanzadas de túnel

Haga clic para ver el cuadro de diálogo Opciones avanzadas de túnel, que permite configurar los ajustes del túnel para la división de la arquitectura de túneles y la división de DNS, así como los ajustes del servidor proxy para clientes que utilicen Microsoft Internet Explorer.

## Opciones avanzadas de túnel

La configuración realizada en este cuadro de diálogo permite controlar el tráfico cifrado, especificar los servidores DNS de la intranet corporativa e indicar los ajustes del servidor proxy que deben enviarse a los exploradores cliente.



## División de la arquitectura de túneles

El cifrado de todo el tráfico del túnel puede requerir un uso excesivo de los recursos del sistema. La división de la arquitectura de túneles permite especificar las redes de las que debe cifrarse el tráfico y evitar así que se cifre el tráfico destinado a otras redes. Es posible especificar qué tráfico del túnel se debe cifrar, o bien especificar qué tráfico *no* debe cifrarse y dejar que el router cifre todo el tráfico restante del túnel. Sólo se puede crear una lista; el tráfico incluido y el excluido son excluyentes mutuamente.

Haga clic en **Incluir tráfico** y utilice las teclas **Agregar**, **Editar** y **Eliminar** para crear una lista con las redes de destino cuyo tráfico debe cifrarse. O bien haga clic en **Excluir tráfico** y cree una lista con las redes de destino cuyo tráfico *no* debe cifrarse.

Haga clic en **Excluir LAN locales** para excluir de forma explícita del cifrado el tráfico del cliente destinado a LAN a las que el router está conectado. Si existen impresoras de red en estas LAN, se deberá utilizar esta opción.

[Más detalles acerca de la división de la arquitectura de túneles.](#)

## Dividir DNS

Si desea que los clientes de VPN con SSL de Cisco IOS utilicen el servidor DNS de la red corporativa solamente para resolver dominios específicos, estos dominios pueden escribirse en esta área. Deben ser dominios de la intranet corporativa. Separe las entradas con un punto y coma y no utilice retornos de carro. Aquí tiene una lista de ejemplo de entradas:

suempresa.com;dev-lab.net;extranet.net

Los clientes deben utilizar los servidores DNS proporcionados por sus ISP para resolver todos los demás dominios.

## Configuraciones del Proxy del Explorador

Los ajustes de esta área se envían a los exploradores Microsoft Internet Explorer cliente con conexiones de túnel completo. Estos ajustes no tienen efecto alguno si los clientes utilizan un explorador distinto.

### No utilizar servidor proxy

Haga clic aquí para que los exploradores cliente de VPN con SSL de Cisco IOS no utilicen un servidor proxy.

**Detectar automáticamente la configuración de proxy**

Haga clic aquí si desea que los exploradores cliente de VPN con SSL de Cisco IOS detecten automáticamente la configuración del servidor proxy.

**Omitir la configuración de proxy para las direcciones locales**

Haga clic aquí si desea que los clientes que se conectan a direcciones locales no usen la configuración del servidor proxy.

**Servidor proxy**

Escriba en estos campos la dirección IP del servidor proxy y el número de puerto del servicio que proporciona. Por ejemplo, si el servidor proxy admite peticiones FTP, especifique la dirección IP del servidor proxy y el puerto 21.

**No usar servidor proxy para direcciones que comiencen por**

Si no desea que los clientes utilicen servidores proxy al enviar tráfico a redes o direcciones IP específicas, puede indicarlos aquí. Utilice un punto y coma para separar las entradas. Por ejemplo, si no desea que los clientes utilicen un servidor proxy al conectarse con cualquier servidor de las redes 10.10.0.0 ó 10.11.0.0, deberá escribir 10.10;10.11. Puede indicar tantas redes como desee.

**Servidores DNS y WINS**

Especifique las direcciones IP de los servidores DNS y WINS corporativos que se enviarán a los clientes VPN con SSL de Cisco IOS. Los clientes VPN con SSL de Cisco IOS usarán estos servidores para acceder a los servicios y hosts de la intranet corporativa.

Proporcione direcciones para servidores WINS y DNS principales y secundarios.

## Más detalles acerca de la división de la arquitectura de túneles

Cuando se establece una conexión VPN con SSL de Cisco IOS con un cliente remoto, todo el tráfico que envía y recibe el cliente puede viajar a través del túnel de VPN con SSL de Cisco IOS, incluido el tráfico que no se encuentra en la intranet corporativa. Esto puede perjudicar el rendimiento de la red. La división de la arquitectura de túneles permite especificar el tráfico que desea enviar a través del túnel de VPN con SSL de Cisco IOS y dejar que el resto del tráfico quede desprotegido y sea gestionado por otros routers.

En el área División de la arquitectura de túneles, puede especificar el tráfico para *incluir* en VPN con SSL de Cisco IOS y excluir el tráfico restante por defecto, o puede especificar el tráfico para *excluir* de VPN con SSL de Cisco IOS e incluir el tráfico restante por defecto.

Por ejemplo, supongamos que nuestra organización utiliza las direcciones de red 10.11.55.0 y 10.12.55.0. Agregue estas direcciones de red a la lista Red de destino y haga clic en el botón de opción **Incluir tráfico**. Todo el tráfico restante de Internet como, por ejemplo, el tráfico a Google o Yahoo, se dirigiría a Internet.

O supongamos que es más práctico excluir el tráfico a ciertas redes del túnel de VPN con SSL de Cisco IOS. En este caso, especifique las direcciones a estas redes en la lista Redes de destino y haga clic en el botón de opción **Excluir tráfico**. Todo el tráfico destinado a las redes de la lista Redes de destino se envía mediante routers no seguros y el tráfico restante a través del túnel de VPN con SSL de Cisco IOS.

Si los usuarios disponen de impresoras en LAN locales que desean utilizar mientras están conectados a VPN con SSL de Cisco IOS, en el área División de la arquitectura de túneles se debe hacer clic en **Excluir LAN locales**.



### Nota

Es posible que la lista Red de destino en el área División de la arquitectura de túneles ya contenga direcciones de red. La configuración del tráfico realizada en el área División de la arquitectura de túneles sobrescribirá los ajustes realizados previamente en las redes indicadas.

## Servidores DNS y WINS

Especifique las direcciones IP de los servidores DNS y WINS corporativos que se enviarán a los clientes VPN con SSL de Cisco IOS. Los clientes VPN con SSL de Cisco IOS usarán estos servidores para acceder a los servicios y hosts de la intranet corporativa.

Proporcione direcciones para servidores WINS y DNS principales y secundarios.

## Contexto: Configuración HTML

Los ajustes realizados en esta ventana controlan el aspecto del portal del contexto de VPN con SSL de Cisco IOS seleccionado.

### Seleccionar tema

Es posible especificar el aspecto del portal seleccionando un tema predefinido en lugar de seleccionar manualmente cada color. Al seleccionar un tema, los ajustes del mismo se muestran en los campos asociados con el botón **Personalizar**.

### Botón Personalizar

Haga clic si desea seleccionar cada color utilizado en el portal y especificar un mensaje de inicio de sesión y un título. Si se ha seleccionado un tema predefinido, los valores de ese tema se muestran en los campos de esta sección. Es posible modificar estos valores, y los valores indicados se utilizarán en el portal del contexto seleccionado. Los cambios realizados en esta ventana sólo afectarán el portal que se está creando, y no los valores por defecto del tema.

#### Mensaje de inicio de sesión

Escriba el mensaje de inicio de sesión que desea que vean los clientes cuando sus exploradores visualicen el portal. Por ejemplo:

Bienvenido a la red de *nombre de la empresa*. Finalice la sesión si no es un usuario autorizado.

#### Título

Escriba el título que desea otorgar al portal. Por ejemplo:

Página de conexión a la red de *nombre de la empresa*

### Color de fondo para el título

El valor por defecto del color de fondo que aparece tras el título es #9999CC. Puede cambiar este valor haciendo clic en el botón ... para seleccionar otro color.

### Color de fondo para títulos secundarios

El valor por defecto del color de fondo que aparece tras el título es #9729CC. Puede cambiar este valor haciendo clic en el botón ... para seleccionar otro color, o bien especificando el valor hexadecimal de otro color.

### Color del texto

El valor por defecto del color del texto es blanco. Puede cambiar este valor haciendo clic en la flecha hacia abajo para seleccionar otro color.

### Color del texto secundario

El valor por defecto del color del texto secundario es negro. Puede cambiar este valor haciendo clic en la flecha hacia abajo para seleccionar otro color.

### Archivo de logotipo

Si dispone de un logotipo que desea que aparezca en el portal, haga clic en el botón ... para buscarlo en el PC. Se guardará en la memoria flash del router después de hacer clic en **Aceptar**, y aparecerá en la esquina superior izquierda del portal.

## Botón Vista previa

Haga clic para obtener una vista previa del portal con el aspecto que tendrá con el tema predefinido o con los valores personalizados especificados.

## Seleccionar color

Haga clic en **Básico** para seleccionar un color predefinido, o bien haga clic en **RGB** para crear un color personalizado.

### Básico

Seleccione el color que desea utilizar en la paleta de la izquierda. El color seleccionado aparecerá en el cuadrado grande a la derecha del diálogo.

## RGB

Utilice los deslizadores de los colores rojo, verde y azul para combinarlos y crear un color personalizado. El color creado aparecerá en el cuadrado grande a la derecha del diálogo.

## Contexto: Listas de servidores de nombres NetBIOS

En esta ventana se muestran todas las listas de servidores de nombres de NetBIOS configuradas para el contexto de VPN con SSL de Cisco IOS seleccionado. CIFS utiliza servidores NetBIOS para mostrar el sistema de archivos de Microsoft Windows corporativo a los usuarios de VPN con SSL de Cisco IOS.

Todas las listas de servidores de nombres configuradas para el contexto aparecen en el área **Listas de servidores de nombres NetBIOS**. Utilice los botones **Agregar**, **Editar** y **Eliminar** para gestionar estas listas. Haga clic en el nombre de una lista para ver su contenido en el área **Detalles del servidor de nombres NetBIOS**.

## Agregar o editar una lista de servidores de nombres NetBIOS

Cree o gestione una lista de servidores de nombres NetBIOS en esta ventana. Es necesario especificar un nombre para cada lista que se crea y proporcionar la dirección IP, el límite de tiempo y el número de reintentos para cada servidor de la lista. Uno de los servidores de la lista debe designarse como el servidor maestro.

En este diálogo se muestran todos los servidores de la lista, junto con los valores de estado de su maestro, límite de tiempo y reintentos.

## Agregar o editar un servidor NBNS

Se debe especificar la dirección IP de cada servidor, así como los segundos que debe esperar el router para intentar volver a conectarse al servidor y el número de veces que el router debe intentar contactar con el servidor.

Marque la opción **Hacer este servidor el servidor maestro** si desea que este sea el primer servidor de la lista con el que el router establezca comunicación.

## Contexto: Listas de mapeo de puertos

Configure las listas de mapeo de puertos para el contexto seleccionado en esta ventana. Las listas pueden estar asociadas con cualquier política de grupo configurada en el contexto seleccionado. Las listas de mapeo de puertos revelan los servicios de la aplicación TCP a los clientes de VPN con SSL de Cisco IOS.

En la parte superior de la ventana se muestran las listas de mapeo de puertos configuradas para el contexto seleccionado. Haga clic en el nombre de una lista para ver los detalles de la lista en la parte inferior de la ventana.

La ventana muestra la dirección IP, el número de puerto utilizado, el número de puerto correspondiente en el cliente y una descripción, en el caso de que exista.

## Agregar o editar una lista de mapeo de puertos

Cree y gestione listas de mapeo de puertos en esta ventana. Cada lista debe tener un nombre y contener al menos una entrada de servidor. Utilice los botones **Agregar**, **Editar** y **Eliminar** para crear, modificar y eliminar entradas de la lista.

## Contexto: Listas de direcciones URL

Las listas de direcciones URL especifican qué enlaces pueden aparecer en el portal de los usuarios de un grupo en concreto. Configure una o varias listas de direcciones URL para cada contexto y, a continuación, utilice las ventanas de la política de grupo para asociar estas listas con políticas de grupo específicas.

En la parte superior de la pantalla se muestran todas las listas de direcciones URL configuradas para el contexto. En la parte inferior de la ventana se muestra el contenido de la lista seleccionada. Para cada lista, se muestra el título que aparece en la parte superior de la lista de URL y todas las direcciones URL de la lista.

Utilice los botones **Agregar**, **Editar** y **Eliminar** para crear y gestionar listas de direcciones URL.

## Agregar o editar una lista de direcciones URL

Se debe especificar un nombre para cada lista de direcciones URL, así como un texto de título que aparecerá en la parte superior de la lista de URL.

El texto del título debe describir el contenido general de los enlaces de la lista. Por ejemplo, si una lista de direcciones URL proporciona acceso a páginas Web de planes de salud o seguros, se puede utilizar el texto de título `Prestaciones médicas`.

Utilice el botón **Agregar** para crear una nueva entrada en la lista, y los botones **Editar** y **Eliminar** para gestionar la lista. Todas las entradas añadidas aparecerán en el área Lista.

## Contexto: Cisco Secure Desktop

Cisco Secure Desktop cifra cookies, archivos del historial del explorador, archivos temporales y documentos adjuntos de correo electrónico que podrían provocar problemas de seguridad si no se cifraran. Al finalizar una sesión de VPN con SSL de Cisco IOS, Cisco Secure Desktop elimina los datos con el algoritmo de saneamiento del Departamento de Defensa de los EE.UU.

Haga clic en **Activar Cisco Secure Desktop** para permitir que todos los usuarios de este contexto puedan descargarse y utilizar **Cisco Secure Desktop**. Si el paquete de instalación del software no se encuentra en el router, aparecerá un mensaje en esta ventana.

Para cargar el paquete de instalación de Cisco Secure Desktop en el router, haga clic en Paquetes en el árbol VPN con SSL de Cisco IOS y siga las instrucciones en la ventana.



# Gateways SSL VPN

En esta ventana se muestran los gateways VPN con SSL de Cisco IOS configurados en el router y se pueden modificar los gateways existentes, así como configurar otros nuevos. Un gateway VPN con SSL de Cisco IOS es el portal del usuario a la red segura.

## Gateways SSL VPN

En esta área de la ventana se enumeran los gateways VPN con SSL de Cisco IOS configurados en el router. Se muestra el nombre, la dirección IP y el estado del gateway, así como el número de contextos configurados para su uso.



El gateway está activado y en funcionamiento.



El gateway está desactivado y no está en funcionamiento.

Haga clic en un gateway para ver sus detalles en la parte inferior de la ventana. Puede activar un gateway que esté **Desactivado** seleccionándolo y haciendo clic en **Activar**. Para hacer que un gateway activado deje de funcionar, selecciónelo y haga clic en **Desactivar**. Para editar un gateway, selecciónelo y haga clic en el botón **Editar**. Para eliminar un gateway, selecciónelo y haga clic en el botón **Eliminar**.

## Detalles del gateway SSL VPN

En esta área de la ventana se muestran los detalles de la configuración del gateway seleccionado en la parte superior de la ventana y los nombres de los contextos VPN con SSL de Cisco IOS configurados para usar este gateway.

Para obtener más información acerca de los detalles de configuración del gateway, haga clic en [Agregar o editar un gateway SSL VPN](#). Para obtener más información sobre los contextos, haga clic en [Contexto de SSL VPN](#).

## Agregar o editar un gateway SSL VPN

En esta ventana se pueden crear o editar gateways de VPN con SSL de Cisco IOS.

### Nombre de gateway

El nombre del gateway identifica de forma unívoca este gateway en el router y es el nombre utilizado para hacer referencia al gateway durante la configuración de los contextos VPN con SSL de Cisco IOS.

### Dirección IP

Seleccione o especifique la dirección IP que debe utilizar el gateway. Debe tratarse de una dirección IP pública y no de una dirección utilizada por otro gateway en el router.

### Certificado digital

Seleccione el certificado que debe enviarse a los clientes de VPN con SSL de Cisco IOS para la autenticación SSL.

### Casilla de verificación Redireccionamiento de HTTP

Desmarque esta casilla si no desea que se utilice el redireccionamiento de HTTP. El redireccionamiento de HTTP redirecciona automáticamente las peticiones HTTP al puerto 443, el puerto que se utiliza para la comunicación segura de VPN con SSL de Cisco IOS.

### Casilla de verificación Habilitar gateway

Desmarque esta casilla si no desea activar el gateway. También es posible activar y desactivar el gateway desde la ventana Gateways SSL VPN.

# Paquetes

Esta ventana permite obtener paquetes de instalación de software que deben descargarse en los clientes de VPN con SSL de Cisco IOS para que puedan admitir funciones de VPN con SSL de Cisco IOS, así como cargarlos en el router. También se puede utilizar esta ventana para eliminar paquetes de instalación instalados.

Siga los pasos que se describen en la ventana para descargar los paquetes de instalación de Cisco.com al PC y, a continuación, para copiarlos desde el PC al router. Si desea obtener alguno de los paquetes de instalación, empiece por el Paso 1 haciendo clic en el enlace al sitio de descarga.



## Nota

---

El acceso a estos sitios de descarga requiere un nombre de usuario y una contraseña de CCO. Si no dispone de un nombre de usuario y una contraseña de CCO, puede obtenerlos haciendo clic en Registro en la parte superior de la página Web Cisco.com. y rellenando el formulario que aparecerá. Recibirá por correo electrónico el nombre de usuario y la contraseña.

---

Si ya ha cargado los paquetes de instalación en el PC o en el router, realice los pasos 2 y 3 para especificar la ubicación actual de los paquetes de instalación y copiarlos en la memoria flash del router.

Haga clic en el botón ... de cada sección para especificar la ubicación actual del paquete de instalación.

Después de especificar la ubicación actual y la que desea utilizar para copiar el paquete en la memoria flash del router, haga clic en **Instalar**.

Una vez cargado en el router, en la ventana aparecerá el nombre, la versión y la fecha de creación del paquete. Si el paquete dispone de una herramienta de administración, en la ventana aparecerá un botón que le permitirá ejecutarla.

El paquete de instalación de cliente de VPN con SSL de Cisco IOS está disponible en el enlace siguiente:

<http://www.cisco.com/cgi-bin/tablebuild.pl/sslvpnclient>

El paquete de instalación de Cisco Secure Desktop está disponible en el enlace siguiente:

<http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop>

## Instalar paquete

Especifique en esta ventana la ubicación actual de un paquete de instalación navegando hasta él. Si el paquete de instalación ya se encuentra en el router, haga clic en **Router** y navegue hasta él. Si se ha cargado en el PC, haga clic en **Mi PC** y navegue hasta él. Cuando haya especificado la ubicación actual del paquete de instalación, haga clic en **Aceptar**.

La ubicación aparecerá en la ventana Paquetes.

# Contextos, gateways y políticas VPN con SSL de Cisco IOS

Cisco SDM ofrece una forma sencilla de configurar las conexiones de VPN con SSL de Cisco IOS para usuarios remotos. Sin embargo, la terminología que utiliza esta tecnología puede resultar confusa. Este tema de ayuda trata sobre los términos de VPN con SSL de Cisco IOS utilizados en las ventanas de configuración de Cisco SDM y describe el modo en el que los componentes de VPN con SSL de Cisco IOS trabajan conjuntamente. También se proporciona un ejemplo de uso del asistente para VPN con SSL de Cisco IOS y las ventanas de edición en Cisco SDM.

Antes de tratar los componentes individualmente, es conveniente recordar lo siguiente:

- Un contexto de VPN con SSL de Cisco IOS puede admitir múltiples políticas de grupo.
- Cada contexto debe tener un gateway asociado.
- Un gateway puede admitir múltiples contextos.
- Si existe más de una política de grupo en el router, se debe utilizar un servidor AAA para la autenticación.

## Contextos de VPN con SSL de Cisco IOS

Un contexto de VPN con SSL de Cisco IOS identifica los recursos necesarios para admitir túneles SSL VPN entre clientes remotos una intranet privada o corporativa, y admite una o varias políticas de grupo. Un contexto de VPN con SSL de Cisco IOS proporciona los siguientes recursos:

- Un gateway VPN con SSL de Cisco IOS asociado, que proporciona una dirección IP a la que los clientes tienen acceso, así como un certificado que sirve para establecer una conexión segura.
- Métodos de autenticación. Los usuarios se pueden autenticar localmente o mediante servidores AAA.
- Los ajustes de la visualización HTML del portal que proporciona enlaces a recursos de red.
- Listas de mapeo de puertos que permiten el uso de subprogramas de Cliente ligero en clientes remotos. Cada lista debe estar configurada para su uso en una política de grupo específica.
- Listas de direcciones URL que contienen enlaces a recursos de la intranet corporativa. Cada lista debe estar configurada para su uso en una política de grupo específica.
- Listas de servidores de nombres NetBIOS. Cada lista debe estar configurada para su uso en una política de grupo específica.

Estos recursos están disponibles al configurar políticas de grupo de VPN con SSL de Cisco IOS.

Un contexto de VPN con SSL de Cisco IOS puede admitir múltiples políticas de grupo. Un contexto de VPN con SSL de Cisco IOS sólo puede asociarse con un gateway.

## Gateways VPN con SSL de Cisco IOS

Un gateway VPN con SSL de Cisco IOS proporciona una dirección IP accesible y un certificado para uno o varios contextos VPN con SSL de Cisco IOS. Cada gateway configurado en un router debe estar configurado con su propia dirección IP; las direcciones IP no pueden compartirse entre varios servidores. Es posible utilizar la dirección IP de una interfaz del router u otra dirección IP accesible, en el caso de que esté disponible. Es necesario configurar un certificado digital o un certificado con firma para uso de los gateways. Todos los gateways del router pueden utilizar el mismo certificado.

Aunque un gateway puede servir para múltiples contextos VPN con SSL de Cisco IOS, deben tenerse en cuenta las restricciones de recursos y accesibilidad de la dirección IP.

## Políticas VPN con SSL de Cisco IOS

Las políticas de grupo de VPN con SSL de Cisco IOS permiten dar cabida a las necesidades de distintos grupos de usuarios. Un grupo de ingenieros que trabaje de forma remota necesitará tener acceso a recursos de red distintos de los que pueda requerir el personal de ventas que trabaje en el campo. Los socios empresariales y los proveedores externos deben poder acceder a la información que necesitan para trabajar con su organización, pero debe asegurarse de que no tengan acceso a información confidencial o a otros recursos que no les sean necesarios. La creación de distintas políticas para cada uno de estos grupos permite ofrecer a los usuarios remotos los recursos que necesitan e impedir que accedan a los demás.

Al configurar una política de grupo, se pueden seleccionar recursos como las listas de direcciones URL, de mapeo de puertos y de servidores de nombres NetBIOS configuradas para el contexto asociado a la política.

Si hay más de una política de grupo configurada en el router, será necesario configurar el router para que utilice un servidor AAA para autenticar los usuarios y determinar a qué grupo de políticas pertenece ese usuario en concreto. Para obtener más información, haga clic en [Más detalles acerca de las políticas de grupo](#).

## Ejemplo

En este ejemplo, un usuario hace clic en **Crear nuevo SSL VPN** y utiliza el asistente para crear la primera configuración de VPN con SSL de Cisco IOS en el router. Al finalizar este asistente se crea un contexto, un gateway y una política de grupo nuevos. La tabla siguiente contiene la información que el usuario especifica en cada ventana del asistente, así como la configuración que crea Cisco SDM con esa información.

Ventana Asistente para VPN con SSL de Cisco IOS	Configuración
<p><b>Ventana Crear SSL VPN</b></p> <p>El área Tareas previas indica que los certificados digitales no están configurados en el router.</p> <p>El usuario hace clic en <b>Certificado con firma automática</b> y configura un certificado en el cuadro de diálogo Certificado con firma automática permanente. El usuario no modifica el nombre Router_Certificate suministrado por Cisco SDM.</p> <p>El usuario hace clic en <b>Crear nuevo SSL VPN</b>.</p>	<p>Cisco SDM configura un certificado con firma automática denominado “Router_Certificate” que estará disponible para el uso en todas las configuraciones de VPN con SSL de Cisco IOS.</p>

Ventana Asistente para VPN con SSL de Cisco IOS	Configuración
<b>Ventana Dirección IP y nombre</b>	
<p>El usuario especifica la información siguiente:</p> <p>Dirección IP: 172.16.5.5</p> <p>Nombre: Asia</p> <p>Seleccionar <b>Activar acceso SDM seguro a través de 192.168.1.1</b>.</p> <p>Certificado: <b>Router_Certificate</b></p>	<p>Cisco SDM crea un contexto denominado “Asia”.</p> <p>Cisco SDM crea un gateway denominado “gateway_1” que utiliza la dirección IP 172.16.5.5 y Router_Certificate. Este gateway se puede asociar con otros contextos VPN con SSL de Cisco IOS.</p> <p>Los usuarios accederán al portal de VPN con SSL de Cisco IOS escribiendo http://172.16.5.5/Asia. Si este gateway está asociado con contextos adicionales, se utilizará la misma dirección IP en la URL para estos contextos. Por ejemplo, si también se ha configurado el contexto Europa para que utilice gateway_1, los usuarios escribirán https://172.16.5.5/Europa para acceder al portal.</p> <p>Una vez enviada la configuración al router, los usuarios deberán escribir http://172.16.5.5:4443 para iniciar Cisco SDM con esta dirección IP.</p> <p>Cisco SDM también empezará a configurar la primera política de grupo, denominada policy_1.</p>
<b>Ventana Autenticación de usuario</b>	
<p>El usuario selecciona <b>Localmente en este router</b>. El usuario añade una cuenta de usuario a la lista existente.</p>	<p>Cisco SDM crea la lista de autenticación “sdm_vpn_xauth_ml_1.” Esta lista se mostrará en la ventana Contextos de VPN con SSL de Cisco IOS cuando el usuario finalice el asistente.</p> <p>Los usuarios enumerados en la ventana Autenticación de usuarios son miembros de esta lista de autenticación y se rigen por la política policy_1.</p>
<b>Ventana Configurar sitios Web de la intranet</b>	
<p>El usuario configura la lista de direcciones URL Ulist_1. Su título es “Taiwan”.</p>	<p>La lista de direcciones URL con el título Taiwán será visible en el portal que verán los usuarios de “sdm_vpn_xauth_ml_1” cuando inicien sesión.</p> <p>La lista de direcciones URL estará disponible para la configuración en otras políticas de grupo configuradas en el contexto “Asia”.</p>



Ventana Asistente para VPN con SSL de Cisco IOS	Configuración
<b>Ventana Activar túnel completo</b>	
El usuario hace clic en <b>Activar túnel completo</b> y selecciona un conjunto de direcciones predefinido. No se configuran opciones avanzadas.	Los PC cliente descargarán el software de cliente de túnel completo cuando inicien sesión por primera vez y se establecerá un solo túnel completo entre el PC y el router al realizar la conexión al portal.
<b>Ventana Personalizar el portal SSL VPN</b>	
El usuario selecciona <b>Brisa oceánica</b> .	Cisco SDM configura los ajustes de la visualización HTTP con este esquema de color. El portal que aparece cuando los usuarios de policy_1 inician sesión utiliza esta configuración. Estos ajustes del portal también se aplican a todas las políticas configuradas en el contexto “Asia”. El usuario puede personalizar los ajustes de la visualización HTTP en la ventana Editar SSL VPN tras ejecutar el asistente.
<b>Ventana Configuración de paso por SSL VPN</b>	
El usuario selecciona <b>Permitir que SSL VPN funcione con NAC y firewall</b> .	Cisco SDMSDM añade una ACL con la entrada siguiente. <pre>permit tcp any host 172.16.5.5 eq 443</pre>
<b>Ventana Resumen</b>	
La ventana Resumen muestra la información que aparece a la derecha. Los detalles adicionales se pueden ver en la ventana Editar SSL VPN.	<p>Nombre de política SSL VPN: policy_1  Nombre de Gateway SSL VPN: gateway_1</p> <p>Lista de métodos de autenticación de usuario (User Authentication Method List): Local</p> <p>Configuración de túnel completo  Estado SVC: Sí  Conjunto de direcciones IP: Pool_1  División de la arquitectura de túneles: Desactivada  DNS dividido: Desactivada  Instale el cliente de túnel completo: Activado</p>

Cuando se envía esta configuración, el router tiene un contexto de VPN con SSL de Cisco IOS denominado Asia, un gateway denominado gateway\_1 y una política de grupo denominada policy\_1. Esta información se muestra en la ventana Editar SSL VPN tal como se indica en la tabla siguiente:

Nombre	Gateway	Dominio	Estado	Estado administrativo
Asia	gateway_1	Asia		En servicio

**Detalles del contexto SSL VPN Asia:**

Nombre de elemento	Valor de elemento
<b>Políticas de grupo</b>	
policy_1	
Servicios	Manipulación de URL, Túnel completo
URL mostradas a los usuarios	http://172.16.5.5/pricelist
	http://172.16.5.5/catalog
Servidores mostrados a los usuarios	<Ninguno>
Servidores WINS	<Ninguno>

policy\_1 proporciona el servicio de VPN con SSL de Cisco IOS básico de manipulación de URL y especifica que se establezca un solo túnel completo entre los clientes y el router. No se configuran más funciones. Puede añadir funciones a policy\_1 como, por ejemplo, Cliente ligero y Sistema de archivos de Internet común seleccionando **Configurar funciones avanzadas para un SSL VPN existente**, seleccionando **Asia** y **policy\_1** en la ventana Seleccionar el grupo de usuarios de VPN con SSL de Cisco IOS, y seleccionando las funciones en la ventana Características avanzadas. En este asistente también se pueden configurar listas de direcciones URL adicionales.

Puede crear una nueva política de grupo en el contexto “Asia” seleccionando **Agregar una nueva política a un SSL VPN existente para un nuevo grupo de usuarios**.

Puede personalizar los ajustes y las políticas configuradas para el contexto Asia seleccionando Asia en la lista de contextos y haciendo clic en **Editar**. La ventana Editar contexto SSL VPN Asia muestra un árbol que permite configurar otros recursos para el contexto, y editar y configurar políticas adicionales. Puede editar los ajustes de gateway\_1 haciendo clic en **Gateways SSL VPN** en el nodo de SSL VPN, seleccionando gateway\_1 y haciendo clic en **Editar**.

## Cómo...

Los temas de “Cómo...” describen tareas de configuración comunes asociadas con esta función.

## ¿Cómo puedo confirmar que VPN con SSL de Cisco IOS funciona?

El mejor modo de determinar que un contexto de VPN con SSL de Cisco IOS proporcionará el acceso configurado a los usuarios es configurarse usted mismo como usuario e intentar acceder a todos los sitios Web y servicios que el contexto debe proporcionar a los usuarios. Utilice el procedimiento siguiente como pauta para realizar esta prueba.

- 
- Paso 1** Asegúrese de que las credenciales que puede utilizar están incluidas en todas las políticas adecuadas en el servidor AAA.
  - Paso 2** Si puede hacerlo, abra una sesión de Cisco SDM en el router para poder supervisar el tráfico de VPN con SSL de Cisco IOS que creará. Esto debe hacerlo en un PC distinto en el caso de que el PC que utiliza para probar el contexto de VPN con SSL de Cisco IOS no se encuentre en una red desde la que pueda acceder a Cisco SDM. Vaya a **Supervisar > Estado de VPN > SSL VPN**.
  - Paso 3** Especifique la dirección URL que dirige cada una de los portales configurados para este contexto de VPN con SSL de Cisco IOS. Asegúrese de que todas las páginas tienen el aspecto configurado y de que todos los enlaces especificados en las listas de direcciones URL para la política aparecen en la página.
  - Paso 4** Pruebe todos los enlaces y servicios que deben estar disponibles para los usuarios incluidos en esta política. Si ninguna de las políticas que está probando ofrece la descarga de Cisco Secure Desktop o el software de cliente de túnel completo, escriba las URL a los portales para estas políticas y haga clic en los enlaces que requerirán la descarga de este software. Asegúrese de que el software se descarga correctamente y de que puede acceder a los servicios a los que debería poder acceder el usuario desde estos enlaces.

- Paso 5** Si ha podido establecer una sesión de Cisco SDM antes de iniciar la prueba, haga clic en la rama del contexto que está probando y observe las estadísticas de tráfico de VPN con SSL de Cisco IOS en la ventana VPN con SSL de Cisco IOS.
- Paso 6** Con los resultados de las pruebas, vuelva a Cisco SDM si fuera necesario y solucione cualquier problema de configuración que haya detectado.
- 

## ¿Cómo se configura una VPN con SSL de Cisco IOS después de configurar un firewall?

Si ya ha configurado un firewall, aún puede usar los asistentes para VPN con SSL de Cisco IOS en Cisco SDM para crear contextos y políticas VPN con SSL de Cisco IOS. Cisco SDM valida los comandos del CLI de VPN con SSL de Cisco IOS que genera frente a la configuración existente en el router. Si detecta una configuración de firewall existente que debe modificarse para permitir el paso al tráfico de VPN con SSL de Cisco IOS, se le informará. Puede permitir que Cisco SDM realice las modificaciones necesarias al firewall, o bien puede dejar intacto el firewall y realizar los cambios manualmente yendo a **Configurar > Firewall y ACL > Editar firewall ACL** y especificando las declaraciones de permiso necesarias para permitir que el tráfico de VPN con SSL de Cisco IOS pase por el firewall.

## ¿Cómo puedo asociar una instancia de VRF con un contexto de VPN con SSL de Cisco IOS?

Las instancias de VRF gestionan una tabla de enrutamiento y una de redireccionamiento para una VPN. Es posible asociar un nombre o una instancia de VRF con un contexto de VPN con SSL de Cisco IOS yendo a **Configurar > VPN > SSL VPN > Editar SSL VPN**. Seleccione el contexto que desea asociar con una instancia de VRF y haga clic en **Editar**. Seleccione el nombre de la instancia de VRF en el diálogo que aparecerá.



### Nota

---

La instancia de VRF ya debe estar configurada en el router.

---



# CAPÍTULO 20

## Resolución de problemas de VPN

---

Cisco SDM permite resolver los problemas de las conexiones VPN que haya configurado. Cisco SDM informa del resultado de las pruebas de conexión y, en caso de que sea negativo, recomienda acciones que se pueden llevar a cabo para corregir los problemas de conexión.

El enlace siguiente proporciona información sobre la resolución de problemas de VPN mediante el uso de la interfaz de línea de comandos (CLI).

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000\\_b/vpnman/vms\\_2\\_2/rmc13/useguide/u13\\_rtrb.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/vpnman/vms_2_2/rmc13/useguide/u13_rtrb.htm)

## Resolución de problemas de VPN

Esta ventana aparece cuando soluciona problemas de una VPN sitio a sitio, un túnel GRE sobre IPSec, una conexión de Easy VPN remoto o una conexión de servidor Easy VPN.



### Nota

---

La resolución de problemas de VPN no solucionará problemas de más de dos pares en la VPN sitio a sitio, GRE sobre IPSec o en las conexiones de cliente Easy VPN.

---

## Detalles del túnel

Esta casilla proporciona detalles del túnel VPN.

### Interfaz

Interfaz para la que se ha configurado el túnel VPN.

### Par

La dirección IP o el nombre de host de los dispositivos del otro extremo de la conexión VPN.

## Resumen

Haga clic en este botón para ver la información resumida de la resolución de problemas.

## Detalles

Haga clic en este botón para ver la información detallada de la resolución de problemas.

## Actividad

En esta columna se muestran las actividades de resolución de problemas.

## Estado

Muestra el estado de cada actividad de resolución de problemas mediante los iconos y textos de alerta siguientes:



La conexión está activa.



La conexión está inactiva.



La prueba se ha superado.



La prueba ha fallado.

### Motivos del fallo

En esta casilla se proporcionan los posibles motivos del fallo del túnel VPN.

## Acciones recomendadas

En este cuadro se proporciona una posible acción/solución para corregir el problema.

### Botón Cerrar

Haga clic en este botón para cerrar la ventana.

### Botón Probar cliente específico

Este botón se activa si prueba conexiones para un servidor Easy VPN configurado en el router. Haga clic en él y especifique el cliente con el que desea probar la conectividad.

Este botón se desactiva cuando se dan las circunstancias siguientes:

- No se ha realizado la prueba básica o ésta no ha finalizado correctamente.
- La imagen de IOS no admite los comandos de depuración requeridos.
- La vista utilizada para iniciar Cisco SDM no dispone de privilegios raíz.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Resolver los problemas de la conexión VPN.	Haga clic en el botón <b>Iniciar</b> . Cuando se esté ejecutando la prueba, la etiqueta del botón <b>Iniciar</b> cambiará a <b>Detener</b> . Tiene la opción de cancelar la resolución de problemas mientras la prueba esté ejecutándose.
Guardar el informe de la prueba.	Haga clic en <b>Guardar informe</b> para guardar el informe de la prueba en formato HTML. Este botón se desactiva cuando la prueba está ejecutándose.

# Resolución de problemas de VPN: Especificar el cliente Easy VPN

Esta ventana le permite especificar el cliente Easy VPN que desea depurar.

## Dirección IP

Especifique la dirección IP del cliente Easy VPN que desea depurar.

## Escuchar solicitud durante X minutos

Especifique el tiempo que el servidor Easy VPN debe escuchar las solicitudes del cliente Easy VPN.

## Botón Continuar

Después de seleccionar el tipo de generación de tráfico que desea, haga clic en este botón para seguir con la prueba.

## Botón Cerrar

Haga clic en este botón para cerrar la ventana.

# Resolución de problemas de VPN: Generar tráfico

Esta ventana permite generar tráfico de VPN de sitio a sitio o de Easy VPN para su depuración. Es posible permitir que Cisco SDM genere tráfico de VPN, o éste puede generarse por parte del usuario.

## El tráfico VPN de esta conexión se define como:

En esta área aparece una lista con el tráfico VPN de la interfaz.

### Acción

Esta columna indica si ese tipo de tráfico está permitido en la interfaz.



**Origen**

Dirección IP de origen.

**Destino**

Dirección IP de destino.

**Servicio**

En esta columna aparece una lista con los tipos de tráfico de la interfaz.

**Registro**

Esta columna indica si se ha activado el registro para ese tráfico.

**Atributos**

Cualquier atributo adicional definido.

**Hacer que SDM genere tráfico VPN**

Seleccione esta opción si desea que Cisco SDM genere tráfico VPN en la interfaz para depurarlo.

**Nota**

---

Cisco SDM no generará tráfico VPN cuando el tráfico del túnel VPN provenga de una lista de control de acceso (ACL) basada en IP o cuando la vista del CLI aplicada y la vigente no sea la vista raíz.

---

**Especificar la dirección IP de un host de la red de origen:**

Especifique la dirección IP de host de la red de origen.

**Especificar la dirección IP de un host de la red de destino:**

Especifique la dirección IP de host de la red de destino.

**Generaré tráfico VPN desde la red de origen**

Seleccione esta opción si desea generar tráfico VPN desde la red de origen.

**Intervalo de tiempo de espera**

Especifique el tiempo en segundos que el servidor Easy VPN debe esperar a que usted genere tráfico de origen. Asegúrese de especificar el tiempo suficiente para cambiar a otros sistemas para generar el tráfico.

### Botón Continuar

Después de seleccionar el tipo de generación de tráfico que desea, haga clic en este botón para seguir con la prueba.

### Botón Cerrar

Haga clic en este botón para cerrar la ventana.

## Resolución de problemas de VPN: Generar tráfico GRE

Esta pantalla aparece cuando se genera tráfico GRE sobre IPSec.

### Hacer que SDM genere tráfico VPN

Seleccione esta opción si desea que Cisco SDM genere tráfico VPN en la interfaz para depurarlo.

#### **Especificar la dirección IP del túnel remoto.**

Especifique la dirección IP del túnel GRE remoto. No utilice la dirección de la interfaz remota.

### Generaré tráfico VPN desde la red de origen

Seleccione esta opción si desea generar tráfico VPN desde la red de origen.

#### **Intervalo de tiempo de espera**

Especifique el tiempo en segundos que el servidor Easy VPN debe esperar a que usted genere tráfico de origen. Asegúrese de especificar el tiempo suficiente para cambiar a otros sistemas para generar el tráfico.

### Botón Continuar

Después de seleccionar el tipo de generación de tráfico que desea, haga clic en este botón para seguir con la prueba.

### Botón Cerrar

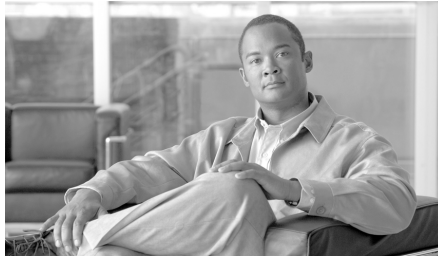
Haga clic en este botón para cerrar la ventana.

## Advertencia de Cisco SDM: SDM activará depuraciones del router

Esta ventana aparece cuando Cisco SDM está listo para empezar la resolución avanzada de problemas. La resolución avanzada de problemas implica el envío de comandos de depuración al router a la espera de resultados y, a continuación, la eliminación de dichos comandos de depuración para que el rendimiento del router no resulte todavía más afectado.

Este mensaje aparece porque el proceso puede tardar varios minutos y puede afectar al rendimiento del router.

■ Advertencia de Cisco SDM: SDM activará depuraciones del router



# CAPÍTULO 21

## Auditoría de seguridad

---

La Auditoría de seguridad es una función que examina las configuraciones existentes del router y actualiza este último para aumentar su seguridad y la de la red. Esta función se basa en la función AutoSecure de Cisco IOS; comprueba y ayuda en la configuración de casi todas las funciones AutoSecure. Para obtener una lista completa de las funciones que la Auditoría de seguridad busca y una lista de las nuevas funciones AutoSecure que la Auditoría de seguridad no admite, consulte el tema [Cisco SDM y AutoSecure de Cisco IOS](#).

La función Auditoría de seguridad tiene dos posibilidades de funcionamiento: mediante el Asistente para la auditoría de seguridad, que permite seleccionar los cambios de configuración que podrían relacionarse con la seguridad y que se implementarán en el router y mediante Bloqueo de un paso, que realiza automáticamente todos los cambios recomendados en la configuración relacionados con la seguridad.

### Realizar una auditoría de seguridad

Esta opción inicia el Asistente para la auditoría de seguridad. Este asistente prueba la configuración del router para determinar si existen posibles problemas de seguridad en la configuración y, a continuación, ofrece una pantalla que permite determinar cuáles de dichos problemas de seguridad se desean corregir. Una vez que se hayan determinado dichos problemas, el Asistente para la auditoría de seguridad realizará los cambios necesarios en la configuración del router para corregirlos.

**Para que Cisco SDM lleve a cabo una auditoría de seguridad y, a continuación, corrija los problemas que haya encontrado:**

- 
- Paso 1** En el panel izquierdo, seleccione **Auditoría de seguridad**.
- Paso 2** Haga clic en **Realizar una auditoría de seguridad**.  
Aparecerá la página de bienvenida del Asistente para la auditoría de seguridad.
- Paso 3** Haga clic en **Siguiente>**.  
Aparecerá la página Configuración de la interfaz de la auditoría de seguridad.
- Paso 4** El Asistente para la auditoría de seguridad necesita saber cuáles de las interfaces de router se conectan a la red interna y cuáles se conectan a los elementos externos a la red. Para cada interfaz que figura en la lista, seleccione la casilla de verificación **Interna** o **Externa** para indicar dónde se conecta la interfaz.
- Paso 5** Haga clic en **Siguiente>**.  
El Asistente para la auditoría de seguridad comprueba la configuración del router para determinar los posibles problemas de seguridad que podrían producirse. Aparecerá una pantalla que muestra el progreso de esta acción y que proporciona una lista de las opciones de configuración que se están comprobando y que indica si la configuración del router actual supera satisfactoriamente dichas comprobaciones. Si desea guardar este informe en un archivo, haga clic en **Guardar informe**.
- Paso 6** Haga clic en **Cerrar**.  
Aparecerá la pantalla Tarjeta de informes de auditoría de seguridad SDM con una lista de los posibles problemas de seguridad.
- Paso 7** Seleccione las casillas **Repararlo** correspondientes a los problemas que desee que Administrador del dispositivo de seguridad de Cisco (Cisco SDM) repare. Si desea obtener una descripción de un problema y una lista de los comandos del IOS de Cisco que se agregarán a la configuración, haga clic en la descripción del problema para ver una página de ayuda acerca del mismo.
- Paso 8** Haga clic en **Siguiente>**.
- Paso 9** Es posible que el Asistente para la auditoría de seguridad muestre una o varias pantallas que requieran la introducción de información para reparar determinados problemas. Especifique la información según sea necesario y haga clic en **Siguiente>** para cada una de las pantallas.
- Paso 10** La página Resumen del asistente muestra una lista de todos los cambios en la configuración que realizará el Asistente para la auditoría de seguridad. Haga clic en **Finalizar** para enviar dichos cambios al router.
-

## Bloqueo de un paso

Esta opción comprueba la configuración del router en búsqueda de posibles problemas de seguridad y realiza automáticamente los cambios necesarios en la configuración para corregir los problemas que encuentre. Las condiciones que se buscan y, en el caso necesario, se corrigen son las siguientes:

- Desactivar el servicio Finger
- Desactivar el servicio PAD
- Desactivar el servicio de pequeños servidores TCP
- Desactivar el servicio de pequeños servidores UDP
- Desactivar el servicio del servidor IP bootp
- Desactivar el servicio IP ident
- Desactivar CDP
- Desactivar la ruta de origen IP
- Activar el servicio de cifrado de contraseñas
- Activar los paquetes “keep-alive” de TCP para sesiones telnet entrantes
- Activar los paquetes “keep-alive“ de TCP para sesiones telnet salientes
- Activar números de secuencia y marcadores de hora en depuraciones
- Activar IP CEF
- Desactivar Gratuitous ARP de IP
- Definir la longitud mínima de la contraseña a menos de 6 caracteres
- Definir la proporción de fallos de autenticación a menos de 3 intentos
- Definir la hora TCP Synwait
- Definir anuncio
- Activar registro
- Definir activación de la contraseña secreta
- Desactivar SNMP
- Definir el intervalo del Programador
- Definir asignación del Programador
- Definir usuarios

- Activar configuración Telnet
- Activar cambio a NetFlow
- Desactivar redireccionamiento IP
- Desactivar ARP Proxy IP
- Desactivar difusión dirigida IP
- Desactivar servicio MOP
- Desactivar IP de destino inalcanzable
- Desactivar respuesta de máscara IP
- Desactivar IP de destino inalcanzable en interfaz NULA
- Activar RPF unidifusión en todas las interfaces externas
- Activar firewall en todas las interfaces externas
- Definir la clase de acceso en el servicio de servidor HTTP
- Definir la clase de acceso en líneas VTY
- Activar SSH para acceder al router

## Página de bienvenida

Esta pantalla describe el Asistente para la auditoría de seguridad y los cambios que éste intentará realizar a la configuración del router.



## Página de selección de la interfaz

Esta pantalla muestra una lista de todas las interfaces y requiere la identificación de las interfaces de router “externas”; es decir, las interfaces que se conectan a redes inseguras como, por ejemplo, Internet. Al identificar las interfaces externas, la Configuración de seguridad sabe para qué interfaces necesita configurar las funciones de seguridad del firewall.

### Columna Interfaz

Esta columna proporciona una lista de cada una de las interfaces de router.

### Columna Externa

Esta columna muestra una casilla de verificación para cada interfaz que figura en la lista de la columna Interfaz. Seleccione la casilla de verificación para aquellas interfaces que se conecten a una red externa a la red como, por ejemplo, Internet.

### Columna Interna

Esta columna muestra una casilla de verificación para cada interfaz que figura en la lista de la columna Interfaz. Seleccione la casilla de verificación para aquellas interfaces que se conecten directamente a la red local y que, por lo tanto, estén protegidas de Internet mediante el firewall.

## Página Tarjeta de informes

La página emergente Tarjeta de informes muestra una lista de los cambios de configuración recomendados que, al aplicarse, harán que la red sea más segura. El botón **Guardar**, que se activa tras realizar todas las comprobaciones, permite guardar la tarjeta de informes en un archivo que se puede imprimir o enviar por correo electrónico. Al hacer clic en **Cerrar**, aparecerá un cuadro de diálogo que incluye una lista de los problemas de seguridad encontrados y una lista de las configuraciones de seguridad que Cisco SDM puede deshacer.

# Página Repararlo

Esta página muestra los cambios recomendados en la configuración en la página de Tarjeta de informes. Utilice la lista **Seleccione una opción** para ver los problemas de seguridad que Cisco SDM puede reparar o las configuraciones de seguridad que Cisco SDM puede deshacer.

## Seleccione una opción: Solucionar los problemas de seguridad

La pantalla Tarjeta de informes muestra una lista de los cambios de configuración recomendados que harán que la red y el router sean más seguros. Los posibles problemas de seguridad de la configuración del router figuran en la columna izquierda. Para obtener más información acerca de un posible problema, haga clic en el problema. La ayuda en línea mostrará una descripción más detallada del mismo y los cambios de configuración recomendados. Para corregir todos los posibles problemas, haga clic en **Reparar todo** y, a continuación, en **Siguiente>** para continuar. Para corregir problemas de seguridad individuales, seleccione la casilla de verificación **Repararlo** junto al problema que desee corregir y, a continuación, haga clic en **Siguiente>** para continuar en el Asistente para la auditoría de seguridad. Este último corregirá los problemas seleccionados y recopilará información adicional del usuario según sea necesario. A continuación, mostrará una lista de los nuevos comandos de configuración que se agregarán a la configuración del router.

### Reparar todo

Haga clic en este botón para colocar una marca de verificación junto a todos los posibles problemas de seguridad que figuran en la pantalla Tarjeta de informes.

## Seleccione una opción: Deshacer las configuraciones de seguridad

Si selecciona esta opción, Cisco SDM mostrará las configuraciones de seguridad que puede deshacer. Para que Cisco SDM deshaga todas las configuraciones de seguridad, haga clic en **Deshacer todo**. Para especificar una configuración de seguridad que desea deshacer, seleccione la casilla **Deshacer** junto a dicha configuración. Cuando haya especificado las configuraciones de seguridad que desea deshacer, haga clic en **Siguiente>**. Debe seleccionar al menos una configuración de seguridad para deshacer.

### Deshacer todo

Haga clic en este botón para colocar una marca de verificación junto a todas las configuraciones de seguridad que Cisco SDM puede deshacer.

Para ver las configuraciones de seguridad que Cisco SDM puede deshacer, haga clic en:

[Configuraciones de seguridad que Cisco SDM puede deshacer](#)

## Deseo que Cisco SDM corrija algunos problemas, pero que deshaga otras configuraciones de seguridad

Si desea que Cisco SDM corrija algunos problemas de seguridad pero que, a la vez, deshaga otras configuraciones de seguridad que no se necesitan, puede ejecutar el Asistente para la auditoría de seguridad una vez para indicar los problemas que se deben reparar y, a continuación, volver a ejecutarlo para seleccionar las configuraciones que desee deshacer.

## Desactivar el servicio Finger

La Auditoría de seguridad desactiva el servicio [finger](#) siempre que esto sea posible. Este servicio se utiliza para saber qué usuarios han iniciado sesión en un dispositivo de red. Aunque esta información por lo general no es extremadamente confidencial, a veces puede resultar de gran utilidad para un atacante.

Además, el servicio Finger se puede utilizar en un tipo específico de ataque de denegación de servicio (DoS) denominado “Finger de la muerte”, que implica el envío de una solicitud Finger a un equipo específico cada minuto, sin desconectarse.

La configuración que se enviará al router para desactivar el servicio Finger es la siguiente:

```
no service finger
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Desactivar el servicio PAD

La Auditoría de seguridad desactiva todos los comandos de ensamblador/desensamblador de paquetes (PAD) y las conexiones entre los dispositivos PAD, así como los servidores de acceso siempre que sea posible.

La configuración que se enviará al router para desactivar el servicio PAD es la siguiente:

```
no service pad
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Desactivar el servicio de pequeños servidores TCP

La Auditoría de seguridad desactiva los servicios pequeños siempre que sea posible. Por defecto, los dispositivos Cisco que ejecutan la versión 11.3 o anterior del Cisco IOS ofrecen “servicios pequeños”: echo, [chargen](#) y discard.

(Los servicios pequeños están desactivados por defecto en la versión del software Cisco IOS 12.0 y superior). Estos servicios, especialmente sus versiones UDP (User Datagram Protocol), no se utilizan con frecuencia para motivos legítimos pero sí pueden utilizarse para lanzar ataques DoS que, de otro modo, se evitarían mediante el filtrado de paquetes.

Por ejemplo, un atacante podrá enviar un paquete DNS (Domain Name System), falsificando la dirección de origen para que sea un servidor DNS que, de otro modo, sería inalcanzable y falsificando el puerto de origen para que sea el puerto del servicio DNS (puerto 53). Si se enviase un paquete como el descrito al puerto “echo” UDP del router, el resultado sería que el router enviaría un paquete DNS al servidor en cuestión. A este paquete, no se le aplicaría ninguna comprobación de lista de acceso saliente, ya que se consideraría que el mismo router lo había generado localmente.

Aunque se puede evitar la mayoría de los abusos de los servicios pequeños o disminuir su nivel de peligro mediante listas de acceso “anti-spoofing”, los servicios siempre deberían desactivarse en los routers que forman parte de un firewall o que se encuentran en una sección de la red que es crítica para la seguridad. Puesto que dichos servicios no son de uso frecuente, la mejor política normalmente es desactivarlos en todos los routers de cualquier descripción.

La configuración que se enviará al router para desactivar el servicio de pequeños servidores TCP es la siguiente:

```
no service tcp-small-servers
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Desactivar el servicio de pequeños servidores UDP

La Auditoría de seguridad desactiva los servicios pequeños siempre que sea posible. Por defecto, los dispositivos Cisco que ejecutan la versión 11.3 o anterior del Cisco IOS ofrecen “servicios pequeños”: echo, [chargen](#) y discard. (Los servicios pequeños están desactivados por defecto en la versión del software Cisco IOS 12.0 y superior). Estos servicios, especialmente sus versiones UDP, no se utilizan con frecuencia para motivos legítimos pero sí pueden utilizarse para lanzar ataques DoS y de otro tipo que, de otro modo, se evitarían mediante el filtrado de paquetes.

Por ejemplo, un atacante podrá enviar un paquete DNS, falsificando la dirección de origen para que sea un servidor DNS que, de otro modo, sería inalcanzable y falsificando el puerto de origen para que sea el puerto del servicio DNS (puerto 53). Si se enviase un paquete como el descrito al puerto “echo” UDP del router, el resultado sería que el router enviaría un paquete DNS al servidor en cuestión. A este paquete, no se le aplicaría ninguna comprobación de lista de acceso saliente, ya que se consideraría que el mismo router lo había generado localmente.

Aunque se puede evitar la mayoría de los abusos de los servicios pequeños o disminuir su nivel de peligro mediante listas de acceso “anti-spoofing”, los servicios siempre deberían desactivarse en los routers que forman parte de un firewall o que se encuentran en una sección de la red que es crítica para la seguridad. Puesto que dichos servicios no son de uso frecuente, la mejor política normalmente es desactivarlos en todos los routers de cualquier descripción.

La configuración que se enviará al router para desactivar el servicio de pequeños servidores UDP es la siguiente:

```
no service udp-small-servers
```

## Desactivar el servicio del servidor IP bootp

La Auditoría de seguridad desactiva el servicio de protocolo Bootstrap (BOOTP) siempre que esto sea posible. BOOTP permite que tanto los routers como los equipos configuren automáticamente la información de Internet necesaria a partir de un servidor de mantenimiento centralizado durante el inicio, incluida la descarga del software Cisco IOS. Por lo tanto, un atacante podrá utilizar BOOTP para descargar una copia del software Cisco IOS del router.

Además, el servicio BOOTP es vulnerable a los ataques DoS y, por lo tanto, deberá desactivarse o filtrarse a través de un firewall.

La configuración que se enviará al router para desactivar el servicio BOOTP es la siguiente:

```
no ip bootp server
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Desactivar el servicio IP ident

La Auditoría de seguridad desactiva el servicio de identificación siempre que esto sea posible. El servicio de identificación permite consultar un puerto TCP para obtener la identificación. Esta función permite que un protocolo no seguro informe de la identidad de un cliente que inicia una conexión TCP y de un host que responde a dicha conexión. Con el servicio de identificación, puede conectar un puerto TCP a un host, emitir una cadena de texto simple para solicitar información y recibir una respuesta de manera similar.

Permitir que un sistema en un segmento conectado directamente conozca que el router es un dispositivo Cisco y que determine el número de modelo y la versión del software Cisco IOS que se está ejecutando es peligroso. Esta información puede utilizarse para elaborar ataques contra el router.

La configuración que se enviará al router para desactivar el servicio de identificación IP es la siguiente:

```
no ip identd
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Desactivar CDP

La Auditoría de seguridad desactiva CDP (Cisco Discovery Protocol) siempre que esto sea posible. CDP es un protocolo de propiedad que los routers Cisco utilizan para identificarse entre ellos en un segmento de LAN. Esto puede ser peligroso ya que permite que un sistema en un segmento conectado directamente conozca que el router es un dispositivo Cisco y determine el número de modelo y la versión del software Cisco IOS que se está ejecutando. Esta información puede utilizarse para elaborar ataques contra el router.

La configuración que se enviará al router para desactivar CDP es la siguiente:

```
no cdp run
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Desactivar la ruta de origen IP

La Auditoría de seguridad desactiva el enrutamiento de origen IP siempre que esto sea posible. El protocolo IP admite opciones de enrutamiento de origen que permiten al remitente de un datagrama IP controlar la ruta que el datagrama utilizará en su camino al destino final y, generalmente, la ruta que cualquier respuesta utilizará. En las redes, estas opciones raramente se utilizan por motivos legítimos. Algunas implantaciones IP más antiguas no procesan correctamente los paquetes de enrutamiento de origen y los equipos que utilizan dichas implantaciones podrían fallar al enviarles datagramas con opciones de enrutamiento de origen.

La desactivación del enrutamiento de origen IP hará que un router Cisco nunca envíe un paquete IP con una opción de enrutamiento de origen.

La configuración que se enviará al router para desactivar el enrutamiento de origen IP es la siguiente:

```
no ip source-route
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Activar el servicio de cifrado de contraseñas

La Auditoría de seguridad activa el cifrado de contraseñas siempre que esto sea posible. El cifrado de contraseñas indica al software Cisco IOS que debe cifrar las contraseñas, los secretos **CHAP** (Challenge Handshake Authentication Protocol) y datos similares que se guardan en el archivo de configuración. Esta opción es de gran utilidad para evitar que usuarios no autorizados lean las contraseñas, por ejemplo, si se fijan en la pantalla mientras el administrador especifica su contraseña.

La configuración que se enviará al router para activar el cifrado de contraseñas es la siguiente:

```
service password-encryption
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Activar los paquetes “keep-alive” de TCP para sesiones telnet entrantes

La Auditoría de seguridad activa los mensajes “keep-alive” de TCP para las sesiones **Telnet** entrantes y salientes, siempre que esto sea posible. La activación de mensajes “keep-alive” de TCP hace que el router genere periódicamente este tipo de mensajes, lo que le permite detectar y abandonar conexiones Telnet interrumpidas.

La configuración que se enviará al router para activar los mensajes “keep-alive” de TCP para las sesiones Telnet entrantes es la siguiente:

```
service tcp-keepalives-in
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).



## Activar los paquetes “keep-alive” de TCP para sesiones telnet salientes

La Auditoría de seguridad activa los mensajes “keep-alive” de TCP para las sesiones **Telnet** entrantes y salientes, siempre que esto sea posible. La activación de mensajes “keep-alive” de TCP hace que el router genere periódicamente este tipo de mensajes, lo que le permite detectar y abandonar conexiones Telnet interrumpidas.

La configuración que se enviará al router para activar los mensajes “keep-alive” de TCP para las sesiones Telnet salientes es la siguiente:

```
service tcp-keepalives-out
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Activar números de secuencia y marcadores de hora en depuraciones

La Auditoría de seguridad activa los números de secuencia y los marcadores de hora en todos los mensajes de depuración y registro, siempre que esto sea posible. Los marcadores de hora en mensajes de registro y depuración indican la hora y fecha en las que se ha generado el mensaje. Los números de secuencia indican la secuencia en la que se han generado los mensajes con marcadores de hora idénticos. Saber la hora y secuencia en las que se generan los mensajes es una herramienta importante a la hora de diagnosticar ataques potenciales.

La configuración que se enviará al router para activar los marcadores de hora y números de secuencia es la siguiente:

```
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timeout msec
service sequence-numbers
```

## Activar IP CEF

La Auditoría de seguridad activa CEF (Cisco Express Forwarding) o DCEF (Distributed Cisco Express Forwarding), siempre que esto sea posible. Puesto que no es necesario generar entradas de caché cuando el tráfico comienza a llegar a los destinos nuevos, CEF funciona de manera más previsible que otros modos cuando se presentan elevados volúmenes de tráfico dirigidos a varios destinos. Cuando se producen ataques SYN, los routers configurados para CEF funcionan mejor que los routers que utilizan la caché tradicional.

La configuración que se enviará al router para activar CEF es la siguiente:

```
ip cef
```

## Desactivar Gratuitous ARP de IP

La Auditoría de seguridad desactiva las solicitudes Gratuitous ARP (Address Resolution Protocol) de IP siempre que esto sea posible. Un Gratuitous ARP es una difusión ARP en la que las direcciones MAC de origen y destino son iguales. Es utilizado principalmente por los hosts para informar a la red acerca de su dirección IP. Un mensaje Gratuitous ARP tipo “spoof” puede ocasionar el almacenamiento incorrecto de la información de asignación de redes, lo que podría causar un fallo en la red.

Para desactivar Gratuitous ARP, se enviará al router la configuración siguiente:

```
no ip gratuitous-arps
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Definir la longitud mínima de la contraseña a menos de 6 caracteres

La Auditoría de seguridad configura el router para que requiera una longitud mínima de contraseña de seis caracteres, siempre que sea posible. Un método que los atacantes utilizan para obtener contraseñas es intentar todas las combinaciones de caracteres hasta descubrir la contraseña. Con contraseñas de mayor longitud se aumenta exponencialmente la cantidad de combinaciones posibles de caracteres, lo que hace que este método de ataque resulte mucho más difícil.

Este cambio de configuración requerirá que todas las contraseñas del router, incluidas las contraseñas de usuario, activación, secretas, consola, AUX, tty y vty, tengan una longitud de al menos seis caracteres. Este cambio de configuración se realizará solamente si la versión de IOS de Cisco que se ejecuta en el router admite la función de longitud mínima de contraseñas.

La configuración que se enviará al router es la siguiente:

```
security passwords min-length <6>
```

## Definir la proporción de fallos de autenticación a menos de 3 intentos

La Auditoría de seguridad configura el router para bloquear el acceso tras tres intentos incorrectos de inicio de sesión, siempre que esto sea posible. Un método de obtención de contraseñas, denominado ataque “diccionario”, consiste en utilizar software que intenta iniciar una sesión utilizando todas las palabras de un diccionario. Esta configuración bloquea el acceso al router durante un período de 15 segundos tras tres intentos incorrectos de inicio de sesión, lo que desactiva el método de ataque diccionario. Además de bloquear el acceso al router, esta configuración genera un mensaje de registro tras tres intentos incorrectos de inicio de sesión, advirtiendo al administrador de dichos intentos.

La configuración que se enviará al router para bloquear el acceso al mismo tras tres intentos incorrectos de inicio de sesión es la siguiente:

```
security authentication failure rate <3>
```

## Definir la hora TCP Synwait

La Auditoría de seguridad establece el tiempo TCP Synwait en 10 segundos, siempre que esto sea posible. El tiempo TCP Synwait es un valor de gran utilidad para detener ataques SYN de tipo “flooding”, una forma de ataque de denegación de servicio (DoS). Una conexión TCP requiere un procedimiento en tres fases para establecer inicialmente la conexión. El autor envía una solicitud de conexión, el destinatario envía un reconocimiento y, a continuación, el autor envía una aceptación de dicho reconocimiento. Una vez finalizado este saludo en tres fases, se establece la conexión y se inicia la transferencia de datos. Un ataque SYN de tipo “flooding” envía solicitudes repetidas de conexión a un host, pero nunca envía la aceptación de los reconocimientos que completan las conexiones, lo que crea cada vez más conexiones incompletas en el host. Puesto que el búfer para conexiones incompletas es normalmente más pequeño que el búfer para conexiones establecidas, este tipo de ataque puede abrumar y desactivar el host. Al definir el tiempo TCP Synwait en 10 segundos, el router desactivará una conexión incompleta tras 10 segundos. De este modo, se evita la acumulación de conexiones incompletas en el host.

La configuración que se enviará al router para definir el tiempo TCP Synwait en 10 segundos es la siguiente:

```
ip tcp synwait-time <10>
```

## Definir anuncio

La Auditoría de seguridad configura un anuncio de texto siempre que esto sea posible. En algunas jurisdicciones, el procesamiento civil o criminal de los piratas informáticos que entran en los sistemas sin autorización se facilita mucho si se proporciona un anuncio que indique a los usuarios no autorizados que el uso es, efectivamente, no autorizado. En otras jurisdicciones, es posible que no tenga derecho a supervisar las actividades de incluso los usuarios no autorizados, a menos que haya tomado medidas para notificarles de la intención de hacerlo. El anuncio de texto es un método para realizar esta notificación.

La configuración que se enviará al router para crear un anuncio de texto es la siguiente (los valores *<nombre de la compañía>*, *<dirección de correo electrónico del administrador>* y *<número de teléfono del administrador>* se sustituyen con los valores adecuados especificados en la Auditoría de seguridad):

```
banner ~
Authorized access only
This system is the property of <nombre de la compañía>.
Disconnect IMMEDIATELY as you are not an authorized user!
Contact <dirección de correo electrónico del administrador> <número de
teléfono del administrador>.
~
```

## Activar registro

La Auditoría de seguridad activará la creación de registros con marcadores de hora y números de secuencia, siempre que sea posible. Puesto que proporcionan información detallada acerca de los eventos de la red, los registros son muy importantes para el reconocimiento de los eventos de seguridad y la respuesta a ellos. Los marcadores de hora y números de secuencia proporcionan información acerca de la fecha, hora y secuencia en las que se producen los eventos de red.

La configuración que se enviará al router para activar y configurar la creación de registros es la siguiente (los valores *<tamaño del búfer de registro>* y *<dirección IP del servidor de registros>* se sustituyen con los valores adecuados especificados en la Auditoría de seguridad):

```
logging console critical
logging trap debugging
logging buffered <tamaño del búfer de registro>
logging <dirección IP del servidor de registros>
```

## Definir activación de la contraseña secreta

La Auditoría de seguridad configurará el comando **enable secret** de Cisco IOS para proporcionar mayor protección para las contraseñas, siempre que sea posible. El comando **enable secret** se utiliza para definir la contraseña que concede acceso privilegiado de administrador al sistema Cisco IOS. Dicho comando utiliza un algoritmo de cifrado más seguro (MD5) para proteger la contraseña que el anterior comando **enable password**. Este cifrado más seguro es una manera fundamental de proteger la contraseña del router y, por consiguiente, el acceso a la red.

La configuración que se enviará al router para configurar el comando es la siguiente:

```
enable secret <>
```

## Desactivar SNMP

La Auditoría de seguridad desactiva SNMP (Simple Network Management Protocol) siempre que esto sea posible. SNMP es un protocolo de red que permite la recuperación y publicación de datos acerca del rendimiento y de los procesos de la red. Su uso es bastante difundido para la supervisión de routers y, con frecuencia, para los cambios en la configuración de los routers. Sin embargo, la versión 1 del protocolo SNMP, que es la que se utiliza con mayor frecuencia, a menudo representa un riesgo de seguridad por los motivos siguientes:

- Utiliza cadenas de autenticación (contraseñas) denominadas *cadenas de comunidad* que se almacenan y envían a través de la red en forma de texto sin formato.
- La mayoría de las implantaciones SNMP envían dichas cadenas varias veces como parte del sondeo periódico.
- Es un protocolo de transacciones basado en datagramas que es fácil de imitar (spoof).

Puesto que SNMP se puede utilizar para recuperar una copia de la tabla de enrutamiento de redes, además de otra información confidencial, Cisco recomienda desactivarlo si la red no lo necesita. Inicialmente, la Auditoría de seguridad solicitará la desactivación de SNMP.

La configuración que se enviará al router para desactivar el servicio SNMP es la siguiente:

```
no snmp-server
```

## Definir el intervalo del Programador

La Auditoría de seguridad configura el intervalo del Programador del router siempre que esto sea posible. Cuando un router conmuta rápidamente una gran cantidad de paquetes, es posible que se dedique tanto tiempo a responder a las interrupciones de las interfaces de red, que las otras tareas queden sin hacerse. Algunas inundaciones (floods) de paquetes muy rápidas pueden causar esta condición. Es posible que se detenga el acceso de administración al router, lo que puede ser muy peligroso cuando el dispositivo está sometido a un ataque. La definición del intervalo del Programador garantiza que el acceso de administración al router esté siempre disponible al obligar al router a ejecutar procesos del sistema después del intervalo de tiempo especificado, incluso cuando el uso de la CPU se encuentra en un 100%.

La configuración que se enviará al router para definir el intervalo del Programador es la siguiente:

```
scheduler interval 500
```

## Definir asignación del Programador

En los routers que no admiten el comando **scheduler interval**, la Auditoría de seguridad configura el comando **scheduler allocate** siempre que esto sea posible. Cuando un router conmuta rápidamente una gran cantidad de paquetes, es posible que se dedique tanto tiempo a responder a las interrupciones de las interfaces de red, que las otras tareas queden sin hacerse. Algunas inundaciones (floods) de paquetes muy rápidas pueden causar esta condición. Es posible que se detenga el acceso de administración al router, lo que puede ser muy peligroso cuando el dispositivo está sometido a un ataque. El comando **scheduler allocate** garantiza un porcentaje de los procesos de la CPU del router para las actividades distintas de la conmutación de redes como, por ejemplo, los procesos de gestión.

La configuración que se enviará al router para definir el porcentaje de asignación del Programador es la siguiente:

```
scheduler allocate 4000 1000
```

## Definir usuarios

La Auditoría de seguridad garantiza la seguridad de las líneas de consola, AUX, vty y tty al configurar cuentas de usuario Telnet para autenticar el acceso a dichas líneas, siempre que esto es posible. La Auditoría de seguridad mostrará un cuadro de diálogo que permite definir cuentas y contraseñas de usuarios para estas líneas.

## Activar configuración Telnet

La Auditoría de seguridad garantiza la seguridad de las líneas de consola, AUX, vty y tty al implementar las configuraciones siguientes siempre que esto sea posible:

- Configura los comandos **transport input** y **transport output** para definir los protocolos que se utilizarán para establecer la conexión con dichas líneas.
- Define el valor de límite de tiempo EXEC en 10 minutos en las líneas de consola y AUX, lo que cierra la sesión de un usuario administrador para estas líneas tras 10 minutos de inactividad.

La configuración que se enviará al router para garantizar la seguridad de las líneas de consola, AUX, vty y tty es la siguiente:

```
!  
line console 0  
transport output telnet  
exec-timeout 10  
login local  
!  
line AUX 0  
transport output telnet  
exec-timeout 10  
login local  
!  
line vty ...  
transport input telnet  
login local
```



## Activar cambio a NetFlow

La Auditoría de seguridad activa el cambio a [NetFlow](#) siempre que esto sea posible. El cambio a NetFlow es una función de Cisco IOS que mejora el rendimiento del enrutamiento cuando se utilizan listas de control de acceso (ACL) y otras funciones que crean y mejoran la seguridad de la red. NetFlow identifica los flujos de paquetes de red en función de las direcciones IP de origen y destino y de los números de puerto TCP. A continuación, NetFlow puede utilizar solamente el paquete inicial de un flujo para compararlo con las listas de control de acceso y para realizar otras comprobaciones de seguridad, en lugar de tener que utilizar todos los paquetes del flujo de red. Esto mejora el rendimiento, lo que permite sacar el máximo provecho de todas las funciones de seguridad del router.

La configuración que se enviará al router para activar el servicio NetFlow es la siguiente:

```
ip route-cache flow
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Desactivar redireccionamiento IP

La Auditoría de seguridad desactiva los mensajes de redireccionamiento ICMP (Internet Message Control Protocol), siempre que esto sea posible. ICMP admite el tráfico IP al transmitir información acerca de las rutas de acceso, rutas y condiciones de red. Los mensajes de redireccionamiento ICMP indican a un nodo final que utilice un router específico como ruta a un destino en particular. En una red IP que funcione correctamente, un router enviará redireccionamientos solamente a los hosts de sus propias subredes locales, ningún nodo final enviará un redireccionamiento y ningún redireccionamiento se atravesará más de un salto de red. No obstante, un atacante podría infringir estas reglas, ya que algunos ataques se basan en este concepto. La desactivación de los redireccionamientos ICMP no tendrá ningún impacto operativo en la red y elimina este posible método de ataque.

La configuración que se enviará al router para desactivar el servicio de mensajes de redireccionamiento ICMP es la siguiente:

```
no ip redirects
```

## Desactivar ARP Proxy IP

La Auditoría de seguridad desactiva ARP (Address Resolution Protocol) proxy siempre que esto sea posible. La red utiliza ARP para convertir direcciones IP en direcciones MAC. Normalmente, ARP se limita a una sola LAN, pero un router puede funcionar como proxy para las solicitudes ARP, lo que hace que las consultas ARP estén disponibles en varios segmentos LAN. Puesto que rompe la barrera de seguridad de la LAN, el ARP proxy sólo debe utilizarse entre dos LAN con el mismo nivel de seguridad, y sólo cuando sea necesario.

La configuración que se enviará al router para desactivar ARP proxy es la siguiente:

```
no ip proxy-arp
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Desactivar difusión dirigida IP

La Auditoría de seguridad desactiva las difusiones dirigidas por IP siempre que esto sea posible. Una difusión dirigida por IP es un datagrama que se envía a la dirección de difusión de una subred a la que la máquina que realiza el envío no está conectada directamente. La difusión dirigida se enruta a través de la red como un paquete de unidifusión hasta que alcanza la subred de destino, donde se convierte en una difusión de capa de enlace. Debido a la naturaleza de la arquitectura de direcciones IP, solamente el último router de la cadena (el que se conecta directamente a la subred de destino) puede identificar de manera concluyente una difusión dirigida. Las difusiones dirigidas a veces se utilizan por motivos legítimos, pero este tipo de uso no es común fuera del sector de servicios financieros.

Las difusiones dirigidas por IP se utilizan para los comunes y populares ataques “smurf” de denegación de servicio y también pueden utilizarse en ataques relacionados. En un ataque “smurf”, el atacante envía solicitudes de eco ICMP desde una dirección de origen falsificada a una dirección de difusión dirigida, lo que hace que todos los hosts de la subred de destino envíen respuestas al origen falsificado. Al enviar un flujo continuo de este tipo de solicitudes, el atacante puede crear un flujo de respuestas mucho más voluminoso, lo que puede inundar completamente el host cuya dirección se está falsificando.

Al desactivar las difusiones dirigidas por IP, se abandonan las difusiones dirigidas que, de otro modo, se “ampliarían” en difusiones de capa de enlace en dicha interfaz.

La configuración que se enviará al router para desactivar las difusiones dirigidas por IP es la siguiente:

```
no ip directed-broadcast
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Desactivar servicio MOP

La Auditoría de seguridad desactivará MOP (Maintenance Operations Protocol) en todas las interfaces Ethernet siempre que sea posible. MOP se utiliza para proporcionar al router información de configuración cuando se comunica con redes DECNet. MOP es vulnerable a distintos tipos de ataques.

La configuración que se enviará al router para desactivar el servicio MOP en las interfaces Ethernet es la siguiente:

```
no mop enabled
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Desactivar IP de destino inalcanzable

La Auditoría de seguridad desactiva los mensajes de host inalcanzable ICMP (Internet Message Control Protocol), siempre que esto sea posible. ICMP admite el tráfico IP al transmitir información acerca de las rutas de acceso, rutas y condiciones de red. Los mensajes de host inalcanzable ICMP se envían si un router recibe un paquete de no difusión que utiliza un protocolo desconocido o si un router recibe un paquete que no puede entregar al destino final porque no conoce ninguna ruta hacia la dirección de destino. Un atacante puede utilizar dichos mensajes para obtener información de asignación de la red.

La configuración que se enviará al router para desactivar los mensajes de host inalcanzable ICMP es la siguiente:

```
int <all-interfaces>  
no ip unreachable
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Desactivar respuesta de máscara IP

La Auditoría de seguridad desactiva los mensajes de respuesta de máscara ICMP (Internet Message Control Protocol), siempre que esto sea posible. ICMP admite el tráfico IP al transmitir información acerca de las rutas de acceso, rutas y condiciones de red. Los mensajes de respuesta de máscara ICMP se envían cuando un dispositivo de red debe conocer la máscara de subred para una subred determinada en la interred. Dichos mensajes se envían al dispositivo que solicita información mediante los dispositivos que disponen de la información solicitada. Un atacante puede utilizar dichos mensajes para obtener información de asignación de la red.

La configuración que se enviará al router para desactivar los mensajes de máscara ICMP es la siguiente:

```
no ip mask-reply
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Desactivar IP de destino inalcanzable en interfaz NULA

La Auditoría de seguridad desactiva los mensajes de host inalcanzable ICMP (Internet Message Control Protocol), siempre que esto sea posible. ICMP admite el tráfico IP al transmitir información acerca de las rutas de acceso, rutas y condiciones de red. Los mensajes de host inalcanzable ICMP se envían si un router recibe un paquete de no difusión que utiliza un protocolo desconocido o si un router recibe un paquete que no puede entregar al destino final porque no conoce ninguna ruta hacia la dirección de destino. Puesto que la interfaz nula es un receptor de paquetes, los paquetes que se envían allí siempre se descartarán y, si no se desactivan, generarán mensajes de host inalcanzable. En dicho caso, si la interfaz nula se utiliza para bloquear un ataque de denegación de servicio, estos mensajes inundarán la red local. La desactivación de estos mensajes evita esta situación. Además, puesto que todos los paquetes bloqueados se envían a la interfaz nula, un atacante que recibe mensajes de host inalcanzable podría utilizar dichos mensajes para determinar la configuración de la lista de control de acceso (ACL).

Si la interfaz “null 0” se ha configurado en el router, la Auditoría de seguridad enviará al router la configuración siguiente para desactivar los mensajes de host inalcanzable ICMP para los paquetes descartados o los paquetes enrutados hacia la interfaz nula:

```
int null 0
no ip unreachable
```

Esta corrección se puede deshacer. Para saber cómo, haga clic en [Cómo deshacer las correcciones de la Auditoría de seguridad](#).

## Activar RPF unidifusión en todas las interfaces externas

La Auditoría de seguridad activa el envío de la ruta inversa (RPF) de unidifusión en todas las interfaces que se conectan a Internet, siempre que esto sea posible. RPF es una función que obliga al router a comprobar la dirección de origen de todos los paquetes contra la interfaz a través de la cual el paquete ha entrado en el router. Si la interfaz de entrada no es una ruta accesible para la dirección de origen según la tabla de enrutamiento, el paquete se rechazará. Esta verificación de la dirección de origen se utiliza para impedir el [spoofing](#) de IP.

Esto funciona solamente cuando el enrutamiento es simétrico. Si la red se ha diseñado de modo que el tráfico desde el host A hacia el host B normalmente pueda utilizar una ruta distinta que el tráfico desde el host B hacia el host A, siempre fallará la comprobación y la comunicación entre ambos hosts no será posible. Este tipo de enrutamiento asimétrico es común en el núcleo de Internet. Antes de activar esta función, asegúrese de que la red no utiliza enrutamiento asimétrico.

Además, RPF de unidifusión puede activarse solamente cuando la función IP CEF (Cisco Express Forwarding) está activada. La Auditoría de seguridad comprobará la configuración del router para ver si la función IP CEF está desactivada. Si la función IP CEF no está activada, la Auditoría de seguridad recomendará su activación y la activará tras su aprobación. Si la función IP CEF no está activada, mediante la Auditoría de seguridad u otro modo, no se activará RPF de unidifusión.

Para activar RPF de unidifusión, se enviará al router la configuración siguiente para todas las interfaces que se conectan fuera de la red privada (el valor *<interfaz externa>* se sustituye con el identificador de la interfaz):

```
interface <interfaz externa>
ip verify unicast reverse-path
```

## Activar firewall en todas las interfaces externas

Si la imagen de Cisco IOS que se ejecuta en el router incluye un conjunto de funciones de firewall, la Auditoría de seguridad activará **CBAC** (Context-Based Access Control) en el router, siempre que sea posible. CBAC es un componente del conjunto de funciones de firewall de Cisco IOS que filtra los paquetes en función de la información de nivel de aplicación como, por ejemplo, los tipos de comandos que se ejecutan durante la sesión. Por ejemplo, si durante una sesión se detecta un comando no admitido, es posible que se deniegue el acceso al paquete.

CBAC mejora la seguridad para las aplicaciones de TCP y User Datagram Protocol (UDP) que utilizan puertos conocidos, como el puerto 80 para **HTTP** o el puerto 443 para Secure Sockets Layer (**SSL**). Para ello, estudia las direcciones de origen y destino. Sin CBAC, el tráfico de aplicación avanzado sólo se permite mediante la creación de listas de control de acceso (ACL). Este enfoque deja las puertas del firewall abiertas, de modo que la mayoría de los administradores suelen denegar este tipo de tráfico de aplicación. Sin embargo, al activar CBAC, es posible permitir con seguridad el tráfico multimedia y de otras aplicaciones abriendo el firewall según sea necesario y cerrándolo el resto del tiempo.

Para activar CBAC, la Auditoría de seguridad utilizará las pantallas Crear firewall de Cisco SDM para generar una configuración de firewall.

## Definir la clase de acceso en el servicio de servidor HTTP

La Auditoría de seguridad activa el servicio **HTTP** en el router con una clase de acceso, siempre que esto sea posible. El servicio HTTP permite la configuración y supervisión remota mediante un explorador Web. Sin embargo, su capacidad de seguridad es limitada, ya que envía una contraseña de texto plano a través de la red durante el proceso de autenticación. Por lo tanto, la Auditoría de seguridad limita el acceso al servicio HTTP al configurar una clase de acceso que permite el acceso solamente a partir de nodos de red conectados directamente.

La configuración que se enviará al router para activar el servicio HTTP con una clase de acceso es la siguiente:

```
ip http server
ip http access-class <std-acl-num>
!
!HTTP Access-class:Allow initial access to direct connected subnets !
!only
access-list <std-acl-num> permit <inside-network>
access-list <std-acl-num> deny any
```

## Definir la clase de acceso en líneas VTY

La Auditoría de seguridad configura una clase de acceso para las líneas `vtty` siempre que esto sea posible. Puesto que las conexiones `vtty` permiten un acceso remoto al router, deben limitarse a los nodos de red conocidos solamente.

La configuración que se enviará al router para configurar una clase de acceso para las líneas `vtty` es la siguiente:

```
access-list <std-acl-num> permit <inside-network>
access-list <std-acl-num> deny any
```

Además, se aplicará la configuración siguiente a todas las líneas `vtty`:

```
access-class <std-acl-num>
```

## Activar SSH para acceder al router

Si la imagen de Cisco IOS que se ejecuta en el router es una imagen criptográfica (imagen que utiliza el cifrado DES (Data Encryption Standard) de 56 bits y que está sujeta a restricciones de exportación), la Auditoría de seguridad implementará las configuraciones siguientes para garantizar la seguridad del acceso `Telnet` siempre que sea posible:

- Activar `SSH` (Secure Shell) para el acceso `Telnet`. `SSH` aumenta significativamente la seguridad del acceso `Telnet`.
- Definir el valor de límite de tiempo de `SSH` en 60 segundos, lo que obligará a las conexiones `SSH` a desactivarse transcurridos los 60 segundos.
- Definir el número máximo de intentos incorrectos de inicio de sesión `SSH` en dos antes de bloquear el acceso al router.

La configuración que se enviará al router para garantizar la seguridad del acceso y de las funciones de transferencia de archivos es la siguiente:

```
ip ssh time-out 60
ip ssh authentication-retries 2
!
line vty 0 4
transport input ssh
!
```



### Nota

Tras realizar los cambios de configuración mencionados anteriormente, deberá especificar el tamaño de la clave de módulo `SSH` y generar una clave. Para ello, utilice la página [SSH](#).

## Activar AAA

“Cisco IOS Authentication, Authorization, and Accounting” (AAA) es una estructura de arquitectura para configurar un conjunto de tres funciones de seguridad independientes en forma congruente. AAA entrega una forma modular de realizar los servicios de autenticación, autorización y contabilidad.

Cisco SDM ejecutará las siguientes tareas preventivas mientras activa AAA para evitar que se pierda el acceso al router:

- Configure la autenticación y autorización para las líneas VTY.  
Se utilizará la base de datos local tanto para la autorización como para la autenticación.
- Configure la autenticación para una línea de consola  
Se utilizará la base de datos local para la autenticación.
- Modifique la autenticación HTTP para que utilice la base de datos local

## Pantalla Resumen de la configuración

Esta pantalla muestra una lista de todos los cambios de configuración que se enviarán al router, en función de los problemas de seguridad que se han seleccionado para ser corregidos en la pantalla Tarjeta de informes.

## Cisco SDM y AutoSecure de Cisco IOS

AutoSecure es una función de Cisco IOS que, al igual que Cisco SDM, facilita la configuración de las funciones de seguridad en el router para mejorar la protección de la red. Cisco SDM implementa casi todas las configuraciones que ofrece la función AutoSecure.

### Funciones AutoSecure implementadas en Cisco SDM

En esta versión de Cisco SDM se han implementado las siguientes funciones AutoSecure. Para obtener más información sobre estos servicios y funciones, haga clic en los enlaces siguientes:

- [Desactivar SNMP](#)
- [Desactivar el servicio Finger](#)



- Desactivar el servicio PAD
- Desactivar el servicio de pequeños servidores TCP
- Desactivar el servicio del servidor IP bootp
- Desactivar el servicio IP ident
- Desactivar CDP
- Desactivar la ruta de origen IP
- Desactivar redireccionamiento IP
- Desactivar ARP Proxy IP
- Desactivar difusión dirigida IP
- Desactivar servicio MOP
- Desactivar IP de destino inalcanzable
- Desactivar IP de destino inalcanzable en interfaz NULA
- Desactivar respuesta de máscara IP
- Activar el servicio de cifrado de contraseñas
- Desactivar IP de destino inalcanzable en interfaz NULA
- Desactivar IP de destino inalcanzable en interfaz NULA
- Definir la longitud mínima de la contraseña a menos de 6 caracteres
- Activar IP CEF
- Activar firewall en todas las interfaces externas
- Definir usuarios
- Activar registro
- Activar firewall en todas las interfaces externas
- Definir la longitud mínima de la contraseña a menos de 6 caracteres
- Activar firewall en todas las interfaces externas
- Definir usuarios
- Definir usuarios
- Definir usuarios
- Activar RPF unidifusión en todas las interfaces externas
- Activar firewall en todas las interfaces externas

## Funciones AutoSecure no implementadas en Cisco SDM

En esta versión de Cisco SDM no se han implementado las siguientes funciones AutoSecure:

- **Disabling NTP (Desactivación de NTP):** en función de la entrada, AutoSecure desactivará el protocolo NTP (Network Time Protocol) en el caso de que no se necesite. De lo contrario, NTP se configurará con la autenticación MD5. Cisco SDM no admite la desactivación de NTP.
- **Configuring AAA (Configuración de AAA):** si no se ha configurado el servicio Autenticación, autorización y contabilidad (AAA), AutoSecure configura el servicio AAA local y solicita la configuración de una base de datos local de nombres de usuario y contraseñas en el router. Cisco SDM no admite la configuración AAA.
- **Setting SPD Values (Definición de los valores SPD):** Cisco SDM no define los valores Selective Packet Discard (SPD).
- **Enabling TCP Intercepts (Activación de las intercepciones TCP):** Cisco SDM no activa intercepciones TCP.
- **Configuring anti-spoofing ACLs on outside interfaces (Configuración de ACL “anti-spoofing” en las interfaces externas):** AutoSecure crea tres listas de acceso con nombre que se utilizan para impedir direcciones de origen tipo “anti-spoofing”. Cisco SDM no configura estas ACL.

## Funciones AutoSecure implementadas de manera distinta en Cisco SDM

- **Desactivar SNMP:** Cisco SDM desactivará SNMP, pero, a diferencia de AutoSecure, no proporcionará ninguna opción para configurar la versión 3 de SNMP.
- **Activar SSH para acceder al router:** Cisco SDM activará y configurará SSH en imágenes criptográficas de Cisco IOS, pero, a diferencia de AutoSecure, no activará el punto de control de servicio (SCP) ni desactivará otros servicios de acceso y de transferencia de archivos como, por ejemplo, FTP.

# Configuraciones de seguridad que Cisco SDM puede deshacer

En esta tabla figura una lista de configuraciones de seguridad que Cisco SDM puede deshacer.

Configuración de seguridad	CLI equivalente
Desactivar el servicio Finger	no service finger
Desactivar el servicio PAD	no service pad
Desactivar el servicio de pequeños servidores TCP	no service tcp-small-servers no service udp-small-servers
Desactivar el servicio del servidor IP bootp	no ip bootp server
Desactivar el servicio IP ident	no ip identd
Desactivar CDP	no cdp run
Desactivar la ruta de origen IP	no ip source-route
Activar cambio a NetFlow	ip route-cache flow
Desactivar redireccionamiento IP	no ip redirects
Desactivar ARP Proxy IP	no ip proxy-arp
Desactivar difusión dirigida IP	no ip directed-broadcast
Desactivar servicio MOP	no mop enabled
Desactivar IP de destino inalcanzable	int <all-interfaces> no ip unreachable
Desactivar respuesta de máscara IP	no ip mask-reply
Desactivar IP de destino inalcanzable en interfaz NULA	int null 0 no ip unreachable
Activar el servicio de cifrado de contraseñas	service password-encryption
Activar los paquetes “keep-alive” de TCP para sesiones telnet entrantes	service tcp-keepalives-in
Activar los paquetes “keep-alive” de TCP para sesiones telnet salientes	service tcp-keepalives-out
Desactivar Gratuitous ARP de IP	no ip gratuitous arps

# Cómo deshacer las correcciones de la Auditoría de seguridad

Cisco SDM puede deshacer esta corrección de seguridad. Si desea que Cisco SDM quite esta configuración de seguridad, ejecute el Asistente para la auditoría de seguridad. En la ventana Tarjeta de informes, seleccione la opción **Deshacer las configuraciones de seguridad**, coloque una marca de verificación en esta configuración y en las demás configuraciones que desee deshacer y haga clic en **Siguiente**>.

## Pantalla Agregar/Editar una cuenta Telnet/SSH

Esta pantalla permite agregar una nueva cuenta de usuario o editar una existente para el acceso Telnet y [SSH](#) al router.

### Nombre de usuario

En este campo especifique el nombre de usuario para la nueva cuenta.

### Contraseña

En este campo especifique la contraseña para la nueva cuenta.

### Confirmar contraseña

En este campo vuelva a especificar la contraseña de la nueva cuenta para su confirmación. La entrada de este campo debe coincidir con la del campo Contraseña.

# Configurar cuentas de usuario para Telnet/SSH

Esta pantalla permite gestionar las cuentas de usuario que disponen de acceso [Telnet](#) o [SSH](#) (Secure Shell) al router. La tabla de esta pantalla muestra todas las cuentas de usuario Telnet, con el nombre de usuario de la cuenta y asteriscos que representan la contraseña de la cuenta. Tenga en cuenta que esta pantalla sólo aparece si no se ha configurado ninguna cuenta de usuario y, por lo tanto, la tabla siempre estará vacía cuando se muestre inicialmente.

## Casilla de verificación Activar la autorización para Telnet

Seleccione esta casilla para activar el acceso Telnet y SSH al router. Cancele la selección para desactivar el acceso Telnet y SSH al router.

## Agregar... ..

Haga clic en este botón para que aparezca la pantalla Agregar una cuenta de usuario, que permitirá agregar una cuenta asignándole un nombre de usuario y contraseña.

## Editar... ..

Haga clic en una cuenta de usuario de la tabla para seleccionarla y, a continuación, en este botón para que aparezca la pantalla Editar una cuenta de usuario, que permite editar el nombre de usuario y contraseña de la cuenta seleccionada.

## Botón Eliminar

Haga clic en una cuenta de usuario de la tabla para seleccionarla y, a continuación, en este botón para eliminar dicha cuenta.

# Página Enable Secret and Banner (Activar contraseña secreta y anuncio)

Esta pantalla permite especificar una nueva función de activación de contraseña secreta y un anuncio de texto para el router.

La función de activación de contraseña secreta es una contraseña cifrada que proporciona acceso de nivel de administrador a todas las funciones del router. Es fundamental que la contraseña secreta sea segura y difícil de descubrir. La contraseña secreta debe tener una longitud de seis caracteres como mínimo. Se recomienda incluir caracteres tanto alfabéticos como numéricos y no utilizar una palabra que se pueda encontrar en un diccionario o que pueda incluir información personal acerca del usuario que otra persona pudiese adivinar fácilmente.

El anuncio de texto aparecerá cada vez que un usuario se conecte al router mediante [Telnet](#) o [SSH](#). El anuncio de texto es una importante consideración de seguridad ya que se trata de un método para notificar a los usuarios no autorizados que el acceso al router está prohibido. En algunas jurisdicciones, esta advertencia es un requisito para el procesamiento civil o criminal.

## Nueva contraseña

Especifique la nueva contraseña secreta en este campo.

## Volver a especificar la nueva contraseña

Vuelva a especificar la nueva contraseña secreta en este campo para su comprobación.

## Anuncio de inicio de sesión

Especifique el anuncio de texto que desee configurar en el router.

# Página Registro

Esta pantalla permite configurar el registro del router al crear una lista de servidores syslog a los que se enviarán los mensajes de registro y al crear el nivel de registro, el cual determina la gravedad mínima que un mensaje de registro debe tener para que éste se capture.

## Tabla Dirección IP/Nombre de host

Esta tabla muestra una lista de los hosts a los que se enviarán los mensajes de registro del router. Estos hosts deberán ser servidores syslog que pueden capturar y gestionar los mensajes de registro del router.

### Agregar... ..

Haga clic en este botón para ver la pantalla Dirección IP/Nombre de host que permitirá agregar un servidor syslog a la lista mediante la introducción de su dirección IP o nombre de host.

### Editar... ..

Haga clic en un servidor syslog en la tabla para seleccionarlo y, a continuación, en este botón para ver la pantalla Dirección IP/Nombre de host que permitirá editar la dirección IP o nombre de host de dicho servidor syslog.

### Botón Eliminar

Haga clic en un servidor syslog en la tabla para seleccionarlo y, a continuación, en este botón para eliminarlo de la misma.

## Campo Definir el nivel de registro

En este campo, seleccione el nivel mínimo de gravedad que debe tener un mensaje de registro del router para que se capture y envíe a los servidores syslog server de la tabla de esta pantalla. La gravedad de un mensaje de registro se indica con un número del 0 al 7, de modo que los números inferiores indican eventos de mayor gravedad. La descripción de cada nivel de gravedad es la siguiente:

- 0: emergencias  
Sistema inutilizable
- 1: alertas  
Se requiere una acción inmediata
- 2: importante  
Condiciones importantes
- 3: errores  
Condiciones de error
- 4: advertencias  
Condiciones de advertencia
- 5: notificaciones  
Una condición normal pero significativa
- 6: informativo  
Sólo mensajes informativos
- 7: depuraciones  
Mensajes de depuración





# CAPÍTULO 22

## Enrutamiento

---

La ventana Enrutamiento muestra las rutas estáticas configuradas y las rutas configuradas de RIP (Routing Internet Protocol), OSPF (Open Shortest Path First) y EIGRP (Extended Interior Gateway Routing Protocol). En esta ventana puede revisar las rutas, agregar rutas nuevas, o bien editar o eliminar rutas existentes.



### Nota

---

En esta ventana se mostrarán las rutas estáticas y dinámicas configuradas para los túneles GRE sobre IPsec. Si en esta ventana elimina una entrada de enrutamiento que se utiliza para la arquitectura de túneles GRE sobre IPsec, dicha ruta dejará de estar disponible para el túnel.

---

### Enrutamiento estático

#### Red de destino

Se trata de la red a la que la ruta estática proporciona una ruta de acceso.

#### Envío

Se trata de la interfaz o [Dirección IP](#) a través de las cuales deben enviarse los paquetes para que alcancen la red de destino.

#### Opcional

En esta área se muestra si se ha especificado una distancia métrica y si la ruta se ha designado como ruta permanente.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Agregar una ruta estática.	Haga clic en <b>Agregar</b> y cree la ruta estática en la ventana Agregar ruta estática de IP.
Editar una ruta estática.	Seleccione la ruta estática y haga clic en <b>Editar</b> . Modifique la información de ruta en la ventana Editar la ruta estática de IP.  Si la ruta configurada no es compatible con SDM, el botón Editar estará desactivado.
Eliminar una ruta estática.	Seleccione la ruta estática y haga clic en <b>Eliminar</b> . A continuación, confirme la eliminación en la ventana de alerta.
Eliminar todas las rutas estáticas.	Haga clic en <b>Eliminar todos</b> . A continuación, confirme la eliminación en la ventana de alerta.



### Nota

- Si SDM detecta una entrada de ruta estática previamente configurada cuya interfaz de próximo salto se ha configurado como interfaz nula, dicha entrada será de sólo lectura.
- Si SDM detecta una entrada de ruta estática previamente configurada con las opciones “etiqueta” o “nombre”, dicha entrada será de sólo lectura.
- Si está configurando un router Cisco 7000 y la interfaz que utiliza para un próximo salto (next hop) no es compatible, dicha ruta se marcará como de sólo lectura.
- Las entradas de sólo lectura no se pueden modificar ni eliminar mediante SDM.

## Enrutamiento dinámico

Esta parte de la ventana permite configurar rutas dinámicas RIP, OSPF y EIGRP.

### Nombre de elemento

Si no se ha configurado ninguna ruta dinámica, esta columna contiene el texto RIP, OSPF y EIGRP. Si se han configurado una o varias rutas, esta columna contiene los nombres de parámetro para el tipo de enrutamiento configurado.

Protocolo de enrutamiento	Parámetros de configuración
RIP	Versión RIP, Red, Interfaz pasiva
OSPF	ID de proceso
EIGRP	Número de sistema autónomo

### Valor de elemento

Esta columna contiene el texto “Activado” y los valores de configuración cuando se ha configurado el tipo de enrutamiento. Contiene el texto “Desactivado” cuando no se ha configurado ningún protocolo de enrutamiento.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Configurar una ruta RIP.	Seleccione la ficha RIP y haga clic en <b>Editar</b> . A continuación, configure la ruta en la ventana RIP Dynamic Route (Ruta dinámica RIP).
Configurar una ruta OSPF.	Seleccione la ficha OSPF y haga clic en <b>Editar</b> . A continuación, configure la ruta en la ventana que aparece.
Configurar una ruta EIGRP.	Seleccione la ficha EIGRP y haga clic en <b>Editar</b> . A continuación, configure la ruta en la ventana que aparece.

# Agregar ruta estática de IP/Editar la ruta estática de IP

Utilice esta ventana para agregar o editar una ruta estática.

## Red de destino

En estos campos, especifique la información acerca de la dirección de la red de destino.

### Prefijo

Especifique la dirección IP de la red de destino. Si desea obtener más información, consulte [Configuraciones de interfaz disponibles](#).

### Máscara de prefijo

Especifique la máscara de subred de la dirección de destino.

### Convierta esta ruta en la ruta por defecto

Marque esta casilla para convertir esta ruta en la ruta por defecto de este router. Una ruta por defecto envía todos los paquetes salientes desconocidos a través de esta ruta.

## Envío

Especifique cómo enviar los datos a la red de destino.

### Interfaz

Haga clic en **Interfaz** para seleccionar la interfaz del router que envía el paquete a la red remota.

### Dirección IP

Haga clic en **Dirección IP** para especificar la dirección IP del router de próximo salto (next hop) que recibe y envía el paquete a la red remota.

## Opcional

De manera opcional, puede proporcionar una distancia métrica para esta ruta y designarla como ruta permanente.

### Distancia métrica para esta ruta

Especifique el valor métrico que debe indicarse en la tabla de enrutamiento. Los valores válidos son de 1 a 255.

### Ruta permanente

Marque esta casilla para convertir esta entrada de ruta estática en una ruta permanente. Las rutas permanentes no se eliminan, incluso si se desactiva la interfaz o el router no puede comunicarse con el router siguiente.

# Agregar/Editar una ruta RIP

Utilice esta ventana para agregar o editar una ruta de RIP (Routing Internet Protocol).

## Versión RIP

Los valores disponibles son RIP versión 1, RIP versión 2 y Por defecto. Seleccione la versión compatible con la imagen de Cisco IOS que ejecuta el router. Si selecciona la versión 1, el router envía paquetes RIP versión 1 y puede recibir paquetes de versión 1. Si selecciona la versión 2, el router envía paquetes RIP versión 2 y puede recibir paquetes de versión 2. Si selecciona la opción Por defecto, el router envía paquetes de versión 1 y puede recibir paquetes RIP versión 1 y versión 2.

## Lista de redes IP

Especifique las redes en las que desea activar RIP. Haga clic en **Agregar** para agregar una red. Haga clic en **Eliminar** para eliminar una red de la lista.

## Lista de interfaces disponibles

Esta lista muestra las interfaces disponibles.

## Convierta la interfaz en pasiva

Si no desea que la interfaz envíe actualizaciones a la interfaz vecina, marque la casilla **Convierta la interfaz en pasiva** que aparece junto a la misma. Sin embargo, la interfaz seguirá recibiendo actualizaciones de enrutamiento.

# Agregar o editar una ruta OSPF

Utilice esta ventana para agregar o editar una ruta OSPF (Open Shortest Path First).

## ID de proceso OSPF

Este campo se puede editar cuando se activa OSPF por primera vez y se desactiva una vez activado el enrutamiento OSPF. El ID de proceso se utiliza para que los demás routers puedan identificar el proceso de enrutamiento OSPF del router.

## Lista de redes IP

Especifique las redes hacia las que desea crear rutas. Haga clic en **Agregar** para agregar una red. Haga clic en **Eliminar** para eliminar una red de la lista.

### Red

La dirección de la red de destino para esta ruta. Si desea obtener más información, consulte [Configuraciones de interfaz disponibles](#).

### Máscara

La máscara de subred que se utiliza en dicha red.

### Área

El número de áreas OSPF para dicha red. Cada router de una determinada área OSPF mantiene una base de datos topológica de dicha área.



#### Nota

---

Si SDM detecta un enrutamiento OSPF previamente configurado que incluye comandos de “área”, la tabla Lista de redes IP será de sólo lectura y no se podrá modificar.

---

## Lista de interfaces disponibles

Esta lista muestra las interfaces disponibles.

## Convierta la interfaz en pasiva

Si no desea que la interfaz envíe actualizaciones a la interfaz vecina, marque la casilla **Convierta la interfaz en pasiva** que aparece junto a la misma. Sin embargo, la interfaz seguirá recibiendo actualizaciones de enrutamiento.

## Agregar

Haga clic en **Agregar** para proporcionar una dirección IP, una máscara de red y un número de área en la ventana Dirección IP.

## Editar

Haga clic en **Editar** para editar la dirección IP, la máscara de red o el número de área en la ventana Dirección IP.

# Agregar o editar una ruta EIGRP

Utilice esta ventana para agregar o eliminar una ruta de EIGRP (Extended IGRP).

## Número de sistema autónomo

El número de sistema autónomo se utiliza para que otros router puedan identificar el proceso de enrutamiento EIGRP del router.

## Lista de redes IP

Especifique las redes hacia las que desea crear rutas. Haga clic en **Agregar** para agregar una red. Haga clic en **Eliminar** para eliminar una red de la lista.

## Lista de interfaces disponibles

Esta lista muestra las interfaces disponibles.

## Convierta la interfaz en pasiva

Si no desea que la interfaz envíe actualizaciones a la interfaz vecina, marque la casilla **Convierta la interfaz en pasiva** que aparece junto a la misma. La interfaz no recibirá ni enviará actualizaciones de enrutamiento.



### Precaución

---

Al convertir una interfaz en pasiva, EIGRP suprime el intercambio de paquetes “hello” entre los routers, lo que resulta en la pérdida de su relación de vecino. De este modo, no solamente se impide el anuncio de actualizaciones de enrutamiento, sino que también se suprimen las actualizaciones de enrutamiento entrantes.

---

## Agregar

Haga clic en **Agregar** para agregar una dirección IP de red de destino a la lista de redes.

## Eliminar

Seleccione una dirección IP y haga clic en **Eliminar** para quitar una dirección IP de la lista de redes.





# CAPÍTULO 23

## Traducción de direcciones de red

---

**NAT** (Network Address Translation) es una forma robusta de traducir direcciones que amplía las capacidades de creación de direcciones al proporcionar traducciones de direcciones estáticas y dinámicas. NAT permite que un host que no dispone de una dirección IP registrada válida se comunique con otros hosts a través de Internet. Los hosts podrán utilizar direcciones privadas o direcciones asignadas a otra empresa; en cualquiera de los casos, NAT permite seguir utilizando estas direcciones no preparadas para Internet pero aún permitir la comunicación con hosts a través de Internet.

## Asistentes de traducción de direcciones de la red

Es posible utilizar un asistente para guiarle en la creación de una regla de Traducción de direcciones de red (**NAT**). Seleccione uno de los siguientes asistentes:

- NAT básica

Elija el asistente de NAT básica si desea conectar su red a Internet (o al exterior) y su red tiene hosts, pero no servidores. Observe el diagrama de muestra que aparece a la derecha cuando se selecciona **NAT Básica**. Si su red está compuesta de sólo PC que necesitan acceso a Internet, seleccione **NAT Básica** y haga clic en el botón **Iniciar**.

- NAT avanzada

Seleccione el Asistente de NAT Avanzada si desea conectar su red a Internet (o al exterior) y su red tiene hosts y servidores, y los servidores deben ser accesibles a los hosts exteriores (hosts de Internet). Observe el diagrama de muestra que aparece a la derecha cuando se selecciona **NAT Avanzada**. Si su red tiene servidores de correo electrónico, servidores Web u otro tipo de servidores y se desea que acepten conexiones desde Internet, seleccione **NAT avanzada** y haga clic en el botón **Iniciar**.

**Nota**

---

Si no desea que sus servidores acepten conexiones desde Internet, es posible utilizar el Asistente de NAT Básica.

---

## Asistente de NAT básica: Bienvenido

La ventana de bienvenida de NAT Básica muestra cómo el asistente le guiará a través de la configuración de NAT para conectar una o más LAN, pero no servidores, a Internet.

## Asistente de NAT básica: Conexión

### Elija una interfaz

En el menú desplegable, seleccione la interfaz que se conecta a Internet. Se trata de la interfaz WAN del router.

### Seleccionar redes

La lista de redes disponibles muestra las redes conectada a su router. Seleccione qué redes compartirán la interfaz WAN en la configuración de NAT que se determine. Para seleccionar una red, marque su casilla de verificación en la lista de redes disponibles.

**Nota**

---

No seleccione una red conectada a la interfaz WAN configurada en esta configuración NAT. Elimine esa red de la configuración de NAT desmarcando su casilla de verificación.

---

La lista muestra la siguiente información para cada red:

- Es el intervalo de direcciones IP asignado a la red
- Interfaz LAN de la red
- Comentarios especificados acerca de la red

Para eliminar una red de la configuración de NAT, desmarque su casilla de verificación.

**Nota**

Si Cisco SDM detecta un conflicto entre la configuración NAT y la configuración VPN existente para la interfaz WAN, informará por medio de un cuadro de diálogo después de que usted haga clic en **Siguiente**.

## Resumen

Esta ventana muestra la configuración NAT que se creó, y permite que esta configuración se guarde. El resumen aparecerá en forma similar a lo siguiente:

Interfaz que está conectada con la Internet o con su proveedor de servicios de Internet:

```
FastEthernet0/0
```

Intervalos de direcciones IP que comparten la conexión a Internet:

```
de 108.1.1.0 a 108.1.1.255
```

```
de 87.1.1.0 a 87.1.1.255
```

```
de 12.1.1.0 a 12.1.1.255
```

```
de 10.20.20.0 a 10.20.20.255
```

Si se utilizó el Asistente de NAT Avanzada, también es posible ver información adicional similar a lo siguiente:

Reglas NAT para servidores:

```
Traducir 10.10.10.19 TCP puerto 6080 a una dirección IP de la  
interfaz de FastEthernet0/0 TCP puerto 80
```

```
Traducir 10.10.10.20 TCP puerto 25 a 194.23.8.1 TCP puerto 25
```

## Asistente de NAT avanzada: Bienvenido

La ventana de bienvenida de NAT Avanzada muestra cómo el asistente le guiará a través de la configuración de NAT para conectar sus LAN o servidores, a Internet.

## Asistente de NAT avanzada: Conexión

### Elija una interfaz

En el menú desplegable, seleccione la interfaz que se conecta a Internet. Se trata de la interfaz WAN del router.

### Direcciones IP públicas adicionales

Haga clic en **Agregar** para especificar las direcciones IP públicas que son de su propiedad. Podrá asignar esta dirección IP a servidores de su red que desee que estén disponible desde Internet.

Para eliminar una dirección IP de esta lista, selecciónela y haga clic en **Eliminar**.

### Agregar dirección IP

Especifique una dirección IP pública que sea de su propiedad. Podrá asignar esta dirección IP a un servidor de su red que desee que esté disponible desde Internet.

## Asistente de NAT avanzada: Redes

### Seleccionar redes

La lista de redes disponibles muestra las redes conectada a su router. Seleccione qué redes compartirán la interfaz WAN en la configuración de NAT que se determine. Para seleccionar una red, marque su casilla de verificación en la lista de redes disponibles.

**Nota**

No seleccione una red conectada a la interfaz WAN configurada en esta configuración NAT. Elimine esa red de la configuración de NAT desmarcando su casilla de verificación.

La lista muestra la siguiente información para cada red:

- Es el intervalo de direcciones IP asignado a la red
- Interfaz LAN de la red
- Comentarios especificados acerca de la red

Para eliminar una red de la configuración de NAT, desmarque su casilla de verificación.

Para agregar a la lista una red no conectada directamente a su router, haga clic en **Agregar redes**.

**Nota**

---

Si Cisco SDM no permite que se marque la casilla de verificación al lado de una red para la que desea configurar una regla NAT, la interfaz asociada con la red ya se ha designado como una interfaz NAT. Este estado se indicará por medio de la palabra *Designada* en la columna Comentarios. Si desea configurar una regla NAT para esa interfaz, salga del Asistente, haga clic en la ficha **Editar NAT**, y luego, en **Designar interfaces NAT** y desmarque la interfaz. Luego, vuelva al Asistente y configure la regla NAT.

---

## Agregar redes

Es posible agregar una red a la lista de redes que están disponibles en el Asistente de NAT avanzada. Es necesario tener la dirección IP y la máscara de red. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

### Dirección IP

Especifique la dirección IP de la red.

### Máscara de subred

Especifique la máscara de subred de la red en este campo, o seleccione el número de bits de subred del campo ubicado a la derecha. La máscara de subred indica al router cuáles bits de la dirección IP designan la dirección de la red y qué bits designan la dirección del host.

## Asistente de NAT avanzada: Direcciones IP públicas del servidor

Esta ventana permite traducir las direcciones IP públicas a direcciones IP privadas de servidores internos que usted desee que estén disponibles desde Internet.

Esta lista muestra las direcciones IP y los puertos privados (si es que se usan) y las direcciones IP y puertos públicos (si es que se usan) a las que están traducidas.

Para reorganizar la lista según las direcciones IP privadas, haga clic en el encabezado de la columna **Dirección IP privada**. Para reorganizar la lista según las direcciones IP públicas, haga clic en el encabezado de la columna **Dirección IP pública**.

### Botón Agregar

Para agregar una regla de traducción para un servidor, haga clic en **Agregar**.

### Botón Editar

Para editar una regla de traducción para un servidor, selecciónela de la lista y haga clic en **Editar**.

### Botón Eliminar

Para eliminar una regla de traducción, selecciónela de la lista y haga clic en **Eliminar**.

## Agregar o editar Regla de traducción de direcciones

En esta ventana es posible especificar o editar la información de traducción de direcciones IP para un servidor.

### Dirección IP privada

Especifique la dirección IP que utiliza el servidor en su red interna. Se trata de una dirección IP que no puede usarse, externamente, en Internet.

## Dirección IP pública

En el menú desplegable, seleccione la dirección IP pública a la que se traducirá la dirección IP privada del servidor. Las direcciones IP que aparecen en el menú desplegable incluyen la dirección IP de la interfaz WAN del router y todas las direcciones IP públicas que sean de su propiedad y que se especificaron en la ventana de conexiones (consulte [Asistente de NAT avanzada: Conexión](#)).

## Tipo de servidor

Seleccione uno de los siguientes tipos de servidor del menú desplegable:

- Servidor Web  
Un host http que atiende páginas HTML y de otro tipo orientado a Internet.
- Servidor de correo electrónico  
Un servidor SMTP para enviar correos por Internet.
- Otros  
Un servidor que no es un servidor Web ni un servidor de correo electrónico, pero que necesita traducción de puertos para proporcionar servicios. Esta opción activa el campo Puerto traducido y el menú desplegable Protocolo.

Si no selecciona un tipo de servidor, todo el tráfico destinado a la dirección IP pública que seleccione par el servidor se destinará a ella, y no se realizará la traducción del puerto.

## Puerto original

Especifique el número del puerto que utiliza el servidor para aceptar solicitudes de servicio desde la red interna.

## Puerto traducido

Especifique el número del puerto que utiliza el servidor para aceptar solicitudes de servicio desde Intenet.

## Protocolo

Seleccione **TCP** o **UDP** para el protocolo que utiliza el servidor con los puertos originales y traducidos.

## Asistente de NAT avanzada: Conflicto ACL

Si aparece esta ventana, Cisco SDM ha detectado un conflicto entre la configuración NAT y una ACL existente en la interfaz WAN. Esta ACL puede ser parte de una configuración de firewall, una configuración de VPN, o la configuración de otra función.

Seleccione modificar la configuración NAT para eliminar el conflicto, o seleccione *no* modificar la configuración NAT. Si elige *no* modificar la configuración NAT, el conflicto puede hacer que otras funciones que estén configuradas dejen de funcionar.

### Ver detalles

Haga clic en el botón **Ver detalles** para ver las modificaciones propuestas a la configuración NAT para resolver el conflicto. Este botón no aparece con todos los conflictos de funciones.

### Detalles

Esta ventana muestra los cambios que Cisco SDM realizará a la configuración NAT para resolver los conflictos entre NAT y otra función configurada en la misma interfaz.

## Reglas de traducción de direcciones de la red

La ventana Reglas de traducción de direcciones de la red permite ver reglas [NAT](#) y los conjuntos de direcciones, así como establecer los límites de tiempo para la traducción. Desde esta ventana también puede designar interfaces como internas o externas.

Para obtener más información acerca de NAT, siga el enlace [Información adicional acerca de NAT](#).



## Designar interfaces NAT

Haga clic para designar interfaces como internas o externas. NAT utiliza las designaciones interna o externa como referencia al interpretar las reglas de traducción. Las interfaces internas son aquellas conectadas a las redes privadas que atiende el servidor. Las interfaces externas se conectan a la WAN o a Internet. Las interfaces designadas como internas y externas se muestran por encima de la lista de regla NAT.

## Conjuntos de direcciones

Haga clic en este botón para configurar o modificar los conjuntos de direcciones. Los conjuntos de direcciones se utilizan con la traducción de direcciones dinámicas. El router puede asignar direcciones dinámicamente desde el conjunto, a medida que se necesiten. Cuando una dirección ya no se necesita, se devuelve al conjunto.

## Límites de tiempo para la traducción

Cuando se configura NAT dinámica, las entradas de traducción tienen un período de límite de tiempo después del cual vencen y se depuran de la tabla de traducciones. Haga clic en este botón para configurar los valores de límite de tiempo para las entradas de traducción NAT y otros valores.

## Reglas de traducción de direcciones de la red

En esta área se muestran las interfaces designadas como internas y externas y las reglas NAT que se han configurado.

### Interfaces internas

Las interfaces internas son aquellas que se conectan a las redes privadas a las que el router presta servicio. NAT utiliza la designación “interna” a la hora de interpretar la regla de traducción NAT. Para designar interfaces internas, haga clic en **Designar interfaces NAT**.

### Interfaces externas

Las interfaces externas son las interfaces de router que se conectan a la WAN o a Internet. NAT utiliza la designación “externa” a la hora de interpretar la regla de traducción NAT. Para designar interfaces externas, haga clic en **Designar interfaces NAT**.

**Dirección original**

La dirección o conjunto de direcciones privadas que se utilizan en la LAN.

**Dirección traducida**

La dirección o intervalo de direcciones legales que se utilizan en Internet o en la red externa.

**Tipo de regla**

Las reglas son reglas de traducción de direcciones estáticas o reglas de traducción de direcciones dinámicas.

La **traducción de direcciones estáticas** permite que los hosts con direcciones privadas accedan a Internet y sean públicamente accesibles desde Internet. Asigna estáticamente una dirección IP privada a una dirección pública o global. Si deseara proporcionar una traducción estática a diez direcciones privadas, crearía una regla estática independiente para cada dirección.

**Traducción de direcciones dinámicas.** Existen dos métodos de creación de direcciones dinámicas mediante NAT. Un método asigna varias direcciones privadas a una sola dirección pública y los números de puerto de las sesiones de host para determinar el host al que se debe enrutar el tráfico de vuelta. El segundo método utiliza conjuntos de direcciones con nombre. Dichos conjuntos de direcciones contienen direcciones públicas. Cuando un host con una dirección privada necesita establecer una comunicación fuera de la LAN, obtiene una dirección pública desde este conjunto. Cuando ya no la necesite, la dirección se devuelve al conjunto.

**Clonar entrada seleccionada al agregar**

Si desea utilizar una regla existente como base para una nueva regla que desea crear, seleccione la regla y esta casilla de verificación. Al hacer clic en **Agregar**, las direcciones de la regla seleccionada aparecen en la ventana Agregar regla de traducción de direcciones. Puede modificar dichas direcciones para obtener las que necesite para la nueva regla, en lugar de escribir la dirección completa en cada campo.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
<p>Designar las interfaces internas y externas.</p> <p>Para que el router realice el proceso NAT, debe asignar al menos una interfaz interna y otra externa.</p>	<p>Haga clic en <b>Designar interfaces NAT</b> y designe las interfaces como internas o externas en la ventana Configuración de la interfaz NAT. Las interfaces también pueden designarse como internas o externas en la ventana Interfaces y conexiones.</p>
<p>Agregar, modificar o eliminar un conjunto de direcciones.</p> <p>Las reglas dinámicas pueden utilizar conjuntos de direcciones para asignar direcciones a los dispositivos a medida que se necesiten.</p>	<p>Haga clic en <b>Conjuntos de direcciones</b> y configure la información del conjunto de direcciones en el cuadro de diálogo.</p>
<p>Fijar el límite de tiempo de traducción.</p>	<p>Haga clic en <b>Límites de tiempos de traducción</b>, y fije el límite de tiempo en la ventana Límites de tiempo de traducción.</p>
<p>Agregar una regla NAT.</p>	<p>Haga clic en <b>Agregar</b> y cree la regla NAT en la ventana Agregar regla de traducción de direcciones.</p> <p>Si desea utilizar una regla NAT existente como plantilla para la nueva regla, seleccione la regla, haga clic en <b>Clonar entrada seleccionada al agregar</b> y, a continuación, en <b>Agregar</b>.</p>
<p>Editar una regla NAT.</p>	<p>Seleccione la regla NAT que desee modificar, haga clic en <b>Editar</b> y modifique la regla en la ventana Editar regla de traducción de direcciones.</p>
<p>Eliminar una regla NAT.</p>	<p>Seleccione la regla NAT que desea eliminar y haga clic en <b>Eliminar</b>. Deberá confirmar la eliminación de la regla en el cuadro de advertencia que aparece.</p>

Si desea:	Haga lo siguiente:
<p>Ver o editar mapas de rutas.</p> <p>Si se han configurado conexiones de red privada virtual (VPN) en el router, las direcciones IP locales de la VPN deben protegerse contra la traducción NAT. Si se ha configurado tanto VPN como NAT, Administrador del dispositivo de seguridad de Cisco) (Cisco SDM) crea mapas de ruta para proteger las direcciones IP en una VPN e impedir que se traduzcan. Adicionalmente, los mapas de rutas pueden configurarse usando la interfaz de línea de comandos (CLI). Es posible visualizar los mapas de rutas configurados y editar la regla de acceso que utilizan.</p>	<p>Haga clic en <b>Ver MAPA de ruta</b>.</p>
<p>Ver cómo realizar tareas de configuración relacionadas.</p>	<p>Consulte uno de los procedimientos siguientes:</p> <ul style="list-style-type: none"> <li>• <a href="#">¿Cómo se configura el paso de NAT (NAT Passthrough) para una VPN?</a></li> <li>• <a href="#">¿Cómo se configura NAT en una interfaz no admitida?</a></li> <li>• <a href="#">¿Cómo se configura el paso de NAT (NAT Passthrough) para un firewall?</a></li> </ul>



**Nota**

Muchas condiciones hacen que las reglas NAT configuradas previamente aparezcan como de sólo lectura en la lista de Reglas de traducción de Direcciones de red. Las reglas NAT de sólo lectura no pueden editarse. Para obtener más información, consulte el tema de ayuda [Motivos por los cuales Cisco SDM no puede modificar una regla NAT](#).

## Designar interfaces NAT

Utilice esta ventana para designar las interfaces internas y externas que desee utilizar en las traducciones NAT. [NAT](#) utiliza las designaciones internas y externas a la hora de interpretar reglas de traducción, ya que las traducciones se realizan desde el interior hacia el exterior o desde el exterior hacia el interior.

Una vez designadas, estas interfaces se utilizan en todas las reglas de traducción NAT. Las interfaces designadas aparecen encima de la lista Reglas de traducción en la ventana NAT principal.

### Interfaz

En esta columna se indican todas las interfaces de router.

### Interna (fiable)

Active esta opción para designar una interfaz como interna. Normalmente, las interfaces internas se conectan a la LAN a la que presta servicio el router.

### Externa (no fiable)

Active esta opción para designar una interfaz como externa. Normalmente, las interfaces externas se conectan a la WAN de la empresa o a Internet.

## Configuración del límite de tiempo para la traducción

Cuando se configuran reglas de traducción NAT dinámicas, las entradas de traducción disponen de un período de límite de tiempo después del cual vencen y se depuran de la tabla de traducciones. Establezca los valores de límite de tiempo para las distintas traducciones en esta ventana.

### Límite de tiempo de DNS

Especifique el número de segundos después del cual se agotará el tiempo de conexión de los servidores [DNS](#).

### Límite de tiempo de ICMP

Especifique el número de segundos después del que expira el límite de tiempo de los flujos de **ICMP** (Internet Control Message Protocol). Por defecto, son 60 segundos.

### Límite de tiempo de PPTP

Especifique el número de segundos después del que expira el límite de tiempo de los flujos de **PPTP** (Point-to-Point Tunneling Protocol) de NAT. Por defecto, son 86400 segundos (24 horas).

### Límite de tiempo de la NAT dinámica

Especifique el número máximo de segundos durante el cual deben permanecer activas las traducciones NAT dinámicas.

### Número máximo de entradas de NAT

Especifique el número máximo de entradas de NAT en la tabla de traducciones.

### Límites de tiempo del flujo de UDP

Especifique el número de segundos durante el cual deben permanecer activas las traducciones para los flujos del protocolo **UDP** (User Datagram Protocol). El valor por defecto es de 300 segundos (5 minutos).

### Límites de tiempo del flujo de TCP

Especifique el número de segundos durante el cual deben permanecer activas las traducciones para los flujos del protocolo **TCP** (Transmission Control Protocol). Por defecto, son 86400 segundos (24 horas).

### Botón Restablecer

Si se hace clic en este botón, se restablecen los parámetros de límite de tiempo a sus valores por defecto.

## Editar mapa de ruta

Cuando se hayan configurado tanto VPN como NAT en un router, los paquetes que normalmente satisfacen los criterios de una regla IPsec no lo harán si NAT traduce sus direcciones IP. En este caso, la traducción NAT provocará el envío de los paquetes sin que éstos se cifren. Cisco SDM puede crear mapas de ruta para impedir que NAT traduzca las direcciones IP que se deseen conservar.

Aunque Cisco SDM sólo crea mapas de ruta para limitar la acción de NAT, dichos mapas también se pueden utilizar para otros objetivos. Si se han creado mapas de ruta mediante el CLI, éstos también aparecerán en esta ventana.

### Nombre

El nombre de este mapa de ruta.

### Entradas del mapa de ruta

Este cuadro proporciona una lista de las entradas del mapa de ruta.

#### Nombre

El nombre de la entrada del mapa de ruta.

#### Núm. secuencia

El número de secuencia del mapa de ruta.

#### Acción

Los mapas de ruta que crea Cisco SDM se configuran con la palabra clave **permit**. Si este campo contiene el valor **deny**, esto significa que el mapa de ruta se ha creado mediante el CLI.

#### Listas de acceso

Las listas de acceso que especifican el tráfico al que se aplica este mapa de ruta.

### Para editar una entrada del mapa de ruta

Seleccione la entrada, haga clic en **Editar** y modifique la entrada en la ventana Editar entrada del mapa de ruta.

## Editar entrada del mapa de ruta

Utilice esta ventana para editar la lista de acceso especificada en una entrada del mapa de ruta.

### Nombre

Campo de sólo lectura que contiene el nombre de la entrada del mapa de ruta.

### Núm. secuencia

Campo de sólo lectura que contiene el número de secuencia del mapa de ruta. Cuando Cisco SDM crea un mapa de ruta, le asigna automáticamente un número de secuencia.

### Acción

Puede ser **permit** o **deny**. Los mapas de ruta que crea Cisco SDM se configuran con la palabra clave **permit**. Si este campo contiene el valor **deny**, esto significa que el mapa de ruta se ha creado mediante el CLI.

### Listas de acceso

Esta área muestra las listas de acceso asociadas con esta entrada. El mapa de ruta utiliza estas listas de acceso para determinar el tráfico que debe proteger contra la traducción NAT.

### Para editar una lista de acceso en una entrada del mapa de ruta

Seleccione la lista de acceso y haga clic en **Editar**. A continuación, modifíquela en las ventanas que aparecen.



## Conjuntos de direcciones

La ventana Conjuntos de direcciones muestra los conjuntos de direcciones configurados que se pueden utilizar en la traducción NAT dinámica.

### Nombre del conjunto

Este campo contiene el nombre del conjunto de direcciones. Utilice este nombre para hacer referencia al conjunto al configurar una regla de NAT dinámica.

### Dirección

Este campo contiene el intervalo de direcciones IP del conjunto. Los dispositivos cuyas direcciones IP coinciden con la regla de acceso especificada en la ventana Agregar regla de traducción de direcciones obtendrán direcciones IP privadas de este conjunto.

### ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Agregar un conjunto de direcciones a la configuración del router.	Haga clic en <b>Agregar</b> y configure el conjunto en la ventana Agregar conjunto de direcciones.  Si desea utilizar un conjunto existente como plantilla para el nuevo conjunto, seleccione el conjunto existente, active la opción <b>Clonar entrada seleccionada al agregar</b> y, a continuación, haga clic en <b>Agregar</b> .
Editar un conjunto de direcciones existente.	Seleccione la entrada del conjunto, haga clic en <b>Editar</b> y modifique la configuración del conjunto en la ventana Editar conjunto de direcciones.
Eliminar un conjunto de direcciones.	Seleccione la entrada del conjunto, haga clic en <b>Eliminar</b> y confirme la eliminación en el cuadro de advertencia que aparece.



#### Nota

Si Cisco SDM detecta un conjunto de direcciones NAT previamente configurado que utiliza la palabra clave “type”, dicho conjunto de direcciones será de sólo lectura y no se podrá modificar.

## Agregar/Editar conjunto de direcciones

Utilice esta ventana para especificar un conjunto de direcciones para la traducción de direcciones dinámicas, una dirección para la traducción de direcciones de puerto (PAT) o un conjunto de rotación del balance de carga TCP.

### Nombre del conjunto

Especifique el nombre del conjunto de direcciones.

### Traducción de direcciones de puerto (PAT)

Existen varias ocasiones en las que la mayoría de las direcciones del conjunto estarán asignadas y que el conjunto de direcciones IP estará casi agotado. Cuando esto suceda, es posible utilizar [PAT](#) con una única dirección IP para satisfacer las solicitudes adicionales de direcciones IP. Si desea que el router utilice PAT cuando el conjunto de direcciones esté a punto de agotarse, active esta casilla de verificación.

### Dirección IP

En el campo izquierdo, especifique la dirección IP con el número más bajo del intervalo y, en el derecho, la dirección IP con el número más alto. Para obtener más información, consulte [Configuraciones de interfaz disponibles](#).

### Máscara de red

Especifique la máscara de subred o el número de bits de red que indican cuántos bits de las direcciones IP son bits de red.

## Agregar o editar regla de traducción de direcciones estáticas: De interna a externa

Utilice este tema de ayuda cuando haya seleccionado **Desde adentro hacia fuera** en la ventana **Agregar Regla de traducción de direcciones estáticas** o en la ventana **Editar Regla de traducción de direcciones estáticas**.

Utilice esta ventana para agregar o editar una regla de traducción de direcciones estáticas. Si se está editando una regla, se desactivan el tipo de regla (estática o dinámica) y su dirección. Si necesita cambiar estos valores, elimine la regla y vuelva a crearla con la configuración deseada.

Dos tipos de traducciones de direcciones estáticas utilizan NAT: estática simple y estática ampliada.



### Nota

---

Si desea crear una regla NAT que traduzca las direcciones de los dispositivos que forman parte de una VPN, Cisco SDM le solicitará permiso para crear un mapa de ruta destinado a proteger dichas direcciones contra la traducción mediante NAT. Si permite que NAT traduzca las direcciones de los dispositivos de una VPN, sus direcciones traducidas no satisfarán la regla IPsec en la política IPsec, y el tráfico se enviará sin cifrar. Para ver los mapas de ruta creados por Cisco SDM o creados mediante la CLI, haga clic en el botón **Ver mapas de ruta** de la ventana NAT.

---

### Dirección

En este tema de ayuda se describe cómo utilizar los campos **Agregar regla de traducción de direcciones** cuando se seleccione la opción **De interna a externa**.

#### De interna a externa

Seleccione esta opción si desea traducir direcciones privadas de la LAN en direcciones legales en Internet o en la intranet de su empresa. Se recomienda seleccionar esta opción si utiliza direcciones privadas en la LAN que no son exclusivas globalmente en Internet.

### Traducir desde la interfaz

Esta área muestra las interfaces desde las que llegan al router los paquetes que necesitan traducción de direcciones. Proporciona campos que permiten especificar la dirección IP de un solo host, o una dirección de red y máscara de subred que representan los hosts de una red.

### Interfaces internas

Si selecciona **De interna a externa** para la opción Dirección, esta área muestra una lista de las interfaces internas designadas.



#### Nota

---

Si en esta área no se incluye ningún nombre de interfaz, cierre la ventana Agregar regla de traducción de direcciones, haga clic en **Designar interfaces NAT** en la ventana NAT y designe las interfaces de router como internas o externas. A continuación, regrese a esta ventana y configure la regla NAT.

---

### Dirección IP

Realice uno de los procedimientos siguientes:

- Si desea crear una asignación estática de uno-a-uno entre la dirección de un solo host y una dirección traducida, denominada *dirección global interna*, especifique la dirección IP para dicho host. No especifique ninguna máscara de subred en el campo Máscara de red.
- Si desea crear asignaciones *n-a-n* entre las direcciones privadas de una subred y las direcciones globales internas correspondientes, especifique cualquier dirección válida de la subred cuyas direcciones desee traducir y especifique una máscara de red en el campo siguiente.

### Máscara de red

Si desea que Cisco SDM traduzca las direcciones de una subred, especifique la máscara para esa subred. Cisco SDM determina el número de red y subred y el conjunto de direcciones que necesitan traducción desde la dirección IP y la máscara que usted indique.

## Traducir a la interfaz

Esta área muestra las interfaces desde las que salen del router los paquetes con las direcciones traducidas. También Proporciona campos para especificar la dirección traducida y otra información.

### Interfaces externas

Si selecciona **De interna a externa** para la opción Dirección, esta área muestra las interfaces externas designadas.

### Tipo

- Seleccione **Dirección IP** si desea que la dirección sea traducida a la dirección definida en el campo Dirección IP.
- Seleccione **Interfaz** si desea que la dirección *Traducir desde* utilice la dirección de una interfaz del router. La dirección *Traducir desde* se traducirá a la dirección IP asignada a la interfaz que especifique en el campo Interfaz.

### Interfaz

Este campo está activado si se selecciona Interfaz en el campo Tipo. Este campo mostrará una lista de las interfaces del router. Seleccione la interfaz a cuya dirección IP desea traducir las direcciones internas locales.



#### Nota

---

Si se selecciona **Interfaz** en el campo Tipo, sólo las traducciones que redireccionen puertos TCP/IP serán admitidas. La casilla de verificación Puerto de redireccionamiento se activa automáticamente y no se puede desmarcar.

---

### Dirección IP

Este campo está activado si se selecciona **Dirección IP** en el campo Tipo. Realice uno de los procedimientos siguientes:

- Si está creando una asignación de uno-a-uno entre una sola dirección **local interna** y una sola dirección **global interna**, especifique la dirección global interna en este campo.
- Si está asignando las direcciones locales internas de una subred a las direcciones globales internas correspondientes, especifique en este campo cualquier dirección IP que desee utilizar en la traducción. La máscara de red que se especifique en el área *Traducir desde* la interfaz se utilizará para calcular las direcciones globales internas restantes.



#### Nota

---

Si no desea especificar ninguna máscara de red en el área Traducir desde la interfaz, Cisco SDM realizará solamente una traducción.

---

## Puerto de redireccionamiento

Active esta casilla de verificación si desea incluir en la traducción información acerca del puerto para el dispositivo interno. De este modo, podrá utilizar la misma dirección IP pública para varios dispositivos, a condición de que el puerto especificado para cada dispositivo sea diferente. Se debe crear una entrada para cada mapeo de puerto para esta dirección “Traducido a”.

Si se trata de un número de puerto TCP, haga clic en **TCP**; si se trata de un número de puerto UDP, haga clic en **UDP**.

En el campo Puerto original, especifique el número del puerto del dispositivo interno.

En el campo Puerto traducido, especifique el número de puerto que debe utilizar el router para esta traducción.

## Escenarios de configuración

Haga clic en [Escenarios de traducción de direcciones estáticas](#) para obtener ejemplos ilustrativos del uso de los campos de esta ventana.

## Agregar o editar regla de traducción de direcciones estáticas: De externa a interna

Utilice este tema de ayuda cuando haya seleccionado **De externa a interna** en la ventana **Agregar Regla de traducción de direcciones estáticas** o en la ventana **Editar Regla de traducción de direcciones estáticas**.

Utilice esta ventana para agregar o editar una regla de traducción de direcciones estáticas. Si está editando una regla, las opciones Tipo de regla (estática o dinámica) y Dirección estarán desactivadas. Si necesita cambiar estos valores, elimine la regla y vuelva a crearla con la configuración deseada.

Dos tipos de traducciones de direcciones estáticas utilizan NAT: estática simple y estática ampliada.

**Nota**

---

Si desea crear una regla NAT que traduzca las direcciones de los dispositivos que forman parte de una VPN, Cisco SDM le solicitará permiso para crear un mapa de ruta destinado a proteger dichas direcciones contra la traducción mediante NAT. Si permite que NAT traduzca las direcciones de los dispositivos de una VPN, sus direcciones traducidas no satisfarán la regla IPsec en la política IPsec, y el tráfico se enviará sin cifrar. Para ver mapas de ruta creados por Cisco SDM o creados mediante la CLI, haga clic en el botón **Ver mapas de ruta** en la ventana NAT.

---

## Dirección

Elija el tipo de dirección de tráfico para esta regla.

### De externa a interna

Seleccione esta opción si desea traducir direcciones entrantes en direcciones que sean válidas para la LAN. Es posible que desee hacerlo cuando está fusionando redes y deba crear un conjunto de direcciones entrantes compatibles con un conjunto existente en la LAN que atiende el router.

En este tema de ayuda se describe el uso de los campos restantes cuando se selecciona la opción De externa a interna.

## Traducir desde la interfaz

Esta área muestra las interfaces desde las que llegan al router los paquetes que necesitan traducción de direcciones. Proporciona campos que permiten especificar la dirección IP de un solo host, o una dirección de red y máscara de subred que representan los hosts de una red.

### Interfaces externas

Si selecciona **De externa a interna**, esta área muestra las interfaces externas designadas.

**Nota**

---

Si en esta área no se incluye ningún nombre de interfaz, cierre la ventana Agregar regla de traducción de direcciones, haga clic en **Designar interfaces NAT** en la ventana NAT y designe las interfaces de router como internas o externas. A continuación, regrese a esta ventana y configure la regla NAT.

---

**Dirección IP**

Realice uno de los procedimientos siguientes:

- Si desea crear una asignación estática de uno-a-uno entre la dirección **global externa** de un solo host remoto y una dirección traducida, denominada *dirección local exterior*, especifique la dirección IP para el host remoto.
- Si desea crear asignaciones *n-a-n* entre las direcciones privadas de una subred y las direcciones **local exterior** correspondientes, especifique cualquier dirección válida de la subred cuyas direcciones desee traducir y especifique una máscara de red en el campo siguiente.

**Máscara de red**

Si desea que Cisco SDM traduzca las direcciones de una subred remota, especifique la máscara para esa subred. Cisco SDM determina el número de red y subred, y el conjunto de direcciones que necesitan traducción desde la dirección IP y la máscara que usted indique.

**Traducir a la interfaz**

Esta área muestra las interfaces desde las que salen del router los paquetes con las direcciones traducidas. También Proporciona campos para especificar la dirección traducida y otra información.

**Interfaces internas**

Si selecciona **De externa a interna**, esta área muestra las interfaces internas designadas.

**Dirección IP**

Realice uno de los procedimientos siguientes:

- Si está creando una asignación de uno-a-uno entre una sola dirección **global externa** y una sola dirección **local exterior**, especifique la dirección **local exterior** en este campo.
- Si está asignando las direcciones **global externa** de una subred remota a las direcciones **local exterior** correspondientes, especifique en este campo cualquier dirección IP que desee utilizar en la traducción. La máscara de red que se especifique en el área Traducir desde la interfaz se utilizará para calcular las direcciones **local exterior** restantes.

**Nota**


---

Si no desea especificar ninguna máscara de red en el área Traducir desde la interfaz, Cisco SDM realizará solamente una traducción.

---



## Puerto de redireccionamiento

Active esta casilla de verificación si desea incluir en la traducción información acerca del puerto para el dispositivo externo. De este modo, podrá utilizar una traducción estática ampliada y utilizar la misma dirección IP pública para varios dispositivos, a condición de que el puerto especificado para cada dispositivo sea diferente.

Si se trata de un número de puerto TCP, haga clic en **TCP**; si se trata de un número de puerto UDP, haga clic en **UDP**.

En el campo Puerto original, especifique el número del puerto del dispositivo externo.

En el campo Puerto traducido, especifique el número de puerto que debe utilizar el router para esta traducción.

## Escenarios de configuración

Haga clic en [Escenarios de traducción de direcciones estáticas](#) para obtener ejemplos ilustrativos del uso de los campos de esta ventana.

## Agregar o editar regla de traducción de direcciones dinámicas: De interna a externa

**Utilice este tema de ayuda cuando haya seleccionado De interna a externa en la ventana Agregar Regla de traducción de direcciones dinámicas o en la ventana Editar Regla de traducción de direcciones dinámicas.**

Utilice esta ventana para agregar o editar una regla de traducción de direcciones. Si se está editando una regla, se desactivan el tipo de regla (estática o dinámica) y su dirección. Si necesita cambiar estos valores, elimine la regla y vuelva a crearla con la configuración deseada.

Una regla de traducción de direcciones dinámicas asigna dinámicamente los hosts a las direcciones utilizando las direcciones de un conjunto de direcciones que son globalmente exclusivas en la red de destino. Para definir el conjunto, especifique un intervalo de direcciones y asigne un nombre único al intervalo. El router configurado utiliza las direcciones disponibles del conjunto (aquellas que no se utilizan para las traducciones estáticas o para su propia dirección IP de WAN) para las conexiones a Internet u otras externas a la red. Cuando una dirección ya no se utiliza, se devuelve al conjunto de direcciones para ser asignada dinámicamente a otro dispositivo más adelante.

**Nota**

---

Si desea crear una regla NAT que traduzca las direcciones de los dispositivos que forman parte de una VPN, Cisco SDM le solicitará permiso para crear un mapa de ruta destinado a proteger dichas direcciones contra la traducción mediante NAT. Si permite que NAT traduzca las direcciones de los dispositivos de una VPN, sus direcciones traducidas no satisfarán la regla IPsec utilizada en la política IPsec, y el tráfico se enviará sin cifrar.

---

## Dirección

Elija el tipo de dirección de tráfico para esta regla.

### De interna a externa

Seleccione esta opción si desea traducir direcciones privadas de la LAN a direcciones legales (globalmente únicas) de Internet o de la intranet de su organización.

En este tema de ayuda se describe el uso de los campos restantes cuando se selecciona la opción De interna a externa.

## Traducir desde la interfaz

Esta área muestra las interfaces desde las que llegan al router los paquetes que necesitan traducción de direcciones. Proporciona campos para especificar la dirección IP de un host individual, o una dirección de red y máscara de subred que represente los hosts de una red.

### Interfaces internas

Si selecciona **De interna a externa** para la opción Dirección, esta área muestra las interfaces internas designadas.

**Nota**

---

Si en esta área no se incluye ningún nombre de interfaz, cierre la ventana Agregar regla de traducción de direcciones, haga clic en **Designar interfaces NAT** en la ventana NAT y designe las interfaces de router como internas o externas. A continuación, regrese a esta ventana y configure la regla NAT.

---

## Regla de acceso

Las reglas de traducción NAT dinámicas utilizan reglas de acceso para especificar las direcciones que necesitan traducción. Si selecciona **De interna a externa**, éstas serán las direcciones [local interna](#). Especifique el nombre o el número de la regla de acceso que define las direcciones que desea traducir. Si no sabe el nombre o número, puede hacer clic en el botón ... y seleccionar una regla de acceso existente. O bien, puede crear una nueva regla de acceso para usarla.

## Traducir a la interfaz

Esta área muestra las interfaces desde las que salen del router los paquetes con las direcciones traducidas. También Proporciona campos para especificar la dirección traducida.

### Interfaces externas

Si selecciona **De interna a externa** para la opción Dirección, esta área muestra las interfaces externas designadas.

### Tipo

Seleccione **Interfaz** si desea que las direcciones *Traducir desde* utilicen la dirección de una interfaz del router. Éstas se traducirán en la dirección que especifique en el campo Interfaz y se utilizará PAT para distinguir cada host de la red. Seleccione **Conjunto de direcciones** si desea que las direcciones se traduzcan en direcciones definidas en un conjunto de direcciones configurado.

### Interfaz

Si se selecciona **Interfaz** en el campo Tipo, este campo muestra las interfaces del router. Seleccione la interfaz a cuya dirección IP desea traducir las direcciones internas locales. Se utilizará PAT para distinguir cada host de la red.

### Conjunto de direcciones

Si se selecciona **Conjunto de direcciones** en el campo Tipo, en este campo puede especificar el nombre de un conjunto de direcciones configurado. O bien, puede hacer clic en **Conjunto de direcciones** para seleccionar o crear un conjunto de direcciones.

## Escenarios de configuración

Haga clic en [Escenarios de traducción de direcciones dinámicas](#) para obtener ejemplos ilustrativos del uso de los campos de esta ventana.

## Agregar o editar regla de traducción de direcciones dinámicas: De externa a interna

Utilice este tema de ayuda cuando haya seleccionado **De externa a interna** en la ventana **Agregar Regla de traducción de direcciones dinámicas** o en la ventana **Editar Regla de traducción de direcciones dinámicas**.

Utilice esta ventana para agregar o editar una regla de traducción de direcciones. Si se está editando una regla, se desactivan el tipo de regla (estática o dinámica) y su dirección. Si necesita cambiar estos valores, elimine la regla y vuelva a crearla con la configuración deseada.

Una regla de traducción de direcciones dinámicas asigna dinámicamente los hosts a las direcciones utilizando las direcciones de un conjunto de direcciones que son globalmente exclusivas en la red de destino. Para definir el conjunto, especifique un intervalo de direcciones y asigne un nombre único al intervalo. El router configurado utiliza las direcciones disponibles del conjunto (aquéllas que no se utilizan para las traducciones estáticas o para su propia dirección IP de WAN) para las conexiones a Internet u otras externas a la red. Cuando una dirección ya no se utiliza, se devuelve al conjunto de direcciones para ser asignada dinámicamente a otro dispositivo más adelante.



### Nota

---

Si crea una regla NAT que traduzca las direcciones de los dispositivos que forman parte de una [VPN](#), Cisco SDM le solicitará permiso para crear un mapa de ruta destinado a proteger dichas direcciones contra la traducción mediante NAT. Si permite que NAT traduzca las direcciones de los dispositivos de una VPN, sus direcciones traducidas no satisfarán la regla IPSec utilizada en la política IPSec, y el tráfico se enviará sin cifrar.

---

### Dirección

Elija el tipo de dirección de tráfico para esta regla.

#### De externa a interna

Seleccione esta opción si desea traducir direcciones entrantes en direcciones que sean válidas para la LAN. Es posible que desee hacerlo cuando está fusionando redes y deba crear un conjunto de direcciones entrantes compatibles con un conjunto existente en la LAN que atiende el router.

En este tema de ayuda se describe el uso de los campos restantes cuando se selecciona la opción **De externa a interna**.

## Traducir desde la interfaz

Esta área muestra las interfaces desde las que llegan al router los paquetes que necesitan traducción de direcciones. Proporciona campos para especificar la dirección IP de un host individual, o una dirección de red y máscara de subred que represente los hosts de una red.

### Interfaces externas

Si selecciona **De externa a interna**, esta área muestra las interfaces externas designadas.



#### Nota

---

Si en esta área no se incluye ningún nombre de interfaz, cierre la ventana Agregar regla de traducción de direcciones, haga clic en **Designar interfaces NAT** en la ventana NAT y designe las interfaces de router como internas o externas. A continuación, regrese a esta ventana y configure la regla NAT.

---

## Regla de acceso

Las reglas de traducción NAT dinámicas utilizan reglas de acceso para especificar las direcciones que necesitan traducción. Si selecciona **De externa a interna**, éstas serán las direcciones [global externa](#). Especifique el nombre o el número de la regla de acceso que define las direcciones que desea traducir. Si no sabe el nombre o número, puede hacer clic en el botón ... y seleccionar una regla de acceso existente. O bien, puede crear una nueva regla de acceso para usarla.

## Traducir a la interfaz

Esta área muestra las interfaces desde las que salen del router los paquetes con las direcciones traducidas. También Proporciona campos para especificar la dirección traducida.

### Interfaces internas

Si selecciona **De externa a interna**, esta área muestra las interfaces internas designadas.

**Tipo**

Seleccione **Interfaz** si desea que las direcciones *Traducir desde* utilicen la dirección de una interfaz del router. Éstas se traducirán en la dirección que especifique en el campo Interfaz y se utilizará PAT para distinguir cada host de la red. Seleccione **Conjunto de direcciones** si desea que las direcciones se traduzcan en direcciones definidas en un conjunto de direcciones configurado.

**Interfaz**

Si se selecciona **Interfaz** en el campo Tipo, este campo muestra las interfaces del router. Seleccione la interfaz a cuya dirección IP desea traducir las direcciones internas locales. Se utilizará PAT para distinguir cada host de la red.

**Conjunto de direcciones**

Si se selecciona Conjunto de direcciones en el campo Tipo, en este campo puede especificar el nombre de un conjunto de direcciones configurado. O bien, puede hacer clic en **Conjunto de direcciones** para seleccionar o crear un conjunto de direcciones.

**Escenarios de configuración**

Haga clic en [Escenarios de traducción de direcciones dinámicas](#) para obtener ejemplos ilustrativos del uso de los campos de esta ventana.

**Cómo...**

Esta sección contiene procedimientos para tareas que el Asistente no le ayuda a realizar.

## ¿Cómo configuro la Traducción de direcciones de externa a interna?

El Asistente de NAT permite configurar una regla de Traducción de direcciones de red (NAT) para traducir las direcciones internas a externas. Para configurar una regla NAT para traducir direcciones internas a externas, siga las instrucciones de una de las siguientes secciones:

- [Agregar o editar regla de traducción de direcciones dinámicas: De externa a interna](#)
- [Agregar o editar regla de traducción de direcciones estáticas: De externa a interna](#)

## ¿Cómo configuro NAT con una LAN y múltiples WAN?

El Asistente de NAT permite configurar una regla de Traducción de direcciones de red (NAT) entre una interfaz LAN del router y una interfaz WAN. Si desea configurar NAT entre una interfaz LAN del router y varias interfaces WAN, use primero el asistente NAT para configurar una regla de traducción de direcciones entre la interfaz LAN del router y una interfaz WAN. Luego, siga las instrucciones de alguna de las siguientes secciones:

- [Agregar o editar regla de traducción de direcciones estáticas: De interna a externa](#)
- [Agregar o editar regla de traducción de direcciones dinámicas: De interna a externa](#)

Cada vez que se agrega una nueva regla de traducción de direcciones utilizando las direcciones de una de estas secciones, seleccione la misma interfaz LAN y una nueva interfaz WAN. Repita este procedimiento para todas las interfaces WAN que desee configurar con reglas de traducción de direcciones.







# CAPÍTULO 24

## Cisco IOS IPS

---

El sistema de prevención de intrusiones del Cisco IOS (Cisco IOS IPS) permite administrar la prevención de intrusiones en routers que usan Cisco IOS versión 12.3(8)T4 o versiones posteriores. Cisco IOS IPS permite supervisar y evitar intrusiones mediante la comparación del tráfico con firmas de amenazas conocidas y el bloqueo del tráfico cuando se detecta una amenaza.

Cisco SDM le permite controlar la aplicación de Cisco IOS IPS en las interfaces, importar y editar los archivos de definiciones de firmas ([SDF](#)) desde [Cisco.com](#) y configurar las acciones que Cisco IOS IPS debe realizar cuando se detecte una amenaza.

### Fichas IPS

Utilice las fichas de la parte superior de la ventana IPS para ver el área donde se necesita trabajar.

- **Crear IPS:** haga clic para ver el Asistente de reglas IPS para crear una nueva regla Cisco IOS IPS.
- **Editar IPS:** haga clic para editar las reglas Cisco IOS IPS y aplicarlas o eliminarlas de las interfaces.
- **Panel de seguridad:** haga clic para ver la tabla Amenazas más frecuentes e implementar firmas asociadas a estas amenazas.
- **Migración IPS:** si el router ejecuta una imagen de Cisco IOS de la versión 12.4(11)T o posterior, puede migrar configuraciones de Cisco IOS IPS creadas mediante versiones anteriores de Cisco IOS.

## Reglas IPS

Una regla Cisco IOS IPS especifica una interfaz, el tipo y dirección del tráfico que se debe examinar y la ubicación del archivo de definición de firmas (SDF) que utiliza el router.

# Crear IPS

En esta ventana puede iniciar el Asistente de reglas IPS.

El Asistente de creación de reglas IPS le solicitará la siguiente información:

- La interfaz en la que debe aplicarse la regla.
- El tráfico sobre el que se aplicará Cisco IOS IPS (entrante, saliente o ambos).
- La ubicación del archivo de definición de firmas (SDF)

Para imágenes de Cisco IOS 12.4(11) o posterior, también se le solicitará la siguiente información:

- Dónde desea guardar archivos que contienen cambios a la configuración de IOS IPS. Un archivo que guarda este tipo de información se conoce como [archivo delta](#).
- La clave pública que se usa para acceder a la información en los archivos delta.
- La categoría de firma. La categoría básica de firma es adecuada para routers con menos de 128 Mb de memoria flash. La categoría avanzada de firma es adecuada para routers con más de 128 Mb de memoria flash.

El escenario de casos de uso ilustra una configuración en la que se utiliza una regla Cisco IOS IPS. Después de que se crea la regla Cisco IOS IPS y se envía la configuración al router, es posible modificar la regla haciendo clic en la ficha **Editar IPS**.

Para obtener más información acerca de Cisco IOS IPS, consulte los documentos del enlace siguiente:

[http://www.cisco.com/en/US/products/ps6634/prod\\_white\\_papers\\_list.html](http://www.cisco.com/en/US/products/ps6634/prod_white_papers_list.html)

Haga clic en el botón **Iniciar el asistente de reglas IPS** para comenzar.

## Crear IPS: Bienvenido

Esta ventana resume las tareas que se realizan cuando se utiliza el Asistente de reglas IPS.

Haga clic en **Siguiente** para comenzar a configurar una regla Cisco IOS IPS.

## Crear IPS: Seleccionar interfaces

Seleccione las interfaces en las que se desea aplicar la regla Cisco IOS IPS, especificando si la regla debe aplicarse al tráfico entrante o al saliente. Si marca tanto las casillas del tráfico entrante como la del saliente, la regla se aplicará al tráfico que va en ambas direcciones.

Por ejemplo: la siguiente configuración aplica Cisco IOS IPS al tráfico entrante en la interfaz BRI 0, y en ambas direcciones de tráfico en la interfaz FastEthernet 0.

Nombre de interfaz	Entrante	Saliente
BRI 0	Seleccionado	—
FastEthernet 0	Seleccionado	Seleccionado

## Crear IPS: Ubicación SDF

Cisco IOS IPS examina el tráfico comparándolo con las firmas contenidas en un archivo de definición de firmas (SDF). El archivo .SDF puede ubicarse en la memoria flash del router o en un sistema remoto al que el router tenga acceso. Es posible especificar múltiples ubicaciones del SDF para que si el router no puede comunicarse con su primera ubicación, éste pueda intentar comunicarse con otras ubicaciones hasta que pueda obtener un archivo .SDF.

Utilice los botones **Agregar**, **Eliminar**, **Desplazar hacia arriba** y **Desplazar hacia abajo** para agregar, eliminar y ordenar una lista de ubicaciones SDF con las que el router puede intentar comunicarse para obtener un archivo SDF. El router comienza en la primera entrada, y avanza hacia abajo en la lista hasta que obtiene un archivo SDF.

Las imágenes de Cisco IOS que admiten Cisco IOS IPS contienen firmas incorporadas. Si se marca la casilla de la parte inferior de la ventana, el router utilizará las firmas incorporadas sólo si éste puede obtener una archivo .SDF desde cualquier ubicación de la lista.

## Crear IPS: Archivo de firma

El archivo de firma Cisco IOS IPS contiene la información de firma por defecto presente en cada actualización del archivo en Cisco.com. Los cambios realizados a esta configuración se guardan en un [archivo delta](#). Por motivos de seguridad, el archivo delta debe firmarse digitalmente. Especifique la ubicación del archivo de firma y proporcione el nombre y el texto de la clave pública que se usará para firmar el archivo delta en esta ventana.

Este tema de ayuda describe la ventana Archivo de firma que aparece cuando el router ejecuta Cisco IOS 12.4(11)T y versiones posteriores.

### Especifique el archivo de firma que desea usar con IOS IPS

Si el archivo de firma ya está presente en el equipo, en la memoria flash del router o en un sistema remoto, haga clic en **Especificar el archivo de firma que desea utilizar con IOS IPS** para ver un cuadro de diálogo en el cual puede especificar la ubicación del archivo de firma.

### Obtenga el archivo de firma más reciente en Cisco.com y guárdelo en el equipo

Haga clic en **Obtenga el archivo de firma más reciente en Cisco.com y guárdelo en el equipo** si el archivo de firma aún no está presente en el equipo o en la memoria flash del router. Haga clic en **Examinar** para especificar dónde desea guardar el archivo de firma y haga clic en **Descargar** para comenzar a descargar el archivo. Cisco SDM descarga el archivo de firma en la ubicación que especifique.

### Configurar clave pública

Todos los cambios realizados a la configuración de firma se guardan en el [archivo delta](#). Este archivo debe firmarse digitalmente con una clave pública. Puede obtener una clave en Cisco.com y pegar la información en los campos Nombre y Clave.



#### Nota

Si ya ha agregado una clave pública a la configuración mediante la CLI de Cisco IOS, debe proporcionar una clave pública en esta pantalla. Después de completar el Asistente de reglas Cisco IOS IPS, puede ir a **Editar configuración > global de IPS**. En la pantalla Configuración global, puede hacer clic en **Editar** en el área Editar requisito previo de IPS y luego hacer clic en **Clave pública** para ver el diálogo Clave pública. En ese diálogo, puede eliminar claves públicas que no necesite.

Siga estos pasos para colocar la información de clave pública en los campos Nombre y Clave.

---

**Paso 1** Vaya al enlace siguiente para obtener la clave pública:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup>

**Paso 2** Descargue la clave en el equipo.

**Paso 3** Copie el texto después de la frase “named-key” en el campo Nombre. Por ejemplo, si la línea de texto que incluye el nombre es la siguiente:

```
named-key realm-cisco.pub signature
```

copie `realm-cisco.pub signature` en el campo Nombre:

**Paso 4** Copie el texto entre la frase `key-string`, y la palabra `quit` en el campo Clave. El siguiente es un texto de ejemplo:

```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
```

---

## Crear IPS: Ubicación y categoría del archivo de configuración

Especifique una ubicación para guardar la información de firma que usará Cisco IOS IPS. Esta información consta del archivo de firma y el [archivo delta](#) que se crea cuando se realizan cambios a la información de firma.

Este tema de ayuda describe la ventana Ubicación del archivo de configuración que aparece cuando el router ejecuta Cisco IOS 12.4(11)T y versiones posteriores.

### Ubicación de configuración

Haga clic en el botón que se encuentra a la derecha del campo Ubicación de configuración para ver un diálogo que permite especificar una ubicación. Después de especificar la información en ese diálogo, Cisco SDM muestra la ruta hacia la ubicación en este campo.

### Elegir categoría

Debido a que la memoria del router y las restricciones de recursos pueden impedir el uso de todas las firmas disponibles, existen dos categorías de firmas: **básica** y **avanzada**. En el campo Elegir categoría, seleccione la categoría que permitirá a Cisco IOS IPS funcionar en forma eficiente en el router. La categoría básica es adecuada para routers con menos de 128 MB de memoria flash disponible. La categoría avanzada es adecuada para routers con más de 128 MB de memoria flash disponible.

## Agregar o editar una ubicación de configuración

Especifique una ubicación para guardar la información de firma y el [archivo delta](#) que usará Cisco IOS IPS.

### Especificar la ubicación de configuración en este router

Para especificar una ubicación en el router, haga clic en el botón que se encuentra a la derecha del campo Nombre de directorio y seleccione el directorio en el cual desea guardar la información de configuración.



#### Nota

---

Si el router tiene un sistema de archivos basado en [LEFS](#), no podrá crear un directorio en la memoria del router. En este caso, flash: se usa como ubicación de configuración.

---

## Especificar la ubicación de configuración mediante URL

Para especificar una ubicación en un sistema remoto, especifique el protocolo y la ruta del [URL](#) necesario para alcanzar la ubicación. Por ejemplo, si desea especificar el URL `http://172.27.108.5/ips-cfg`, escriba `172.27.108.5/ips-cfg`.



### Nota

No incluya el protocolo en la ruta especificada. Cisco SDM agrega automáticamente el protocolo. Si especifica el protocolo, Cisco SDM muestra un mensaje de error.

En los campos Número de reintentos y Límite de tiempo, especifique cuántas veces el router intentará contactarse con el sistema remoto y cuánto tiempo esperará una respuesta antes de detener los intentos de contacto.

## Selección de directorio

Haga clic en la carpeta en la cual desea guardar la información de configuración. Si desea crear una carpeta nueva, haga clic en **Nueva carpeta**, proporcione un nombre para ésta en el diálogo que aparece, selecciónela y haga clic en **Aceptar**.

## Archivo de firma

Especifique la ubicación del archivo de firma que usará Cisco IOS IPS.

### Especificar el archivo de firma en la memoria flash

Si el archivo de firma se encuentra en la memoria flash del router, haga clic en el botón que se encuentra a la derecha del campo. Cisco SDM muestra los nombres de archivo de firma del formato correcto para que usted elija.

## Especificar el archivo de firma mediante URL

Si el archivo de firma se encuentra en un sistema remoto, seleccione el protocolo que se usará y especifique la ruta al archivo. Por ejemplo, si el archivo de firma IOS-S259-CLI.pkg se encuentra en 10.10.10.5, y se usará el protocolo FTP, seleccione **ftp** como protocolo y especifique

```
10.10.10.5/IOS-S259-CLI.pkg
```



### Nota

No incluya el protocolo en la ruta especificada. Cisco SDM agrega automáticamente el protocolo. Si especifica el protocolo, Cisco SDM muestra un mensaje de error. Además, cuando usa una URL, debe especificar un nombre de archivo que se ajuste a la convención de nombres de archivos IOS-Snnn-CLI.pkg, como, por ejemplo, el archivo utilizado en el ejemplo anterior.

## Especificar el archivo de firma en el equipo

Si el archivo de firma se encuentra en el equipo, haga clic en **Examinar**, acceda a la carpeta que contiene el archivo y seleccione el nombre de archivo. Debe seleccionar un paquete específico de Cisco SDM del formato sigv5-SDM-Sxxx.zip; por ejemplo, sigv5-SDM-S260.zip.

## Crear IPS: Resumen

A continuación, se muestra un ejemplo de un resumen de Cisco IOS IPS en un router que ejecuta una versión de Cisco IOS anterior a 121.4(11)T.

```
Interfaz seleccionada: FastEthernet 0/1
```

```
Dirección de exploración de IPS: Ambos
```

```
Ubicación del archivo de definición de firmas (SDF): flash//sdmips.sdf
```

```
Integración habilitada: sí
```

En este ejemplo, Cisco IOS IPS está activado en la interfaz FastEthernet 0/1, y se explora tanto el tráfico entrante como el saliente. El archivo **SDF** se llama sdmips.sdf y se ubica en la memoria flash del router. El router se configura para utilizar las definiciones de firmas incorporadas en la imagen de Cisco IOS que ejecuta el router.



## Crear IPS: Resumen

La ventana Resumen muestra la información que se ha especificado para que se pueda revisar antes de enviar los cambios al router.

Este tema de ayuda describe la ventana Resumen que aparece cuando el router ejecuta Cisco IOS 12.4(11)T y versiones posteriores. A continuación, se muestra un ejemplo de la ventana Resumen.

La regla IPS se aplicará al tráfico saliente en las siguientes interfaces.

```
FastEthernet0/1
```

La regla IPS se aplicará al tráfico entrante en las siguientes interfaces.

```
FastEthernet0/0
```

Ubicación del archivo de firma:

```
C:\SDM-Test-folder\sigs5-SDM-S260.zip
```

Clave pública:

```
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B8BE84
33251FA8 F79E393B B2341A13 CAFFC5E6 D5B3645E 7618398A EFB0AC74 11705BEA
93A96425 CF579F1C EA6A5F29 310F7A09 46737447 27D13206 F47658C7 885E9732
CAD15023 619FCE8A D3A2BCD1 0ADA4D88 3CBD93DB 265E317E 73BE085E AD5B1A95
59D8438D 5377CB6A AC5D5EDC 04993A74 53C3A058 8F2A8642 F7803424 9B020301 0001
```

Ubicación de configuración

```
flash:/configloc/
```

Categoría seleccionada de firmas:

```
avanzada
```

En este ejemplo, la política Cisco IOS IPS se aplica a las interfaces FastEthernet 0/0 y FastEthernet 0/1. El archivo de firma está ubicado en el equipo. La ubicación de configuración se encuentra en la memoria flash del router, en un directorio llamado configloc.

# Editar IPS

En esta ventana, puede ver los botones de Cisco IOS IPS para configurar y administrar políticas, mensajes de seguridad, firmas y otros elementos de Cisco IOS IPS.

## Botón Políticas IPS

Haga clic para ver la ventana [Editar IPS](#), donde es posible activar o desactivar Cisco IOS IPS en una interfaz y ver información sobre la forma en que se aplica Cisco IOS IPS. Si se activa Cisco IOS IPS en una interfaz, puede, en forma opcional, especificar qué tráfico se debe examinar en busca de intrusiones.

## Botón Configuración global

Haga clic para ver la ventana [Editar IPS: Configuraciones globales](#), donde se realizan los ajustes que afectan la operación general de Cisco IOS IPS.

## Actualización automática

Este botón aparece si la imagen de Cisco IOS en el router es de la versión 12.4(11)T o posterior. La actualización automática permite configurar el router para obtener automáticamente las actualizaciones de firmas más recientes del Cisco Security Center. Para obtener más información, consulte [Editar IPS: Actualización automática](#).

## Configuración SEAP

Este botón aparece si la imagen de Cisco IOS en el router es de la versión 12.4(11)T o posterior. Procesamiento de acción de evento de firma ([SEAP](#)) otorga un mayor control sobre IOS IPS al proporcionar anulaciones y filtrado avanzados.

## Botón Mensajes SDEE

Los mensajes de Intercambio seguro de eventos del dispositivo (SDEE) informan sobre el progreso de la iniciación y operación de Cisco IOS IPS. Haga clic en este nodo para ver la ventana [Editar IPS: Mensajes SDEE](#), donde es posible revisar los mensajes SDEE y filtrarlos para ver sólo los mensajes de error, de estado o de alerta.

## Botón Firmas

Haga clic en este botón para mostrar la ventana [Editar IPS: Firmas](#), donde puede administrar firmas en el router.

## Botón CIDS de módulo de red

Este botón está visible si el router tiene instalado un módulo de red con Sistema de detección de intrusiones de Cisco. Haga clic para gestionar el módulo IDS.

# Editar IPS: Políticas IPS

Esta ventana muestra el estado de Cisco IOS IPS de todas las interfaces del router y permite activar y desactivar Cisco IOS IPS en las interfaces.

## Interfaces

Utilice esta lista para filtrar las interfaces que se muestran en el área de lista de interfaces. Elija una de las siguientes opciones:

- Todas las interfaces: todas las interfaces del router.
- Interfaces IPS: interfaces en las que Cisco IOS IPS está activado.

## Botón Activar

Haga clic en este botón para activar Cisco IOS IPS en la interfaz seleccionada. Puede especificar las direcciones de tráfico en las que se aplicará Cisco IOS IPS y las ACL que se utilizarán para definir el tipo de tráfico que se examinará. Consulte el apartado [Activar o editar IPS en una interfaz](#) para obtener más información.

## Botón Editar

Haga clic en este botón para editar las características de Cisco IOS IPS que se aplican a la interfaz seleccionada.

## Botón Desactivar

Haga clic en este botón para desactivar Cisco IOS IPS en la interfaz seleccionada. Un menú contextual le mostrará las direcciones de tráfico en las que se ha aplicado Cisco IOS IPS y le permitirá seleccionar la dirección en la que desea desactivar Cisco IOS IPS. Si desactiva Cisco IOS IPS en una interfaz en la que se había aplicado, Cisco SDM anula la asociación de todas las reglas Cisco IOS IPS de esa interfaz.

## Botón Desactivar todo

Haga clic en este botón para desactivar Cisco IOS IPS en todas las interfaces en las que se había activado. Si desactiva Cisco IOS IPS en una interfaz en la que se había aplicado, Cisco SDM anula la asociación de todas las reglas Cisco IOS IPS de esa interfaz.

## Nombre de interfaz

El nombre de la interfaz. Por ejemplo: Serie0/0 o FE0/1.

## IP

Esta columna puede contener los siguientes tipos de direcciones IP:

- Dirección IP configurada de la interfaz.
- Cliente DHCP: la interfaz recibe una dirección IP de un servidor DHCP (Dynamic Host Configuration Protocol).
- Negociada: la interfaz recibe una dirección IP a través de una negociación con el dispositivo remoto.
- No numerada: el router utilizará un conjunto de direcciones IP suministrado por el proveedor de servicios del router y los dispositivos de la LAN.
- No aplicable: no se puede asignar ninguna dirección IP al tipo de interfaz.

## IPS entrante/IPS saliente

- Activado: Cisco IOS IPS está activado para esta dirección de tráfico.
- Desactivado: Cisco IOS IPS está desactivado para esta dirección de tráfico.

## Estado de la red VFR

Estado del ensamblaje de fragmentos virtuales (**VFR**). Los valores posibles son:

- Activado: se activa VFR.
- Desactivado: se desactiva VFR.

Cisco IOS IPS no puede identificar el contenido de los fragmentos IP ni recopilar información de puerto de dichos fragmentos para compararlo con una firma. A causa de ello, se permite el paso de los fragmentos a la red sin antes ser examinados o sin crear una lista de control de acceso (ACL) dinámica.

VFR permite al firewall Cisco IOS crear las ACL dinámicas pertinentes, protegiendo, con ello, la red contra distintos ataques de fragmentación.

## Descripción

Breve descripción de la conexión, en el caso de agregarla.

## Detalles del filtro IPS



Si no se aplica ningún filtro, esta área no contendrá entradas. Si se ha aplicado algún filtro, se mostrará entre paréntesis el nombre o el número de la ACL.

### Botones Filtro entrante y Filtro saliente

Haga clic en estos botones para ver las entradas del filtro aplicado al tráfico entrante o saliente.

### Descripciones de los campos

**Acción:** indica si se permite o deniega el tráfico.

-  Permitir el tráfico de origen.
-  Prohibir el tráfico de origen.

**Origen:** dirección del host o de red, o cualquier host o red.

**Destino:** dirección del host o de red, o cualquier host o red.

**Servicio:** tipo de servicio filtrado: IP, TCP, UDP, IGMP o ICMP.

**Registro:** indica si se registra el tráfico denegado.

**Atributos:** opciones configuradas mediante CLI.

**Descripción:** cualquier descripción suministrada.

## Activar o editar IPS en una interfaz

Utilice esta ventana para seleccionar las interfaces en las que desea activar la detección de intrusiones y para especificar los filtros **IPS** para examinar el tráfico.

### Botones Filtro entrante y Filtro saliente

Utilice estos botones para especificar si va a activar Cisco IOS IPS en el tráfico entrante y saliente, sólo en el tráfico entrante o sólo en el tráfico saliente.

### Filtro entrante

(Opcional) Escriba el nombre o número de la regla de acceso que especifica el tráfico entrante que deberá examinarse. La ACL que especifique aparecerá en la ventana de configuración de las reglas IPS cuando seleccione la interfaz con la que está asociada. Si necesita desplazarse hasta la regla de acceso o bien crear una nueva, haga clic en el botón ...

### Filtro saliente

(Opcional) Escriba el nombre o número de la regla de acceso que especifica el tráfico saliente que debe examinarse. La ACL que especifique aparecerá en la ventana de configuración de las reglas IPS cuando seleccione la interfaz con la que está asociada. Si necesita desplazarse hasta la regla de acceso o bien crear una nueva, haga clic en el botón ...

### Botón...

Utilice este botón para especificar un filtro. Haga clic en este botón para mostrar un menú con las siguientes opciones:

- Seleccionar una regla existente. Consulte el apartado [Seleccionar una regla](#) para obtener más información.
- Crear una nueva regla. Consulte el apartado [Agregar/Editar una regla](#) para obtener más información.
- Ninguno (borrar la asociación de reglas) Utilice esta opción para eliminar un filtro de una dirección de tráfico en la que se ha aplicado.

## Activar la verificación del fragmento en esta interfaz

(Opción activada por defecto). Active esta opción si desea que el firewall de Cisco IOS verifique los fragmentos IP en esta interfaz. Consulte el apartado [Estado de la red VFR](#) para obtener más información.

## Activar la verificación de fragmento en otras interfaces

Si la verificación de fragmento del tráfico saliente está activada, el router deberá examinar el tráfico entrante que llegue a las interfaces que envían el tráfico saliente a la interfaz que se está configurando. Especifique abajo las interfaces.

Si el botón de selección Entrante está seleccionado, no aparecerá esta área.

## Especificar el archivo de firma

El cuadro Especificar el archivo de firma contiene información acerca de la versión [SDF](#) que está utilizando el router y permite actualizar el SDF a una versión más reciente. Para especificar un SDF nuevo, haga clic en el botón ... ubicado junto al campo Archivo de firma y especifique un archivo nuevo en el diálogo que aparece.

# Editar IPS: Configuraciones globales

Esta ventana permite ver y establecer la configuración global para Cisco IPS. Este tema de ayuda describe la información que puede ver si la imagen de Cisco IOS en ejecución es anterior a la versión 12.4(11)T.

## Tabla Configuración global

Esta tabla en la ventana Configuración global muestra la configuración global actual y sus valores. Haga clic en **Editar** para cambiar alguno de estos valores.

Nombre de elemento	Valor de elemento
Syslog	Si está activado, las notificaciones se enviarán al servidor syslog especificado en Propiedades del sistema.
SDEE	Security Device Event Exchange. Si está activado, se generarán eventos SDEE.

Eventos SDEE	Número de eventos SDEE que se almacenarán en el búfer del router.
Suscripción SDEE	Número de suscripciones SDEE simultáneas.
Opciones de motor	<p>Las opciones del motor son:</p> <ul style="list-style-type: none"> <li>• Cierre por fallo: por defecto, mientras Cisco IOS compila una firma nueva para un motor determinado, se permite el paso de paquetes sin examinar para el motor correspondiente. Cuando esta opción está activada, Cisco IOS abandona los paquetes durante el proceso de compilación.</li> <li>• Usar las firmas integradas (como copia de seguridad): si Cisco IOS IPS no encuentra o no consigue cargar las firmas desde las ubicaciones especificadas, puede hacer que las firmas integradas en Cisco IOS activen Cisco IOS IPS. Por defecto, esta opción está activada.</li> <li>• Denegar acción en la interfaz IPS: recomendado cuando el router está realizando el equilibrio de carga. Cuando está activada, esta opción hace que Cisco IOS IPS active ACL en las interfaces Cisco IOS IPS en lugar de activarlas en las interfaces de donde provienen los ataques.</li> </ul>
Eventos de rechazo	Esta opción utiliza el parámetro Shun Time. Shun Time es el tiempo que tardarán las acciones de rechazo en ejecutarse. Una acción de rechazo tiene lugar cuando se agrega un host o una red a una ACL con el fin de denegar el tráfico de ese host o red.



## Ubicaciones de SDF configuradas

La ubicación de una firma es una URL que suministra una ruta a un SDF. Para buscar un SDF, el router intenta ponerse en contacto con la primera ubicación de la lista. Si no lo consigue, intenta, una por una, las ubicaciones siguientes hasta que encuentra un SDF.

### Botón Agregar

Haga clic en este botón para agregar una URL a la lista.

### Botón Editar

Haga clic en este botón para editar una ubicación seleccionada.

### Botón Eliminar

Haga clic en este botón para eliminar una ubicación seleccionada.

### Botones Desplazar hacia arriba y Desplazar hacia abajo

Utilice estos botones para cambiar el orden de preferencia de las URL de la lista.

## Volver a cargar firmas

Haga clic para recompilar las firmas en todos los motores de firmas. Durante este lapso, el software Cisco IOS no podrá utilizar las firmas del motor para explorar los paquetes.

## Editar configuración global

Edite la configuración que produce un efecto sobre la operación general de Cisco IOS IPS en esta ventana, en las fichas Syslog y SDEE, y Motor global.

## Activar notificación Syslog (Fichas Syslog y SDEE)

Active esta casilla de verificación para que el router pueda enviar mensajes de alarma, evento o error a un servidor syslog. Para que este método de notificación funcione, es preciso que haya un servidor syslog identificado en Propiedades del sistema.

## SDEE (Fichas Syslog y SDEE)

Introduzca el número de suscripciones SDEE simultáneas, en el intervalo de 1 a 3, en el campo **Número de suscripciones SDEE simultáneas**. Una suscripción SDEE es una alimentación directa de eventos SDEE.

En el campo **Número máximo de eventos SDEE para almacenar**, introduzca el número máximo de alertas SDEE que desee que el router almacene, en el intervalo de 10 a 2000. Si almacena más alertas, utilizará más memoria del router.

En el campo **Número máximo de mensajes SDEE para almacenar**, introduzca el número máximo de mensajes SDEE que desee que el router almacene, en el intervalo de 10 a 500. Si almacena más mensajes, utilizará más memoria del router.

## Activar cierre por fallo del motor (Ficha Motor global)

Por defecto, mientras el software Cisco IOS compila una firma nueva para un motor determinado, se permite el paso de paquetes sin examinar para el motor correspondiente. Active esta opción para que el software Cisco IOS rechace los paquetes durante el proceso de compilación.

## Usar las firmas integradas (como copia de seguridad) (Ficha Motor global)

Si Cisco IOS IPS no encuentra o no puede cargar las firmas de las ubicaciones especificadas, puede utilizar las firmas integradas de Cisco IOS para activar Cisco IOS IPS. Por defecto, esta opción está activada.

## Activar Denegar acción en la interfaz (Ficha Motor global)

Esta opción se aplica si se configuran las acciones de firmas en “denyAttackerInline” o “denyFlowInline”. Por defecto, Cisco IOS IPS aplica las ACL a las interfaces desde donde proviene el ataque y no a las interfaces Cisco IOS IPS. Si se activa esta opción, Cisco IOS IPS aplica las ACL directamente a las interfaces Cisco IOS IPS y no a las interfaces que recibieron originalmente el tráfico de ataque. Si el router no está realizando el equilibrio de carga, esta configuración no debe activarse. Si el router está realizando el equilibrio de carga, se recomienda activar esta opción.

## Límite de tiempo (Ficha Motor global)

Esta opción le permite especificar el número de minutos, en el intervalo de 0 a 65535, que tardan las acciones de rechazo en ejecutarse. El valor por defecto es de 30 minutos. Una acción de rechazo tiene lugar cuando se agrega un host o una red a una ACL con el fin de denegar el tráfico de ese host o red.

## Agregar o editar una ubicación de firma

Especifique la ubicación desde la que Cisco IOS IPS debe cargar un archivo [SDF](#). Para especificar múltiples ubicaciones SDF, abra este diálogo nuevamente y especifique la información para otro archivo .SDF.

### Especificar SDF en este router

Especifique la parte de la memoria del router en que se encuentra el archivo .SDF mediante el menú desplegable Ubicación. Por ejemplo: el menú puede incluir las entradas *disk0*, *usbflash1* y *flash*. A continuación, seleccione el nombre del archivo haciendo clic en la flecha hacia abajo junto al campo Nombre del archivo o introduzca el nombre del archivo en el campo correspondiente.

### Especificar SDF usando URL

Si el archivo SDF se ubica en un sistema remoto, es posible especificar la URL en la que éste reside.

#### Protocolo

Seleccione el protocolo que debe utilizar el router para obtener el archivo SDF, como *http* o *https*.

#### URL

Introduzca la dirección URL con el formato siguiente:

*ruta-a-archivo-firma*



#### Nota

---

El protocolo que seleccione en el menú Protocolo aparecerá a la derecha del campo URL. *No* vuelva a introducir el protocolo en el campo URL.

---

La siguiente URL se entrega como ejemplo del formato. *no* es una URL válida a un archivo de firmas e incluye el protocolo para mostrar la URL completa:

`https://172.16.122.204/mysigs/vsensor.sdf`

### Autoguardar

Marque esta opción si desea que el router guarde, automáticamente, el archivo SDF en caso de un fallo de éste. Esto elimina la necesidad de reconfigurar Cisco IOS IPS con este archivo SDF cuando el router vuelva a funcionar.

## Editar IPS: Mensajes SDEE

Esta ventana muestra una lista de los mensajes [SDEE](#) recibidos por el router. Los mensajes SDEE se generan cuando existen cambios en la configuración de Cisco IOS IPS.

### Mensajes SDEE

Seleccione el tipo de mensaje SDEE para mostrar:

- Todos: se muestran los mensajes de advertencia, estado y error SDEE.
- Error: sólo se muestran los mensajes de error de SDEE.
- Estado: sólo se muestran los mensajes de estado de SDEE.
- Alertas: sólo se muestran los mensajes de alerta de SDEE.

### Ver por

Seleccione el campo de mensaje SDEE para buscar.

### Criterios

Especifique la cadena de búsqueda.

### Botón Ir

Haga clic en este botón para iniciar la búsqueda en la cadena especificada en el campo Criterios.

### Tipo

Los tipos son: Error, Estado y Alertas. Haga clic en [Texto de los mensajes SDEE](#) para ver los mensajes SDEE posibles.

### Hora

La hora en que se recibió el mensaje.

### Descripción

Descripción disponible.

## Botón Actualizar

Haga clic en él para ver los nuevos mensajes SDEE.

## Botón Cerrar

Haga clic en él para cerrar la ventana Mensajes SDEE.

## Texto de los mensajes SDEE

Este tema indica los mensajes SDEE posibles.

## Mensajes de estado IDS

### Mensaje de error

```
ENGINE_BUILDING: %s - %d signatures - %d of %d engines
```

**Explicación** Se desencadena cuando Cisco IOS IPS comienza a crear el micromotor de firmas (SME).

### Mensaje de error

```
ENGINE_BUILD_SKIPPED: %s - there are no new signature  
definitions for this engine
```

**Explicación** Se desencadena cuando no hay definiciones de firmas o bien no se ha producido ningún cambio en las definiciones de firmas existentes de un SME del Sistema de detección de intrusiones.

### Mensaje de error

```
ENGINE_READY: %s - %d ms - packets for this engine will be  
scanned
```

**Explicación** Se desencadena cuando un SME del IDS ha realizado la generación y está listo para examinar paquetes.

**Mensaje de error**

```
SDF_LOAD_SUCCESS: SDF loaded successfully from %s
```

**Explicación** Se desencadena cuando un archivo SDF se carga satisfactoriamente desde una ubicación determinada.

**Mensaje de error**

```
BUILTIN_SIGS: %s to load builtin signatures
```

**Explicación** Se desencadena cuando el router recurre a cargar las firmas incorporadas.

**Mensajes de error IDS****Mensaje de error**

```
ENGINE_BUILD_FAILED: %s - %d ms - engine build failed - %s
```

**Explicación** Se desencadena cuando Cisco IOS IPS no consigue reanudar la generación después de la carga de un archivo SDF. Se envía uno de estos mensajes para cada motor que falló. Esto significa que el motor Cisco IOS IPS no pudo importar las firmas para el motor especificado en el mensaje. Una memoria insuficiente es la causa más probable para este problema. Cuando esto sucede, Cisco IOS IPS descarta la nueva firma incorporada que pertenece a este motor.

**Mensaje de error**

```
SDF_PARSE_FAILED: %s at Line %d Col %d Byte %d Len %d
```

**Explicación** Se desencadena cuando un archivo SDF no se analiza correctamente.

**Mensaje de error**

```
SDF_LOAD_FAILED: failed to %s SDF from %s
```

**Explicación** Se desencadena cuando, por algún motivo, no se consigue cargar un archivo SDF.

**Mensaje de error**

```
DISABLED: %s - IDS disabled
```

**Explicación** Se ha desactivado IDS. El mensaje debería indicar la causa.

**Mensaje de error**

```
SYSEERROR: Unexpected error (%s) at line %d func %s() file %s
```

**Explicación** Se desencadena cuando se produce un error interno del sistema inesperado.

## Editar IPS: Configuraciones globales

Varias opciones de configuración de Cisco IOS IPS están disponibles con imágenes de Cisco IOS 12.4(11)T y posterior. Éstas se describen en este tema de ayuda. Los controles en pantalla y las opciones de configuración disponibles antes de Cisco IOS 12.4(11)T, como la configuración global de Syslog y SDEE se describen en [Editar IPS: Configuraciones globales](#).

Este tema de ayuda describe la ventana Configuración global que aparece cuando el router ejecuta Cisco IOS 12.4(11)T y versiones posteriores.

### Opciones de motor

Las opciones de motor disponibles con imágenes de Cisco IOS 12.4(11)T y posterior son las siguientes:

- Cierre por fallo: opción por defecto, mientras el Cisco IOS compila una firma nueva para un motor determinado, se permite el paso de paquetes sin examinar para el motor correspondiente. Cuando esta opción está activada, Cisco IOS abandona los paquetes durante el proceso de compilación.
- Denegar acción en la interfaz IPS: recomendado cuando el router está realizando el equilibrio de carga. Cuando está activada, esta opción hace que Cisco IOS IPS active ACL en las interfaces Cisco IOS IPS en lugar de activarlas en las interfaces de donde provienen los ataques.

## Tabla Editar requisito previo IPS

Esta tabla muestra la información acerca de cómo el router se provisiona para Cisco IOS IPS. Haga clic en **Editar** para cambiar alguno de estos valores. Los datos de ejemplo en la siguiente tabla indican que la ubicación de configuración es el directorio configloc en la memoria flash, que el router está utilizando la categoría básica de firmas y que se ha configurado una clave pública para permitir que el router acceda a la información en el directorio configloc.

Nombre de elemento	Valor de elemento
Ubicación de configuración	flash:/configloc/
Categoría seleccionada	básica
Clave pública	Configurada

## Editar configuración global

El diálogo Editar configuración global contiene una ficha Syslog y SDEE, y una ficha Motor global. Haga clic en el enlace a continuación para obtener la información que desea consultar:

- [Fichas Syslog y SDEE](#)
- [Ficha Motor global](#)

## Fichas Syslog y SDEE

El diálogo Syslog y SDEE que aparece cuando el router utiliza una imagen de Cisco IOS 12.4(11)T o posterior permite configurar la notificación syslog y parámetros para suscripciones [SDEE](#), eventos y mensajes.

### Activar notificación syslog

Active esta casilla de verificación para que el router pueda enviar mensajes de alarma, evento o error a un servidor syslog. Para que este método de notificación funcione, es preciso que haya un servidor syslog identificado en Propiedades del sistema.



## SDEE

Especifique el número de suscripciones SDEE simultáneas, en el intervalo de 1 a 3, en el campo Número de suscripciones SDEE simultáneas. Una suscripción SDEE es una alimentación directa de eventos SDEE.

En el campo Número máximo de eventos SDEE para almacenar, introduzca el número máximo de alertas SDEE que desee que el router almacene, en el intervalo de 10 a 2000. Si almacena más alertas, utilizará más memoria del router.

En el campo Número máximo de mensajes SDEE para almacenar, introduzca el número máximo de mensajes SDEE que desee que el router almacene, en el intervalo de 10 a 500. Si almacena más mensajes, utilizará más memoria del router.

## Ficha Motor global

El diálogo Motor global que aparece cuando el router utiliza una imagen de Cisco IOS 12.4(11)T o posterior permite configurar los ajustes descritos en las secciones siguientes.

### Activar cierre por fallo del motor

Por defecto, mientras el software Cisco IOS compila una firma nueva para un motor determinado, se permite el paso de paquetes sin examinar para el motor correspondiente. Active esta opción para que el software Cisco IOS rechace los paquetes durante el proceso de compilación.

### Activar Denegar acción en la interfaz IPS

Esta opción se aplica si se configuran las acciones de firmas en “denyAttackerInline” o “denyFlowInline”. Por defecto, Cisco IOS IPS aplica la ACL a las interfaces desde donde proviene el ataque y no a las interfaces Cisco IOS IPS. Si se activa esta opción, Cisco IOS IPS aplica las ACL directamente a las interfaces Cisco IOS IPS y no a las interfaces que recibieron originalmente el tráfico de ataque. Si el router no está realizando el equilibrio de carga, esta configuración no debe activarse. Si el router está realizando el equilibrio de carga, se recomienda activar esta opción.

## Editar requisitos previos de IPS

El diálogo Editar requisitos previos de IPS contiene fichas para las siguientes categorías de información. Haga clic en un enlace para obtener la información que desea consultar:

- [Ficha Ubicación de configuración](#)
- [Ficha Selección de categoría](#)
- [Ficha Clave pública](#)

### Ficha Ubicación de configuración

Si se ha configurado una ubicación de configuración en el router, puede editarla. Si no se ha configurado ninguna, puede hacer clic en Agregar y configurar una. El botón Agregar se desactiva si ya se ha configurado una ubicación de configuración. El botón Editar se desactiva cuando no se ha configurado ninguna ubicación de configuración. Consulte el apartado [Crear IPS: Ubicación y categoría del archivo de configuración](#) para obtener más información.

### Ficha Selección de categoría

Si especifica una categoría de firma, SDM configura el router con un subconjunto de firmas apropiadas para una cantidad específica de memoria del router. También puede quitar una configuración de categoría existente si desea eliminar restricciones de categoría al seleccionar firmas.

#### Configurar categoría

Haga clic en **Configurar categoría** y seleccione **básica** o **avanzada**. La categoría básica es adecuada para routers con menos de 128 MB de memoria flash disponible. La categoría avanzada es adecuada para routers con más de 128 MB de memoria flash disponible.

#### Eliminar categoría

Si desea quitar la configuración de categoría, haga clic en **Eliminar categoría**.

### Ficha Clave pública

Este diálogo muestra las claves públicas configuradas para Cisco IOS IPS. Puede agregar o eliminar claves desde este diálogo. Para agregar una clave, haga clic en **Agregar** y configure la clave en el diálogo que aparece.

Para quitar una clave, seleccione el nombre de clave y haga clic en **Eliminar**.

## Agregar clave pública

Puede copiar el nombre de la clave y la clave desde el siguiente sitio en Cisco.com:

<http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup>

Copie el nombre de la clave y péguelo en el campo Nombre en este diálogo. Luego, copie la clave desde la misma ubicación y péguela en el campo Clave. Para obtener instrucciones detalladas que explican exactamente qué partes del texto copiar y pegar, consulte [Configurar clave pública](#).

## Editar IPS: Actualización automática

Las actualizaciones de archivo de firma se publican en Cisco.com. Cisco SDM puede descargar la actualización de archivo de firma que especifique o puede descargar automáticamente la más reciente según una programación definida.

Este tema de ayuda describe la ventana Actualización automática que aparece cuando el router ejecuta Cisco IOS 12.4(11)T y versiones posteriores.

### Antes de configurar la actualización automática

Antes de configurar la actualización automática, debe sincronizar el reloj del router con el reloj del equipo. Para ello, siga estos pasos:

- 
- Paso 1** Vaya a **Configurar > Tareas adicionales > Propiedades del router > Fecha/Hora**.
  - Paso 2** En la ventana Fecha/Hora, haga clic en **Cambiar configuración**.
  - Paso 3** Seleccione la opción **Sincronizar con el reloj de mi equipo local** y haga clic en el botón **Sincronizar**.
  - Paso 4** Cierre el diálogo.
-

## Descargar archivo de firma de Cisco.com

Para que Cisco SDM descargue un archivo de firma específico de Cisco.com a su equipo, especifique el archivo que desea que Cisco SDM descargue y especifique la ubicación donde se guardará el archivo. El paquete de firma en uso muestra la versión que Cisco IOS IPS está usando actualmente. Se requiere un inicio de sesión de CCO para descargar archivos de firma y obtener otra información de Cisco.com desde las páginas Web de Cisco IOS IPS.

Para descargar el archivo de firma más reciente, haga clic en **Obtener el archivo más reciente**. Haga clic en **Examinar** para especificar dónde desea guardar el archivo y en **Descargar** para guardar el archivo en su equipo.

Para examinar los archivos disponibles antes de descargar, haga clic en **Enumerar los archivos disponibles para descargar**. A continuación, haga clic en el botón ubicado a la derecha del campo Lista de paquetes de firma. Haga clic en **Actualizar** en el menú contextual para examinar la lista de archivos disponibles. Para ver el archivo readme, haga clic en **Mostrar readme**. Seleccione el archivo que desea y use los botones **Examinar** y **Descargar** para guardarlo en su equipo.

## Actualización automática

Haga clic en **Activar actualización automática** si desea que Cisco SDM obtenga automáticamente las actualizaciones desde un servidor remoto específico.

### Configuración de URL de actualización automática de IPS

Especifique el nombre de usuario y la contraseña requerida para iniciar sesión en el servidor y especifique la [URL](#) al archivo de actualización en los campos de Configuración de URL de actualización automática de IPS. La siguiente es una URL de ejemplo:

```
tftp://:192.168.0.2/jdoe/ips-auto-update/IOS_update.zip
```

### Programación

Especifique una programación para cuando desea que el router obtenga la actualización desde el servidor. Puede especificar varios valores en cada columna para indicar un intervalo o para indicar varios valores de tiempo. Para especificar que desea obtener la actualización desde el servidor a la 1:00 a.m. todos los días, de domingo a jueves, seleccione los valores en la siguiente tabla.

Minuto	Hora	Fecha	Día
0	1	Seleccione 1 y 31.	Seleccione las casillas para domingo a jueves.

Haga clic en **Aplicar cambios** para enviar al router los cambios que realice en los campos de Actualización automática. Haga clic en **Descartar cambios** para quitar los datos que ha especificado en estos campos.

## Editar IPS: Configuración SEAP

Cisco IOS IPS disponible con Cisco IOS versión 12.4(11)T o posterior implementa Procesamiento de acción de evento de firma (**SEAP**). Esta ventana describe las funciones SEAP que puede configurar. Para comenzar la configuración, haga clic en uno de los botones bajo el botón Configuración SEAP.

Puede realizar la configuración SEAP para Cisco IOS IPS cuando el router ejecuta Cisco IOS 12.4(11)T y versiones posteriores.

### Editar IPS: Configuración SEAP: Índice de valor de destino

El índice de valor de destino (**TVR**) es un valor definido por el usuario que representa el valor percibido por el usuario del host de destino. Éste permite que el usuario aumente el riesgo de un evento asociado con un sistema crítico y no enfatice el riesgo de un evento en un destino de valor bajo.

Use los botones ubicados a la derecha de las columnas Índice de valor de destino y Dirección IP de destino para agregar, eliminar y editar entradas de destino. Haga clic en **Seleccionar todos** para resaltar automáticamente todos los índices de valor de destino. Haga clic en **Agregar** para mostrar un cuadro de diálogo donde pueda crear una nueva entrada TVR. Haga clic en **Editar** para cambiar la información de la dirección IP de una entrada.

## Columna Índice de valor de destino

Los destinos se pueden calificar como Alto, Bajo, Medio, Crítico para la misión o No Value. Una vez que se ha creado una entrada de destino, no se puede cambiar el índice. Si necesita cambiar el índice, debe eliminar la entrada de destino y volver a crearla usando el índice que desee.

## Columna Dirección IP de destino

La dirección IP de destino puede ser una dirección IP única o un intervalo de direcciones IP. Los ejemplos siguientes muestran dos entradas. Una es una entrada de dirección IP única y la otra es un intervalo de direcciones.

Índice de valor de destino	Dirección IP de destino
Alto	192.168.33.2
Medio	10.10.3.1-10.10.3.55

## Aplicar cambios

Cuando haya especificado la información que desea en la ventana Índice de valor de destino, haga clic en **Aplicar cambios**. El botón **Aplicar cambios** se desactiva cuando no hay cambios para enviar al router.

## Descartar cambios

Para borrar la información que ha especificado en la ventana Índice de valor de destino, pero que no ha enviado al router, haga clic en **Descartar cambios**. El botón Descartar cambios se desactiva cuando no hay cambios en espera para enviarse al router.

## Agregar Índice de valor de destino

Para agregar una entrada TVR, seleccione el índice de valor de destino y especifique una Dirección IP de destino o un intervalo de direcciones IP.

### Índice de valor de destino (TVR)

Los destinos se pueden calificar como Alto, Bajo, Medio, Crítico para la misión o Sin valor. Una vez que se ha usado un índice para una entrada de destino, no se puede usar para entradas adicionales. Por lo tanto, especifique en la misma entrada todos los destinos a los que desea otorgar el mismo índice.

### Direcciones IP de destino

Puede especificar una dirección IP de destino o un intervalo de direcciones, como se muestra en los siguientes ejemplos:

```
192.168.22.33  
10.10.11.4-10.10.11.55
```

Las direcciones IP de destino especificadas se muestran en la ventana Índice de valor de destino.

## Editar IPS: Configuración SEAP: Anulaciones de acción de evento

Las anulaciones de acción de evento permiten cambiar las acciones asociadas con un evento según el Índice de riesgo **RR** de dicho evento. Para hacer esto, se debe asignar un intervalo RR para cada acción de evento. Si se produce un evento y su RR está dentro del intervalo definido, la acción se agrega al evento. Las anulaciones de acción de evento son una forma de agregar acciones de evento globalmente sin tener que configurar cada firma individualmente.

### Utilizar anulaciones de acción de evento

Seleccione la casilla Utilizar anulaciones de acción de evento para que Cisco IOS IPS use las anulaciones de acción de evento. Puede agregar y editar las anulaciones de acción de evento aunque no estén activadas en el router.

## Seleccionar todo

El botón Seleccionar todo funciona con los botones Activar, Desactivar y Eliminar. Si desea activar o desactivar todas las anulaciones de acción de evento, haga clic en **Seleccionar todo** y, luego, en **Activar** o **Desactivar**. Para eliminar todas las anulaciones de acción de evento, haga clic en **Seleccionar todo** y, a continuación, en **Eliminar**.

## Botones Agregar y Editar

Haga clic en **Agregar** para mostrar un cuadro de diálogo donde puede especificar la información para una anulación de acción de evento. Seleccione una anulación de acción de evento y haga clic en **Editar** para cambiar la información para una anulación de acción de evento.

## Eliminar

Haga clic en **Eliminar** para quitar las anulaciones de acción de evento seleccionadas o para quitar todas las anulaciones de acción de evento si hace clic en **Seleccionar todo**.

## Activar y Desactivar

Los botones Activar y Desactivar permiten activar o desactivar las anulaciones de acción de evento. Seleccione una anulación de acción de evento o haga clic en **Seleccionar todo** para activar o desactivar todas las anulaciones de acción de evento.

## Aplicar cambios

Cuando haya especificado la información que desea en la ventana Anulaciones de acción de evento, haga clic en **Aplicar cambios**. El botón **Aplicar cambios** se desactiva cuando no hay cambios para enviar al router.

## Descartar cambios

Si desea borrar la información que ha especificado en la ventana Anulaciones de acción de evento, pero que no ha enviado al router, haga clic en **Descartar cambios**. El botón **Descartar cambios** se desactiva cuando no hay cambios en espera para enviarse al router.



## Agregar o editar una anulación de acción de evento

Para agregar una anulación de acción de evento, seleccione la acción de evento, actívela o desactívela y especifique el intervalo RR. Si está editando, no puede cambiar la acción de evento.

### Acción de evento

Seleccione una de las siguientes acciones de evento:

- **Deny Attacker Inline:** no transmite este paquete y paquetes futuros desde la dirección del atacante durante un período de tiempo especificado (sólo en línea).
- **Deny Connection Inline:** no transmite este paquete y paquetes futuros en el flujo TCP (sólo en línea).
- **Deny Packet Inline:** no transmite este paquete.
- **Produce Alert:** escribe una <evIdsAlert> en el registro.
- **Reset TCP Connection:** envía TCP resets para secuestrar y finalizar el flujo TCP.

### Activado

Haga clic en **Sí** para activar la anulación de acción de evento o en **No** para desactivarla. También puede activar y desactivar anulaciones de acción de evento en la ventana Anulación de acción de evento.

### Índice de riesgo

Especifique el límite inferior del intervalo RR en la casilla Mín y el límite superior del intervalo en la casilla Máx. Cuando el valor RR de un evento está dentro del intervalo especificado, Cisco IOS IPS agrega la anulación especificada por la Acción de evento. Por ejemplo, si a Deny Connection Inline se le asigna un intervalo RR de 90-100, y ocurre un evento con un RR de 95, Cisco IOS IPS responde denegando la conexión en línea.

## Editar IPS: Configuración SEAP: Filtros de acción de evento

Los filtros de acción de evento permiten que Cisco IOS IPS realice acciones individuales en respuesta a un evento sin requerir que ejecute todas las acciones o elimine el evento completo. Los filtros funcionan eliminando acciones de un evento. Un filtro que elimina todas las acciones de un evento elimina efectivamente dicho evento. Los filtros de acción de evento se procesan como una lista ordenada. Puede desplazar los filtros hacia arriba o hacia abajo en la lista para que el router procese un filtro antes que otros.

La ventana Filtros de acción de evento muestra los filtros de acción de evento configurados y permite reordenar la lista de filtros de modo que Cisco IOS IPS procesa los filtros en el orden deseado.

### Utilizar filtros de acción de evento

Seleccione **Utilizar filtros de acción de evento** para activar el uso de filtros de acción de evento. Puede agregar, editar y eliminar filtros de acción de evento y reorganizar la lista para especificar el orden en que el router procesará los filtros aunque no esté activado el filtrado de acción de evento.

### Área de lista de filtros de acción de evento

Para obtener una descripción de las columnas en el área de la lista de filtros de acción de evento, consulte [Agregar o editar un filtro de acción de evento](#).

### Botones de la lista de filtros de acción de evento

Los botones de la lista de filtros de acción de evento permiten crear, editar y eliminar filtros de acción de evento y colocar los filtros de acción de evento en el orden en que desea que se ubiquen en la lista. Los botones se describen en las siguientes secciones.

#### Seleccionar todo

El botón **Seleccionar todo** funciona con los botones **Activar**, **Desactivar** y **Eliminar**. Para activar o desactivar todos los filtros de acción de evento, haga clic en **Seleccionar todo** y luego en **Activar** o **Desactivar**. Para eliminar todos los filtros de acción de evento, haga clic en **Seleccionar todo** y, a continuación, en **Eliminar**.

### Agregar

Haga clic en el botón **Agregar** para agregar un filtro de acción de evento al final de la lista. Aparece un diálogo que permite especificar los datos para el filtro.

### Insertar antes

Para insertar un nuevo filtro de acción de evento antes de uno existente, seleccione la entrada de filtro existente y haga clic en **Insertar antes**. Aparece un diálogo que permite especificar los datos para el filtro.

### Insertar después

Para insertar un nuevo filtro de acción de evento después de uno existente, seleccione la entrada de filtro existente y haga clic en **Insertar después**. Aparece un diálogo que permite especificar los datos para el filtro.

### Desplazar hacia arriba

Seleccione un filtro de acción de evento y haga clic en el botón **Desplazar hacia arriba** para mover el filtro hacia arriba en la lista.

### Desplazar hacia abajo

Seleccione un filtro de acción de evento y haga clic en el botón **Desplazar hacia abajo** para mover el filtro hacia abajo en la lista.

### Editar

Haga clic en el botón **Editar** para editar un filtro de acción de evento seleccionado.

### Activar

Haga clic en el botón **Activar** para activar un filtro de acción de evento seleccionado. Para activar todos los filtros de acción de evento, haga clic en **Seleccionar todo** y, a continuación, en **Activar**.

### Desactivar

Haga clic en el botón **Desactivar** para desactivar un filtro de acción de evento seleccionado. Para desactivar todos los filtros de acción de evento, haga clic en **Seleccionar todo** y, a continuación, en **Desactivar**.

### Eliminar

Haga clic en el botón **Eliminar** para eliminar un filtro de acción de evento seleccionado. Si desea eliminar todos los filtros de acción de evento, haga clic en **Seleccionar todo** y, a continuación, en **Eliminar**.

### Aplicar cambios

Cuando haya especificado la información que desea en esta ventana, haga clic en **Aplicar cambios**. El botón Aplicar cambios se desactiva cuando no hay cambios para enviar al router.

### Descartar cambios

Si desea borrar la información que ha especificado en esta ventana, pero que no ha enviado al router, haga clic en **Descartar cambios**. El botón Descartar cambios se desactiva cuando no hay cambios en espera para enviarse al router.

## Agregar o editar un filtro de acción de evento

La siguiente información describe los campos en los diálogos Agregar y Editar filtro de acción de evento.

### Nombre

SDM proporciona nombres de filtro de acción de evento que comienzan con Q00000 y aumenta la parte numérica del nombre en 1 cada vez que agrega un filtro de acción de evento. También puede especificar un nombre que seleccione. Si está editando un filtro de acción de evento, el campo Nombre será de sólo lectura.

### Activado

Haga clic en **Sí** para activar el filtro de acción de evento o en **No** para desactivarlo. También puede activar y desactivar filtros de acción de evento en la ventana Filtro de acción de evento.

## ID de firma

Para ID de firma, especifique un intervalo de ID de firma desde 900 a 65535 o especifique un ID que se encuentre dentro de ese intervalo. Si especifica un intervalo, use un guión (-) para separar los límites superior e inferior del intervalo. Por ejemplo, especifique 988-5000.

## ID de subfirma

Para ID de subfirma, especifique un intervalo de ID de subfirma desde 0 a 255 o especifique un ID de subfirma en ese intervalo. Si especifica un intervalo, use un guión (-) para separar los límites superior e inferior del intervalo. Por ejemplo, especifique 70-200

## Dirección de atacante

Para dirección de atacante, especifique un intervalo de direcciones desde 0.0.0.0 a 255.255.255.255 o especifique una dirección que se encuentre dentro de ese intervalo. Si especifica un intervalo, use un guión (-) para separar los límites superior e inferior del intervalo. Por ejemplo, especifique 192.168.7.0-192.168.50.0.

## Puerto de atacante

Para puerto de atacante, especifique un intervalo de números de puerto desde 0 a 65535 o especifique un número de puerto que se encuentre dentro de ese intervalo. Si especifica un intervalo, use un guión (-) para separar los límites superior e inferior del intervalo. Por ejemplo, especifique 988-5000.

## Dirección de víctima

Para dirección de víctima, especifique un intervalo de direcciones desde 0.0.0.0 a 255.255.255.255 o especifique una dirección que se encuentre dentro de ese intervalo. Si especifica un intervalo, use un guión (-) para separar los límites superior e inferior del intervalo. Por ejemplo, especifique 192.168.7.0-192.168.50.0.

## Puerto de víctima

Para puerto de víctima, especifique un intervalo de números de puerto desde 0 a 65535 o especifique un número de puerto que se encuentre dentro de ese intervalo. Si especifica un intervalo, use un guión (-) para separar los límites superior e inferior del intervalo. Por ejemplo, especifique 988-5000.

## Índice de riesgo

Para índice de riesgo, especifique un intervalo **RR** entre 0 y 100.

## Acciones que se quitarán

Haga clic en las acciones que desea quitar de los eventos coincidentes. Para quitar más de una acción de los eventos coincidentes, mantenga presionada la tecla **Ctrl** cuando selecciona eventos adicionales. Todos los eventos que seleccione para este filtro aparecerán en la ventana Filtros de acción de evento.

## Detenerse en coincidencia

Si desea que Cisco IOS IPS se detenga cuando un evento coincide con este filtro de acción de evento, haga clic en **Sí**. Si desea que Cisco IOS IPS evalúe los eventos coincidentes con los otros filtros, haga clic en **No**.

## Comentarios

Puede agregar comentarios para describir el propósito de este filtro. Este campo es opcional.

## Editar IPS: Firmas

Cisco IOS IPS evita intrusiones al comparar el tráfico con las firmas de ataques conocidos. Las imágenes de Cisco IOS que admiten Cisco IOS IPS tienen firmas incorporadas que se pueden utilizar, y también puede hacer que Cisco IOS IPS importe firmas para que el router las utilice al examinar el tráfico. Las firmas importadas se guardan en un archivo de definición de firmas ([SDF](#)).

Esta ventana permite ver las firmas Cisco IOS IPS configuradas en el router. Es posible agregar firmas personalizadas o importar firmas desde archivos de definición de firmas (SDF) descargados desde Cisco.com. También es posible editar, eliminar, activar y desactivar las firmas.

Cisco IOS IPS se entrega con un archivo SDF que contiene firmas que su router puede usar. Para obtener más información acerca del SDF entregado con Cisco IOS IPS, y cómo hacer que Cisco IOS IPS lo utilice, haga clic en [Archivos de definición de firmas entregados con IPS](#).

### Árbol de firmas

El árbol de firmas permite que se filtre la lista de firmas al costado derecho, de acuerdo con el tipo de firma que desea visualizar. Primero, seleccione la rama para el tipo general de firmas que desea visualizar. La lista de firmas muestra las firmas configuradas para el tipo que seleccionó. Si un símbolo de sumar (+) aparece a la izquierda de la rama, hay subcategorías que usted puede usar para refinar el filtro. Haga clic en el signo + para expandir la rama y seleccione la subcategoría de firmas que desea visualizar. Si la lista de firmas está vacía, no existen firmas configuradas disponibles para ese tipo.

Por ejemplo: Si desea visualizar todas las firmas de ataque, haga clic en la carpeta **Ataque** de la rama. Si desea ver las subcategorías que es posible utilizar para filtrar la visualización de las firmas de ataque, haga clic en el signo + al lado de la carpeta Ataque. Si desea ver las firmas de Denegación de servicios (DoS), haga clic en la carpeta **DoS**.

## Botón Importar

Haga clic aquí para importar un archivo de definición de firmas desde el PC o desde el router. Cuando haya seleccionado el archivo, Cisco IOS IPS muestra las firmas disponibles en el archivo, y es posible seleccionar las que desee importar al router. Para obtener más información acerca de cómo seleccionar las firmas que se importarán, consulte [Importar firmas](#).



### Nota

---

Sólo es posible importar firmas desde el router si éste tiene un sistema de archivos basado en DOS.

---

Los archivos SDF están disponibles en Cisco. Haga clic en la siguiente URL para descargar un archivo SDF desde Cisco.com (requiere una conexión):

<http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup>

Cisco mantiene un centro de alerta que ofrece información sobre amenazas emergentes. Consulte el apartado [Cisco Security Center](#) para obtener más información.

## Lista Ver por/Criterios

Las listas desplegables Ver por y Criterios permiten filtrar la visualización según los tipos de firmas que desee ver. Primero seleccione los criterios en la lista desplegable Ver por y, a continuación, seleccione el valor de éstos en la lista desplegable Criterios.

Por ejemplo: Si selecciona **Motor** en la lista Ver por, la lista Criterios cambiará a Motor y permitirá seleccionar alguno de los motores disponibles como, por ejemplo, **Atomic.ICMP** y **Service.DNS**.

Si selecciona **ID de firma** o **Nombre de firma**, deberá especificar un valor en el campo de criterios.

## Total [n] Nuevas [n] Eliminadas [n]

Este texto muestra el recuento de las firmas nuevas y de las eliminadas.

## Seleccionar todo

Haga clic para seleccionar todas las firmas de la lista.



## Agregar

Haga clic en **Agregar** si desea efectuar una de las acciones siguientes:

- **Agregar nuevas**: seleccione esta opción para agregar una nueva firma y proporcionar parámetros de firma en el diálogo que aparece.
- **Clonar**: esta opción se activa si se selecciona una firma que no pertenece a un motor codificado por defecto. Está desactivada si la firma utiliza uno de los motores codificados por defecto de Cisco IOS.

## Editar

Haga clic en el botón Editar para editar los parámetros de la firma seleccionada.

## Eliminar

Haga clic en **Eliminar** para que la firma seleccionada se elimine de la lista. Para ver las firmas que eliminó, haga clic en **Detalles**. Para obtener más información acerca del estado y manejo de estas firmas, consulte [Firmas marcadas para su eliminación](#).



### Nota

---

Es posible visualizar y supervisar las firmas OPACL de TrendMicro, pero no es posible editarlas, eliminarlas, activarlas ni desactivarlas. Si se selecciona una firma OPACL de TrendMicro, se desactivan los botones **Editar**, **Eliminar**, **Activar** y **Desactivar**. El Servidor de control de incidentes de Cisco asume el control de estas firmas.

---

## Activar

Haga clic en **Activar** para activar la firma seleccionada. Las firmas activadas se indican mediante una marca verde. Una firma desactivada y activada posteriormente presenta un icono de espera amarillo en la columna ! para indicar que es preciso aplicar el cambio al router.

## Desactivar

Haga clic en **Desactivar** para desactivar la firma seleccionada. Las firmas desactivadas se designan mediante un icono rojo. Si se desactiva la firma durante la sesión actual, aparecerá un icono de espera amarillo en la columna ! para indicar que es preciso aplicar el cambio al router.

## Botón Resumen o Detalles

Haga clic en este botón para mostrar u ocultar las firmas marcadas para su eliminación.

## Lista Firmas


Muestra las firmas recuperadas del router y cualquier firma agregada desde un SDF.



### Nota

Las firmas seleccionadas para importar que sean idénticas a las firmas implementadas no se importarán y no aparecerán en la lista de firmas.

La lista de firmas se puede filtrar mediante los controles de selección.

<b>Activado</b>	Las firmas activadas se indican mediante un icono verde. Si están activadas, se ejecutan las acciones especificadas cuando se detecta la firma.  Las firmas desactivadas se indican mediante un icono rojo. Si están desactivadas, se desactivan también las acciones, que no se ejecutarán.
<b>Alerta (!)</b>	Esta columna puede contener el icono de espera amarillo.    Este icono sirve para indicar firmas nuevas o firmas modificadas que no se han enviado al router.
<b>ID de firma</b>	ID numérico de la firma. Por ejemplo: el ID de la firma de ICMP Echo Reply es 2000.
<b>ID de subfirma</b>	ID de la subfirma.
<b>Nombre</b>	Nombre de la firma. Por ejemplo: ICMP Echo Reply.
<b>Acción</b>	Acción que se ejecutará al detectar la firma.
<b>Filtro</b>	ACL asociada a la firma correspondiente.
<b>Gravedad</b>	Nivel de gravedad del evento. Los niveles de gravedad son: informativo, inferior, medio y superior.
<b>Motor</b>	Motor al que pertenece la firma.

### Menú contextual del botón derecho del ratón

Si hace clic con el botón derecho sobre una firma, Cisco SDM mostrará un menú contextual con las siguientes opciones:

- Acciones: haga clic en esta opción para seleccionar las acciones que se ejecutarán cuando coincida la firma. Consulte el apartado [Asignar acciones](#) para obtener más información.
- Definir la gravedad en: haga clic en esta opción para configurar el nivel de gravedad de una firma en: alta, media, baja o informativa.
- Restaurar los valores por defecto: haga clic en esta opción para restaurar los valores por defecto de una firma.
- Quitar filtro: haga clic en esta opción para quitar un filtro aplicado a la firma.
- Ayuda NSDB (se necesita una cuenta CCO): haga clic en esta opción para visualizar la ayuda en la base de datos de seguridad de la red (NSDB).

### Firmas marcadas para su eliminación

Esta área se puede ver si hace clic en el botón **Detalles**. Enumera las firmas eliminadas de la Lista de firmas y las firmas marcadas para su eliminación dado que se especificó que las firmas importadas deben reemplazar a las firmas ya configuradas en el router. Consulte el apartado [Cómo importar firmas](#) para obtener más información.

Las firmas marcadas para su eliminación permanecen activas en la configuración de Cisco IOS IPS hasta que se hace clic en **Aplicar cambios**. Si sale de la ventana Firmas y desactiva Cisco IOS IPS, las firmas marcadas se eliminarán si se vuelve a activar Cisco IOS IPS.

#### Botón Anular eliminación de todos

Haga clic en este botón para restablecer todas las firmas en la lista de las firmas marcadas y eliminadas.

#### Botón Anular eliminación

Haga clic en este botón para restaurar las firmas especificadas marcadas para su eliminación. Al hacer clic, se eliminará la marca de las firmas y éstas volverán a figurar en la lista de firmas activas.

## Botón Aplicar cambios

Haga clic en este botón para enviar al router las firmas importadas recientemente, las ediciones de firmas y las firmas activadas o desactivadas recientemente. Al aplicarse los cambios, el icono amarillo de espera desaparecerá de la columna !. Estos cambios se guardan en la memoria flash del router en el archivo sdmips.sdf. Este archivo se crea automáticamente la primera vez que hace clic en **Aplicar cambios**.



### Nota

Si intenta importar firmas y estas firmas son idénticas a las firmas implementadas, el botón **Aplicar cambios** estará desactivado.

## Botón Descartar cambios

Haga clic en este botón para descartar los cambios acumulados.



### Nota

Si intenta importar firmas y estas firmas son idénticas a las firmas implementadas, el botón **Descartar cambios** estará desactivado.

## Puerto de víctima

Para puerto de víctima, especifique un intervalo de números de puerto desde 0 a 65535 o especifique un número de puerto que se encuentre dentro de ese intervalo. Si especifica un intervalo, use un guión (-) para separar los límites superior e inferior del intervalo. Por ejemplo, especifique 988-5000.

## Índice de riesgo

Para índice de riesgo, especifique un intervalo **RR** entre 0 y 100.

## Acciones que se quitarán

Haga clic en las acciones que desea quitar de los eventos coincidentes. Para quitar más de una acción de los eventos coincidentes, mantenga presionada la tecla **Ctrl** cuando selecciona eventos adicionales. Todos los eventos que seleccione para este filtro aparecerán en la ventana Filtros de acción de evento.

## Detenerse en coincidencia

Si desea que Cisco IOS IPS se detenga cuando un evento coincide con este filtro de acción de evento, haga clic en **Sí**. Si desea que Cisco IOS IPS evalúe los eventos coincidentes con los otros filtros, haga clic en **No**.

## Comentarios

Puede agregar comentarios para describir el propósito de este filtro. Este campo es opcional.

## Editar IPS: Firmas

Cisco IOS IPS evita intrusiones al comparar el tráfico con las firmas de ataques conocidos. Las imágenes de Cisco IOS que admiten Cisco IOS IPS tienen firmas incorporadas que Cisco IOS IPS puede utilizar, y también puede hacer que Cisco IOS IPS importe firmas para que el router las utilice al examinar el tráfico. Las firmas importadas se guardan en un archivo de definición de firmas (SDF).

Este tema de ayuda describe la ventana Firmas que aparece cuando el router ejecuta Cisco IOS 12.4(11)T y versiones posteriores.

La ventana Firmas permite ver las firmas Cisco IOS IPS configuradas en el router. Es posible agregar firmas personalizadas o importar firmas desde archivos de definición de firmas (SDF) descargados desde Cisco.com. También puede editar, activar, desactivar, retirar y dejar sin efecto el retiro de las firmas.

## Árbol de firmas

El árbol de firmas permite que se filtre la lista de firmas al costado derecho, de acuerdo con el tipo de firma que desea visualizar. Primero, seleccione la rama para el tipo general de firmas que desea visualizar. La lista de firmas muestra las firmas configuradas para el tipo que seleccionó. Si un símbolo de sumar (+) aparece a la izquierda de la rama, hay subcategorías que usted puede usar para refinar el filtro. Haga clic en el signo + para expandir la rama y seleccione la subcategoría de firmas que desea visualizar. Si la lista de firmas está vacía, no existen firmas configuradas disponibles para ese tipo.

Por ejemplo: Si desea visualizar todas las firmas de ataque, haga clic en la carpeta **Ataque** de la rama. Si desea ver las subcategorías que es posible utilizar para filtrar la visualización de las firmas de ataque, haga clic en el signo + al lado de la carpeta Ataque. Si desea ver las firmas de Denegación de servicios (DoS), haga clic en la carpeta **DoS**.

## Botón Importar

Haga clic aquí para importar un archivo de definición de firmas desde el PC o desde el router. Cuando haya seleccionado el archivo, Cisco IOS IPS muestra las firmas disponibles en el archivo, y puede seleccionar las que desee importar al router. Para obtener más información acerca de cómo seleccionar las firmas que se importarán, consulte [Importar firmas](#).



### Nota

---

Sólo es posible importar firmas desde el router si éste tiene un sistema de archivos basado en DOS.

---

Los archivos SDF están disponibles en Cisco. Haga clic en la siguiente URL para descargar un archivo SDF desde Cisco.com (requiere una conexión):

<http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup>

Cisco mantiene un centro de alerta que ofrece información sobre amenazas emergentes. Consulte el apartado [Cisco Security Center](#) para obtener más información.

## Lista Ver por/Criterios

Las listas desplegables Ver por y Criterios permiten filtrar la visualización según los tipos de firmas que desee ver. Primero seleccione los criterios en la lista desplegable Ver por y, a continuación, seleccione el valor de éstos en la lista desplegable Criterios.

Por ejemplo: Si selecciona **Motor** en la lista Ver por, la lista Criterios cambiará a Motor y permitirá seleccionar alguno de los motores disponibles como, por ejemplo, **Atomic.ICMP** y **Service.DNS**.

Si selecciona **ID de firma** o **Nombre de firma**, deberá especificar un valor en el campo de criterios.

## Total [n]

Este texto muestra el número total de las firmas en el router.

## Seleccionar todo

Haga clic para seleccionar todas las firmas de la lista.

## Lista Ver por/Criterios

Las listas desplegables Ver por y Criterios permiten filtrar la visualización según los tipos de firmas que desee ver. Primero seleccione los criterios en la lista desplegable Ver por y, a continuación, seleccione el valor de éstos en la lista desplegable Criterios.

Por ejemplo: Si selecciona **Motor** en la lista Ver por, la lista Criterios cambiará a Motor y permitirá seleccionar alguno de los motores disponibles como, por ejemplo, **Atomic.ICMP** y **Service.DNS**.

Si selecciona **ID de firma** o **Nombre de firma**, deberá especificar un valor en el campo de criterios.

## Total [n]

Este texto muestra el número total de las firmas en el router.

## Seleccionar todo

Haga clic para seleccionar todas las firmas de la lista.

## Desactivar

Haga clic en **Desactivar** para desactivar la firma seleccionada. Las firmas desactivadas se designan mediante un icono rojo. Si se desactiva la firma durante la sesión actual, aparecerá un icono de espera amarillo en la columna ! para indicar que es preciso aplicar el cambio al router.

## Retire

Haga clic en **Retire** para evitar que una firma se compile para exploración.

## Unretire

Haga clic en **Unretire** para permitir que la firma se compile para exploración.

## Lista Firmas


Muestra las firmas recuperadas del router y cualquier firma agregada desde un SDF.



**Nota**

Las firmas seleccionadas para importar que sean idénticas a las firmas implementadas no se importarán y no aparecerán en la lista de firmas.

La lista de firmas se puede filtrar mediante los controles de selección.

<b>Activado</b>	Las firmas activadas se indican mediante un icono verde. Si están activadas, se ejecutan las acciones especificadas cuando se detecta la firma.  Las firmas desactivadas se indican mediante un icono rojo. Si están desactivadas, se desactivan también las acciones, que no se ejecutarán.
<b>Alerta (!)</b>	Esta columna puede contener el icono de espera amarillo.    Este icono sirve para indicar firmas nuevas o firmas modificadas que no se han enviado al router.
<b>ID de firma</b>	ID numérico de la firma. Por ejemplo: el ID de la firma de ICMP Echo Reply es 2000.
<b>ID de subfirma</b>	ID de la subfirma.
<b>Nombre</b>	Nombre de la firma. Por ejemplo: ICMP Echo Reply.
<b>Acción</b>	Acción que se ejecutará al detectar la firma.
<b>Gravedad</b>	Nivel de gravedad del evento. Los niveles de gravedad son: informativo, inferior, medio y superior.
<b>Índice de fidelidad</b>	El <a href="#">índice de fidelidad</a> de la firma.
<b>Retirado</b>	Un valor verdadero o falso. Verdadero si la firma se ha retirado. Falso en caso contrario. Las firmas retiradas no se compilan.
<b>Motor</b>	Motor al que pertenece la firma.



### Menú contextual del botón derecho del ratón

Si hace clic con el botón derecho sobre una firma, Cisco SDM mostrará un menú contextual con las siguientes opciones:

- Acciones: haga clic en esta opción para seleccionar las acciones que se ejecutarán cuando coincida la firma. Consulte el apartado [Asignar acciones](#) para obtener más información.
- Índice de fidelidad: haga clic para especificar un [índice de fidelidad](#) para la firma.
- Definir la gravedad en: haga clic en esta opción para configurar el nivel de gravedad de una firma en: alta, media, baja o informativa.
- Restaurar los valores por defecto: haga clic en esta opción para restaurar los valores por defecto de una firma.
- Ayuda NSDB (se necesita una cuenta CCO): haga clic en esta opción para visualizar la ayuda en la base de datos de seguridad de la red (NSDB).

### Aplicar cambios

Haga clic en **Aplicar cambios** para enviar al router las firmas importadas recientemente, las ediciones de firmas y las firmas activadas o desactivadas recientemente. Al aplicarse los cambios, el icono amarillo de espera desaparecerá de la columna !. Estos cambios se guardan en la memoria flash del router en el archivo sdmips.sdf. Este archivo se crea automáticamente la primera vez que hace clic en **Aplicar cambios**.



#### Nota

---

Si intenta importar firmas y estas firmas son idénticas a las firmas implementadas, el botón **Aplicar cambios** estará desactivado.

---

### Descartar cambios

Haga clic en **Descartar cambios** para descartar los cambios acumulados.



#### Nota

---

Si intenta importar firmas y estas firmas son idénticas a las firmas implementadas, el botón **Descartar cambios** estará desactivado.

---

## Editar firma

Use los campos en el diálogo Editar firma para editar la firma seleccionada. Los cambios que realiza se guardan en un [archivo delta](#) que se guarda en la memoria flash del router. Los elementos de firmas se describen en las siguientes secciones.

Este tema de ayuda describe la ventana Editar firmas que aparece cuando el router ejecuta Cisco IOS 12.4(11)T y versiones posteriores.

### ID de firma

Valor numérico exclusivo asignado a esta firma. Este valor permite a Cisco IOS IPS identificar una firma específica.

### ID de subfirma

Valor numérico exclusivo asignado a esta subfirma. El ID de subfirma se utiliza para identificar una parte de la firma.

### Gravedad de alerta

Seleccione uno de los siguientes niveles para categorizar la gravedad de la alerta: alta, media, baja o informativa.

### Índice de fidelidad de firma

El índice de fidelidad de firma es un valor definido por el autor de la firma para cuantificar la confianza de que la firma producirá valores positivos verdaderos. Este valor se define antes de que se implemente una firma y puede ajustarse cuando están disponibles los datos de rendimiento de firma.

### Promiscuous Delta (Delta promiscuo)

Promiscuous Delta es un factor que se resta del índice de riesgo (RR) de un evento cuando el router está operando en modo promiscuo. El delta promiscuo se resta del RR siempre que se desencadena una alerta cuando el sistema se implementa en modo promiscuo.

**Nota**

---

Aunque el delta promiscuo se puede volver a configurar según la firma, no se recomienda que cambie la configuración predefinida del delta promiscuo.

---

## Descripción de firma

La descripción de firma incluye el nombre y la versión de la firma, las notas de alerta disponibles del [Cisco Security Center](#), comentarios del usuario e información adicional.

## Motor

El [motor de firmas](#) asociado a esta firma. Atomic IP es un motor que se usa con frecuencia.

La casilla Motor contiene campos que permiten ajustar una gran variedad de parámetros de firma. Por ejemplo, puede especificar la acción a realizar si coincide esta firma y se genera un evento, puede especificar el protocolo de capa 4 para inspeccionar en busca de eventos que coincidan con esta firma, y puede especificar parámetros IP, como longitud de encabezado y tipo de servicio.

## Event Counter (Contador de evento)

Los controles de la casilla Event Counter permiten especificar los parámetros descritos en las siguientes secciones.

### Event Count (Recuento de evento)

El número de veces que debe ocurrir un evento antes de que se genere una alerta.

### Event Count Key (Clave de recuento de evento)

El tipo de información que se usa para hacer el recuento de un evento mientras ocurre. Por ejemplo, si selecciona las **direcciones y los puertos del atacante y de la víctima**, cada vez que tiene estos 4 elementos de información para un evento, el recuento aumenta en 1. Si selecciona **dirección de atacante**, sólo se necesita esa información.

### Event Interval (Intervalo de evento)

El número de segundos entre eventos que se envían al registro. Si selecciona **Sí**, aparece un campo adicional que permite especificar el número de segundos.

## Alert Frequency (Frecuencia de alerta)

El propósito del parámetro de frecuencia de alerta es reducir el volumen de las alertas escritas en el registro.

### Summary Mode (Modo Resumen)

Existen cuatro modos: Fire All (Activar todas), Fire Once (Activar una vez), Summarize (Resumir) y Global Summarize (Resumir globalmente). El modo Resumen se cambia dinámicamente para adaptarse al volumen de alerta actual. Por ejemplo, puede configurar la firma en Activar todas, pero después de alcanzar un cierto umbral, comienza a resumir.

### Summary Key (Clave de resumen)

El tipo de información que se usa para determinar cuándo resumir. Por ejemplo, si selecciona las **direcciones y los puertos del atacante y de la víctima**, cada vez que tiene estos 4 elementos de información para un evento, se produce el resumen. Si selecciona **dirección de atacante**, sólo se necesita esa información.

### Especificar umbral de resumen global

Opcionalmente, puede especificar umbrales numéricos para determinar cuándo resumir eventos en el registro. Si selecciona **Sí**, puede especificar un umbral de resumen global y un intervalo de resumen.

## Estado

En la casilla Estado, puede especificar si la firma debe activarse, desactivarse o retirarse. Además, la casilla Estado puede mostrar las firmas que están obsoletas.

## Selección de archivos

Esta ventana permite cargar un archivo desde el router. Esta ventana sólo permite ver sistemas de archivos DOSFS.

El lado izquierdo de la ventana muestra un árbol expansible que representa el sistema de directorio de la memoria flash de su router Cisco y de los dispositivos USB conectados a ese router.

El lado derecho de la ventana muestra una lista con los nombres de los archivos y directorios encontrados en el directorio especificado en el lado izquierdo de la ventana. También muestra el tamaño de cada archivo en bytes, así como la fecha y hora de la última modificación de cada archivo y directorio.

Es posible seleccionar un archivo para cargar de la lista al lado derecho de la ventana. Bajo la lista de archivos, se encuentra un campo Nombre de archivo que contiene la ruta completa del archivo seleccionado.



---

**Nota**

---

Si se está seleccionando un archivo de configuración para provisionar su router, el archivo debe ser un archivo CCD o tener una extensión .cfg.

---

### Nombre

Haga clic en **Nombre** para ordenar los archivos y directorios alfabéticamente por nombre. Haga clic en **Nombre** nuevamente para invertir el orden.

### Tamaño

Haga clic en **Tamaño** para ordenar los archivos y directorios por tamaño. Los directorios siempre tienen un tamaño de cero bytes, aunque no estén vacíos. Haga clic en **Tamaño** nuevamente para invertir el orden.

### Hora de modificación

Haga clic en **Hora de modificación** para ordenar los archivos y directorios por fecha y hora de modificación. Haga clic en **Hora de modificación** nuevamente para invertir el orden.

## Asignar acciones

Esta ventana contiene las acciones que pueden ejecutarse al detectarse la coincidencia de una firma. Las acciones disponibles dependen de la firma, aunque a continuación, enumeramos las acciones más comunes:

- **alarm**: genera un mensaje de alarma. Igual que **produce-verbose-alert**.
- **deny-attacker-inline**: crea una ACL que deniega todo el tráfico desde la dirección IP que se considera el origen del ataque por parte del sistema Cisco IOS IPS. Igual que **denyAttackerInline**.
- **deny-connection-inline**: rechaza el paquete y todos los paquetes futuros en este flujo de TCP. Igual que **produce-alert** y **denyFlowInline**.
- **deny-packet-inline**: no transmite este paquete (en línea únicamente). Igual que **drop**.
- **denyAttackerInline**: crea una ACL que deniega todo el tráfico desde la dirección IP que se considera el origen del ataque por parte del sistema Cisco IOS IPS. Igual que **deny-attacker-inline**.
- **denyFlowInline**: crea una ACL que deniega todo el tráfico desde la dirección IP que se considera el origen del ataque que pertenece a 5-tuple (src ip, src port, dst ip, dst port y protocolo I4). **denyFlowInline** es más granular que **denyAttackerInline**. Igual que **produce-alert** y **deny-connection-inline**.
- **drop**: rechaza el paquete no válido. Igual que **deny-packet-inline**.
- **produce-alert**: genera una alerta. Igual que **denyFlowInline** y **deny-connection-inline**.
- **produce-verbose-alert**: genera una alerta que incluye un volcado codificado del paquete no válido. Igual que **alarm**.
- **reset**: restablece la conexión y rechaza el paquete no válido. Igual que **reset-tcp-connection**.
- **reset-tcp-connection**: envía TCP RESETS para finalizar el flujo TCP. Igual que **restablecer**.

## Importar firmas

Use la ventana Importar IPS para importar firmas desde un archivo SDF u otro archivo en el equipo. La información de esta ventana indica qué firmas están disponibles en el archivo SDF y cuáles ya están implementadas en el router.

### Cómo importar firmas

Para importar firmas, siga los pasos descritos a continuación:

---

**Paso 1** Use el árbol de firmas, la lista desplegable Ver por y la lista desplegable Lista de criterios para mostrar las firmas que desee importar.

En la lista de firmas, anule la selección de la casilla de verificación **Importar** para las firmas que *no* desee importar. Si desea anular la selección de la casilla de verificación **Importar** para todas las firmas, haga clic en el botón **Borrar todo**, que cambiará al botón **Seleccionar todo**.

**Paso 2** Marque la casilla de verificación **No importe firmas definidas como Desactivadas** si no desea importar firmas cuya utilización pueda perjudicar el rendimiento del router.

**Paso 3** Haga clic en el botón **Combinar** para combinar las firmas importadas con las firmas ya configuradas en el router o el botón **Sustituir** para reemplazar las firmas ya configuradas.

Consulte [Botón Combinar](#) y [Botón Sustituir](#) para obtener más información.

**Paso 4** Haga clic en el botón **Aplicar cambios** en la ventana Editar IPS para implementar las firmas importadas.

Puede modificar las firmas importadas antes de implementarlas. No se importarán las firmas seleccionadas para importar que sean idénticas a las firmas implementadas. Si todas las firmas importadas son idénticas a las firmas implementadas, el botón **Aplicar cambios** estará desactivado.

---

## Árbol de firmas

Si se necesita una descripción del árbol de firmas, haga clic en este enlace: [Árbol de firmas](#). Es posible utilizar el árbol de firmas en esta ventana para reunir las firmas que se desea importar, categoría por categoría.

Por ejemplo: es posible que desee agregar firmas desde la categoría OS y desde la categoría Servicios. Esto se logra seleccionando la rama **OS** del árbol, y cualquier rama de esa parte del árbol que desee, como la rama UNIX o la rama Windows. Cuando se visualizan los tipos de firmas que desea importar, es posible hacer selecciones en el área de lista de firmas. Luego, es posible seleccionar la rama **Servicio** y seleccionar cualquiera de las firmas de servicio que desee.

## Lista Ver por/Criterios

Los cuadros de lista Ver por/Criterios permiten filtrar la visualización según los tipos de firmas que desee ver. Primero seleccione los criterios en la lista Ver por y, a continuación, seleccione el valor de éstos en la lista a la derecha (la lista de criterios).

Por ejemplo: Si selecciona **Motor** en la lista Ver por, la lista de criterios se etiquetará como Motor y permitirá seleccionar alguno de los motores disponibles como, por ejemplo, **Atomic.ICMP** y **Service.DNS**.

Si selecciona **ID de firma** o **Nombre de firma**, deberá especificar un valor en la lista de criterios.

## Área de lista de firmas

La lista de firmas muestra las firmas disponibles en el archivo SDF según los criterios seleccionados en el árbol de firmas. El texto de firmas ya encontrado en el router de destino está de color azul.

El área de lista de firmas tiene las siguientes columnas:

- ID de firma: valor numérico exclusivo asignado a la firma. Este valor permite a Cisco IOS IPS identificar una firma específica.
- Nombre: nombre de la firma. Por ejemplo: *FTP Improper Address*.
- Gravedad: alta, media, baja o informativa.



- Implementada: si la firma ya está implementada en el router, esta columna contiene *Sí* . Si la firma no está implementada en el router, esta columna contiene *No* .
- Importar: esta columna contiene una casilla de verificación para cada firma. Si desea importar la firma, marque esta casilla.

**Nota**

---

Todas las firmas importadas desde un archivo SDF o .zip con el nombre IOS-Sxxx.zip pueden mostrarse en la lista de firmas. Cuando las firmas se importan desde un archivo .zip con un nombre diferente, sólo se mostrarán las firmas encontradas a través de las listas desplegables Ver por y Lista de criterios.

---

**Botón Combinar**

Haga clic en esta opción para combinar las firmas que está importando con las firmas que ya están configuradas en el router.

**Botón Sustituir**

Haga clic en esta opción para reemplazar las firmas ya configuradas en el router con las firmas que desee importar. Las firmas ya configuradas en el router que *no* se encuentran en la lista de firmas que desea importar están marcadas para su eliminación y se enumeran en **Firmas marcadas para su eliminación** en **Editar IPS > Firmas**. Consulte el apartado [Firmas marcadas para su eliminación](#) para obtener más información.

**Agregar, editar o duplicar firma**

Esta ventana contiene campos y valores descritos en la sección Definiciones de campos. Los campos varían en función de la firma, por consiguiente, no presentaremos una lista exhaustiva de todos los campos que pueda ver.

## Definiciones de campos

Los campos que se indican a continuación se encuentran en las ventanas Agregar, Editar y Clonar firmas.

- **ID de firma:** valor numérico exclusivo asignado a la firma. Este valor permite a Cisco IOS IPS identificar una firma específica.
- **Nombre de firma:** nombre asignado a la firma.
- **ID de subfirma:** valor numérico único asignado a esta subfirma. El ID de subfirma se utiliza para identificar una porción de la firma.
- **AlarmInterval:** manejo especial de eventos previstos. Utilice AlarmInterval Y con MinHits X para X alarmas en intervalos de Y segundos.
- **AlarmSeverity:** gravedad indicada en la alarma para esta firma.
- **AlarmThrottle:** técnica utilizada para lanzar alarmas.
- **AlarmTraits:** rasgos definidos por el usuario que describen más detalladamente la firma.
- **ChokeThreshold:** valor umbral de los intervalos de alarmas de los modos AlarmThrottle para cambiar de uno a otro. Si ChokeThreshold está definido, Cisco IOS IPS activa automáticamente los modos AlarmThrottle cuando detecte un gran número de alarmas en ThrottleInterval.
- **Enabled:** muestra si la firma está o no activada. Es preciso que la firma esté activada para que Cisco IOS IPS proteja contra el tráfico especificado por dicha firma.
- **EventAction:** muestra las acciones que Cisco IOS IPS ejecutará cuando se active esta firma.
- **FlipAddr:** “True” si las direcciones de origen y destino, y sus puertos asociados se intercambian en el mensaje de alarma. “False”, si no se produce un intercambio (por defecto).
- **MinHits:** número mínimo de ocurrencias de la firma antes de que se envíe un mensaje de alarma. Una ocurrencia es la aparición de la firma en la clave de la dirección.
- **SigComment:** comentario o texto de descripción de la firma.

- **SigVersion:** versión de la firma.
- **ThrottleInterval:** número de segundos que definen un intervalo de Alarm Throttle. Se utiliza con el parámetro AlarmThrottle para ajustar limitadores especiales de la alarma.
- **WantFrag:** “True” activa la inspección de los paquetes fragmentados únicamente. “False” activa la inspección de los paquetes no fragmentados únicamente. Seleccione “no definido” para activar la inspección de los paquetes fragmentados y no fragmentados.

## Cisco Security Center

El Cisco Security Center ofrece información sobre amenazas emergentes y enlaces a las firmas Cisco IOS IPS disponibles para proteger la red de ellas. En este enlace están disponibles los informes y las descargas (requiere inicio de sesión):

<http://tools.cisco.com/MySDN/Intelligence/searchSignatures.x>

## Archivos de definición de firmas entregados con IPS

Para asegurar que el router tiene disponibles todas las firmas que su memoria pueda conservar, Cisco SDM se entrega con uno de los siguientes archivos SDF:

- 256MB.sdf: si la cantidad de RAM disponible es mayor que 256 MB. El archivo 256MB.sdf contiene 500 firmas.
- 128MB.sdf: si la cantidad de RAM disponible está entre 128 MB y 256 MB. El archivo 128MB.sdf contiene 300 firmas.
- attack-drop.sdf: si la cantidad de RAM disponible es de 127 MB o menos. El archivo attack-drop.sdf contiene 82 firmas.

Si el router ejecuta Cisco IOS versión 12.4(11)T o posterior, debe utilizar un archivo SDF que tenga un nombre del formato sigv5-SDM-Sxxx.zip; por ejemplo, sigv5-SDM-S260.zip.



### Nota

El router debe estar ejecutando Cisco IOS versión 12.3(14)T o posterior para poder utilizar todos los motores de firmas disponibles en archivos 256MB.sdf y 128MB.sdf. Si el router usa una versión anterior, no estarán disponibles todos los motores de firmas.

Para utilizar un archivo SDF en la memoria del router, determine qué archivo SDF se ha instalado y configure Cisco IOS IPS para que lo utilice. Los procedimientos indicados a continuación le indican cómo hacerlo.

### Determinar qué archivo SDF está en la memoria

Para determinar qué archivo SDF está en la memoria del router, abra una sesión Telnet al router, y especifique el comando **show flash** . La salida será similar a lo siguiente:

```
System flash directory:
File Length Name/status
  1 10895320 c1710-k9o3sy-mz.123-8.T.bin
  2 1187840 ips.tar
  3 252103 attack-drop.sdf
  4 1038 home.shtml
  5 1814 sdmconfig-1710.cfg
  6 113152 home.tar
  7 758272 es.tar
  8 818176 common.tar
[14028232 bytes used, 2486836 available, 16515068 total]
16384K bytes of processor board System flash (Read/Write)
```

En este ejemplo, el archivo **attack-drop.sdf** se encuentra en la memoria del router. En algunos routers, como los que tienen un sistema de archivos de disco, se utiliza el comando **dir** para visualizar el contenido de la memoria del router.

### Configuración de IPS para utilizar un SDF

Para hacer que Cisco IOS IPS utilice el archivo SDF en la memoria del router, haga lo siguiente:

- 
- Paso 1** Haga clic en **Configuración global**.
  - Paso 2** En la lista Ubicaciones de SDF configurados, haga clic en **Agregar**.
  - Paso 3** En el cuadro de diálogo que aparece, haga clic en **Especificar SDF en flash** e indique el nombre del archivo SDF.
  - Paso 4** Haga clic en **Aceptar** para cerrar el cuadro de diálogo.
-

# Panel de seguridad

El Panel de seguridad le permite mantener actualizado el router con firmas para las amenazas de seguridad más recientes. Debe configurar Cisco IOS IPS en el router antes de implementar las firmas utilizando el Panel de seguridad.

## Tabla Amenazas más frecuentes

La tabla Amenazas más frecuentes muestra las últimas amenazas más frecuentes de Cisco en el caso de que el estado de las firmas asociadas indique que están disponibles para su implementación o bajo investigación. Algunas de las últimas amenazas de la tabla están asociadas a firmas que pueden implementarse en el router. El texto de firmas ya encontrado en el router está de color azul.

Para obtener las últimas amenazas más frecuentes, haga clic en el botón **Actualizar lista de amenazas más frecuentes**.



### Nota

---

No puede actualizar las amenazas más frecuentes utilizando el botón **Actualizar** de Cisco SDM o el comando Actualizar del explorador.

---

La tabla de amenazas más frecuentes incluye las siguientes columnas:

- **Estado del dispositivo:** indica si la firma asociada a la amenaza ya está activada en el router. Es posible que aparezca el siguiente símbolo en la columna Estado del dispositivo:
  - ✔ La firma ya está activada en el router.
  - ⋯ La firma no está disponible en el router o está disponible pero *no* está activada.
- **ID de firma** es un número único que identifica la firma asociada a la amenaza.
- **ID de subfirma** es un número único que identifica la subfirma. Si la firma asociada a la amenaza no posee una subfirma, el **ID de subfirma** es 0.
- **Nombre** es el nombre asignado a la amenaza.
- **Urgencia** indica si el nivel de la amenaza es alto (Mantenimiento de prioridad) o normal (Mantenimiento estándar).

- **Estado de la amenaza** indica si la firma asociada a la amenaza está disponible o si la amenaza aún está bajo investigación.
- **Implementar** contiene las casillas de verificación que pueden seleccionarse si la firma asociada a la amenaza está disponible para su implementación.

## Seleccionar SDF

Haga clic en el botón **Examinar** y seleccione el archivo SDF de Cisco IOS que desee utilizar. El archivo SDF de Cisco IOS debe estar presente en su equipo. El formato que tiene el nombre de archivo depende de la versión de Cisco IOS que ejecuta el router.

- Si el router ejecuta una imagen de Cisco IOS anterior a 12.4(11)T, el SDF debe tener un nombre con el formato IOS-Sxxx.zip, donde xxx es un número de tres dígitos. Por ejemplo: un archivo SDF de Cisco IOS IPS puede tener el nombre IOS-S193.zip.
- Si el router ejecuta una imagen de Cisco IOS versión 12.4(11)T o posterior, el archivo SDF debe tener un nombre con el formato sigv5-SDM-Sxxx.zip; por ejemplo, sigv5-SDM-S260.zip.

La ubicación de un archivo SDF de Cisco IOS que seleccione se muestra en el campo Ubicación del archivo SDF. El campo Ubicación del archivo SDF es de sólo lectura.

Después de descargar un archivo SDF de Cisco IOS por primera vez, Cisco SDM recuerda la ubicación del archivo. La próxima vez que cargue el Panel de seguridad, Cisco SDM seleccionará el último archivo SDF de Cisco IOS en función del número de tres dígitos incluido en el nombre del archivo.



### Nota

---

El archivo SDF de Cisco IOS con el número de tres dígitos más alto en su nombre será el archivo SDF de Cisco IOS más reciente.

---

## Implementación de firmas desde la tabla Amenazas más frecuentes

Antes de intentar la implementación de firmas desde la tabla Amenazas más frecuentes, asegúrese de haber:

- Configurado Cisco IOS IPS en el router
- Descargado el archivo de Cisco IOS más reciente en el equipo

Para implementar firmas desde la tabla Amenazas más frecuentes, siga los pasos descritos a continuación:

- 
- Paso 1** Haga clic en el botón **Actualizar lista de amenazas más frecuentes** para asegurarse de que tenga la última lista de amenazas más frecuentes.
- Paso 2** En la columna Implementar, marque la casilla de verificación de cada firma de amenaza más frecuente que desee implementar de la tabla Amenazas más frecuentes.
- Sólo se pueden seleccionar las amenazas más frecuentes cuyo estado sea **Firma disponible**. Las firmas disponibles con un icono rojo en la columna Aplicado se especifican automáticamente para su implementación.
- Paso 3** Haga clic en el botón **Examinar** y seleccione el archivo de Cisco IOS más reciente si necesita asegurarse de estar utilizando el archivo de firmas más reciente.
- Es posible que necesite hacer esto si la ubicación del archivo SDF más reciente se ha modificado desde que se especificó por última vez en el Panel de seguridad, o si el formato del nombre no es IOS-Sxxx.zip, donde xxx es un número de tres dígitos.
- Paso 4** Haga clic en el botón **Implementar firmas** para implementar las firmas seleccionadas en el router.
- Si alguna de las firmas seleccionadas no se encuentra en el archivo de Cisco IOS, se mostrará una advertencia. No obstante, todas las firmas encontradas aún podrán implementarse. Después de implementadas en el router, las firmas se activan automáticamente y se agregan a la lista de firmas activas del router.
-

# Migración IPS

Si tiene una configuración existente de Cisco IOS IPS que desea migrar a Cisco IOS IPS, disponible en Cisco IOS 12.4(11)T o versiones posteriores, puede utilizar el asistente para migración de IPS para efectuar la migración.

**Nota**

Si el router utiliza una imagen de Cisco IOS de la versión 12.4(11)T o posterior, debe migrar una configuración creada antes de esta versión si desea usar Cisco IOS IPS en el router. Si no migra la configuración, no se cambiarán los comandos de configuración, pero Cisco IOS IPS no funcionará.

Haga clic en el botón **Iniciar asistente para migración de IPS** para comenzar el proceso de migración.

## Asistente para migración: Bienvenido

En la ventana de bienvenida al asistente para migración se enumeran las tareas que el asistente ayuda a realizar. Haga clic en **Cancelar** si no desea ejecutar el asistente para la migración de IPS.

El asistente para migración de IPS está disponible cuando el router ejecuta Cisco IOS 12.4(11)T y versiones posteriores.

## Asistente para migración: Seleccione el archivo de firma de copia de seguridad de IOS IPS

El archivo de copia de seguridad contiene la información de Cisco IOS IPS que se migrará. Éste puede ser un archivo de definición de firmas (**SDF**), como `attack-drop.sdf`, o `128MB.sdf`. Si realiza cambios a la información de firma, como desactivar firmas o cambiar los atributos de firmas específicas, los registros de los cambios se mantienen en un archivo independiente. Si utilizó Cisco SDM para realizar cambios, Cisco SDM los guarda en un archivo llamado `sdmips.sdf`, que guarda en la memoria flash del router. Si realizó cambios manualmente, es posible que le haya dado otro nombre al archivo y que haya guardado una copia de seguridad en el equipo.

Haga clic en el botón **...** que se encuentra junto al campo del archivo de copia de seguridad para ver un diálogo que permite examinar este archivo de copia de seguridad en la memoria flash del router o en el equipo.



## Archivo de firma

Especifique la ubicación del archivo de firma de copia de seguridad en este diálogo.

### Especificar el archivo de firma en la memoria flash

Si el archivo de firma de copia de seguridad se encuentra en la memoria flash, haga clic en el botón punta de flecha hacia abajo que se encuentra junto a este campo y seleccione el archivo.

### Especificar el archivo de firma en el equipo

Si el archivo de firma de copia de seguridad se encuentra en el equipo, haga clic en el botón **Examinar** ubicado junto a este campo y acceda al archivo.

# Java Heap Size

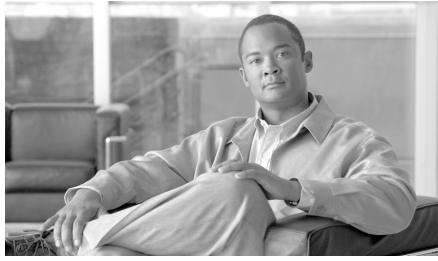
Cisco SDM muestra la ventana Java Heap Size cuando el tamaño de pila Java es muy bajo para admitir una función SDM. Complete el siguiente procedimiento para definir el tamaño de pila en el valor indicado en la ventana.

- 
- Paso 1** Salga de Cisco SDM.
- Paso 2** Haga clic en **Inicio > Panel de control > Java**.
- Paso 3** Abra el diálogo Configuración de tiempo de ejecución de Java. La ubicación de este diálogo varía según la versión.
- Haga clic en la ficha **Avanzado**. Localice el diálogo Configuración de tiempo de ejecución de Java y vaya al [Paso 4](#). Si el diálogo no está disponible en la ficha Avanzado, vaya a **b**.
  - Haga clic en la ficha **Java**. Localice el diálogo Configuración de tiempo de ejecución de Java. Haga clic en el botón **Ver** si es necesario para ver el diálogo y vaya al [Paso 4](#).

- Paso 4** En la columna Parámetros de tiempo de ejecución de Java, especifique el valor indicado en la ventana. Por ejemplo, si la ventana indica que debe usar el valor `-Xmx256m`, especifique ese valor en la columna Parámetros de tiempo de ejecución de Java. La siguiente tabla muestra valores de ejemplo.

Nombre de producto	Versión	Ubicación	Parámetros de tiempo de ejecución de Java
JRE	1.5.0_08	C:\Program Files\java\jre1.5.0_08	-Xmx256m

- Paso 5** Haga clic en **Aceptar** en el diálogo Configuración de tiempo de ejecución de Java.
- Paso 6** Haga clic en **Aplicar** en el panel de control de Java y, a continuación, haga clic en **Aceptar**.
- Paso 7** Reinicie Cisco SDM.
-



# CAPÍTULO 25

## Gestión del módulo de red

---

Si el router posee módulos de red controlados por otras aplicaciones tales como el Sistema de Detección de Intrusos (IDS), Administrador del dispositivo para router seguro (Cisco SDM) proporciona un medio para iniciar dichas aplicaciones.

### Gestión del módulo de red IDS

Si el router tiene instalado un módulo de red [IDS](#) de Cisco, esta ventana mostrará información de estado básica de dicho módulo. Si se ha configurado el módulo de red IDS, también podrá iniciar el software Intrusion Detection Device Manager ([IDM](#)) en dicho módulo y seleccionar las interfaces del router que desee que éste supervise desde esta ventana.

Si Cisco SDM detecta que no se ha configurado el módulo de red IDS, le solicitará que abra una sesión en el módulo de red para que pueda configurarlo. Puede utilizar [Telnet](#) o [SSH](#) para esta sesión.

#### Botones de control del módulo de red IDS

Cisco SDM permite emitir desde esta ventana una serie de comandos básicos para el módulo de red IDS.

##### **Recargar**

Haga clic en este botón para volver a cargar el sistema operativo del módulo de red IDS.

**Restablecer**

Haga clic en este botón para restablecer el hardware del módulo de red IDS. Sólo debe utilizarse para recuperar el sistema del estado No superado o después de cerrar el módulo de red IDS.

**Cerrar**

Haga clic en este botón para cerrar el módulo de red IDS. Antes de quitar el módulo del router, siempre deberá cerrarlo.

**Iniciar IDM**

Haga clic en este botón para iniciar el software IDM en el módulo IDS. Cuando se inicia dicho software, Cisco SDM muestra un cuadro de diálogo que solicita la dirección IP de la interfaz Fast Ethernet externa del módulo IDS. Cuando Cisco SDM obtiene la dirección correcta, abre una ventana de IDM. Para obtener más información acerca de este cuadro de diálogo, consulte [Determinación de la dirección IP](#).

Para obtener más información acerca de cómo ejecutar la aplicación IDM, consulte los documentos del enlace siguiente:

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/index.htm>

**Actualizar**

Haga clic en este botón para actualizar la visualización del estado.



**Estado del módulo de red IDS**

Esta área muestra el estado general del módulo de red IDS. Contiene los tipos de información siguientes.

- Módulo de servicio: nombre del módulo de red.
- Estado: estado del módulo de red. Los estados posibles son: Steady, Shutdown y/o Failed.
- Versión del software: versión de IDM que se está ejecutando en el módulo.
- Modelo: número del modelo del módulo de red.
- Memoria: cantidad de memoria disponible en el módulo de red.

## Configuración de la interfaz de supervisión del módulo de red IDS

Esta área de la ventana muestra qué interfaces del router envían tráfico al módulo de red IDS para que se supervise.

	Un icono de marca de verificación situado junto al nombre de la interfaz indica que el módulo de red IDS está supervisando el tráfico de la interfaz.
	Un icono rojo con una X situado junto al nombre de la interfaz indica que el módulo de red IDS no está supervisando el tráfico de la interfaz.

### Configurar

Haga clic en este botón para agregar o quitar interfaces de la lista. Cuando se hace clic en **Configurar**, Cisco SDM comprueba que el módulo de red IDS esté configurado y que el router tenga la configuración necesaria para comunicarse con dicho módulo de red. Si algunas de las configuraciones no se han efectuado, Cisco SDM mostrará una lista de comprobación con los elementos configurados y los que todavía no lo están. Haga clic en los elementos que no se han configurado para finalizar el proceso de configuración. A continuación, Cisco SDM volverá a verificar estos elemento para que pueda agregar o quitar interfaces de la lista Configuración de interfaces del módulo de red, IDS.

## Dirección IP de la interfaz del sensor IDS

Cisco SDM se comunica con el módulo de red **IDS** mediante la dirección IP de la interfaz Fast Ethernet interna del módulo. Esta ventana aparece cuando Cisco SDM no puede detectar la dirección IP y permite al usuario suministrar una sin tener que salir de Cisco SDM. Esta ventana no aparecerá si se ha configurado el módulo de red IDS con una dirección IP estática, o bien, si se ha configurado como una dirección IP no numerada en otra interfaz con una dirección IP.

La introducción de una dirección IP en esta ventana puede crear una interfaz de retrobucle nueva. Las interfaces de retrobucle pueden verse en la ventana Interfaces y conexiones. Sólo el router verá la dirección IP que especifique, por lo que puede ser cualquier dirección que desee utilizar.

## Dirección IP

Especifique la dirección IP que desea utilizar para la interfaz [sensor IDS](#). Cisco SDM ejecutará una de las acciones siguientes:

- Creará una interfaz de retrobucle. Se utilizará el número 255 si está disponible; de lo contrario, se recurrirá a otro número. Esta interfaz de retrobucle se mostrará en la ventana Interfaces y conexiones.
- Configurarán la interfaz de retrobucle con la dirección IP que especifique.
- Configurarán la IP no numerada del módulo de red IDS en la interfaz de retrobucle.
- Si el módulo de red IDS ya está configurado como IP no numerada en una interfaz de retrobucle ya existente, pero dicha interfaz no tiene una dirección IP válida, se asignará a esta interfaz de retrobucle la dirección IP que especifique en esta ventana.

## Determinación de la dirección IP

Cisco SDM muestra esta ventana cuando es necesario determinar la dirección IP de un módulo de red que se está intentando gestionar. Generalmente se trata de la dirección IP de la interfaz Ethernet externa del módulo. Cisco SDM puede utilizar la dirección que se usó la última vez que se ejecutó la aplicación de gestión, puede intentar encontrar la dirección IP, o bien, puede aceptar una dirección especificada en esta ventana.

Seleccione un método y haga clic en **Aceptar**. Si el método seleccionado no se ejecuta correctamente, puede elegir otro.

### Utilizar la última dirección IP de Cisco SDM conocida

Haga clic para que Cisco SDM utilice la dirección IP que se usó la última vez que se ejecutó la aplicación de gestión para este módulo de red. Si la dirección IP del módulo no se ha cambiado desde que se ejecutó la aplicación de gestión por última vez y Ud. no desea que Cisco SDM busque la dirección, utilice esta opción.

## Permitir que Cisco SDM descubra la dirección IP

Haga clic para que Cisco SDM intente encontrar la dirección IP del módulo de red. Puede usar esta opción si no conoce la dirección IP y si no está seguro de que la última dirección IP de Cisco SDM utilizada para conectarse con el módulo de red sigue siendo la correcta.

### Especificar

Si conoce la dirección IP del módulo de red, elija esta opción y especifique la dirección. Cisco SDM recordará la dirección y podrá seleccionar la opción **Utilizar la última dirección IP SDM conocida** la próxima vez que inicie el módulo de red.

## Lista de verificación de la configuración del módulo de red IDS

Esta ventana se abre cuando se hace clic en **Configurar** en la ventana Gestión del módulo de red IDS para especificar las interfaces del router cuyo tráfico debe analizarse, pero al módulo de red de IDS o al router les falta un ajuste de configuración necesario para que los dos dispositivos puedan comunicarse. Muestra qué ajustes de configuración son necesarios y, en algunos casos, permite completar la configuración desde Cisco SDM.

- ✓ Un icono de marca de verificación en la columna Acción indica que se ha efectuado el ajuste de la configuración.
- ✗ Un icono con una X en la columna Acción significa que es preciso ajustar la configuración para que el router pueda comunicarse con el módulo de red IDS.

### Interfaz del sensor del módulo de red IDS

- ✗ Si esta fila contiene un icono con una X en la columna Acción, significa que no se ha configurado la interfaz del sensor del módulo de red IDS con una dirección IP. Haga doble clic en la fila y especifique una dirección IP para el sensor IDS en el cuadro de diálogo que se abra. La dirección IP del sensor IDS es la dirección que utilizan Cisco SDM y el router cuando se comunican con el módulo de red IDS. Puede tratarse de una dirección privada y, en dicho caso, sólo el host donde está instalado el router podrá alcanzarla.

## Fecha y hora

- ✘ Si esta fila contiene un icono con una X en la columna Acción, significa que los ajustes del reloj del router no se han configurado. Haga doble clic en esta fila y especifique la fecha y la hora en la ventana Propiedades de fecha y hora.

## Configuración de CEF IP

- ✘ Si esta fila contiene un icono con una X en la columna Acción, significa que no se ha activado Cisco Express Forwarding (CEF) en el router. Haga doble clic en esta fila y, a continuación, en **Sí** para activar CEF IP en el router.

## Configuración inicial de módulo de red IDS

- ✘ Si esta fila contiene un icono con una X en la columna Acción, significa que Cisco SDM ha detectado que la dirección IP por defecto del módulo de red IDS no se ha cambiado. Haga doble clic en esta fila y Cisco SDM le solicitará que inicie una sesión en el módulo IDS y que complete la configuración. Puede utilizar [Telnet](#) o [SSH](#) para esta sesión.

Para obtener más información acerca de cómo configurar el módulo IDS, consulte los documentos del enlace siguiente.

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/index.htm>

## Actualizar

- ✘ Una vez haya cambiado los ajustes de configuración, puede hacer clic en este botón para actualizar la lista de comprobación. Si la columna Acción sigue conteniendo el icono con la X, indica que queda un ajuste por efectuar.



## Configuración de supervisión de la interfaz del módulo de red IDS

Utilice esta ventana para seleccionar las interfaces del router cuyo tráfico desea que el módulo de red IDS supervise.

### Interfaces supervisadas

Estas listas contienen las interfaces cuyo tráfico supervisa el módulo de red IDS. Para agregar una interfaz a esta lista, seleccione una en la lista Interfaces disponibles y haga clic en el botón con las flechas hacia la izquierda (<<). Para quitar una interfaz de la lista, selecciónela y haga clic en el botón con las flechas hacia la derecha (>>).

### Interfaces disponibles

Estas listas contienen las interfaces cuyo tráfico no está supervisando actualmente el módulo de red IDS. Para agregar una interfaz a la lista Interfaces supervisadas, seleccione una y haga clic en el botón con las flechas hacia la izquierda (<<).

## Inicio de sesión del módulo de red

Introduzca el nombre de usuario y la contraseña requeridos para iniciar sesión en el módulo de red. Estas credenciales posiblemente no sean las mismas credenciales requeridas para registrarse en el router.

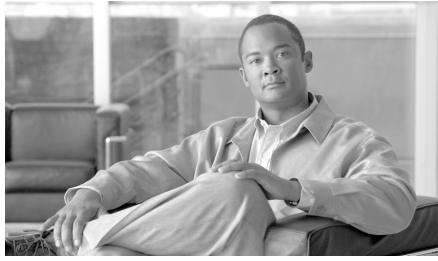
## Función No disponible

La ventana aparece cuando intenta configurar una función que la imagen de Cisco IOS del router no admite. Si desea usar esta función, obtenga una imagen Cisco IOS que sí la admita desde Cisco.com.

## Selección de interfaz del módulo de switch

Esta ventana aparece cuando existe más de un módulo de switch instalado en el router, y le permite seleccionar aquél que desea gestionar. Haga clic en el botón de radio ubicado al lado del módulo de switch que desea gestionar, y luego haga clic en **Aceptar**.





# CAPÍTULO 26

## Calidad de servicio (QoS)

---

El Asistente para la calidad de servicio (**QoS**) permite a un administrador de redes activar la calidad de servicio (QoS) en las interfaces WAN del router. QoS también puede activarse en los túneles y las interfaces VPN IPsec. Las ventanas de edición de QoS permiten al administrador editar las políticas creadas mediante el asistente.

### Crear política de QoS

El Asistente para QoS permite a un administrador de redes activar la calidad de servicio (**QoS**) en las interfaces WAN del router. QoS también puede activarse en los túneles y las interfaces VPN IPsec.

La política se aplica al tráfico saliente de la interfaz.

#### Ficha Crear política de QoS

Haga clic aquí para agregar una nueva política de QoS.

#### Ficha Editar política de QoS

Haga clic aquí para editar una política de QoS existente.

#### Botón Iniciar asistente para QoS

Haga clic aquí para iniciar el Asistente para QoS. Este asistente permite configurar las políticas de QoS en las interfaces WAN.

# Asistente para QoS

Esta ventana resume la información que proporcionará al completar el asistente para política de QoS.

Haga clic en el botón **Siguiente** para comenzar a configurar una política de QoS.

## Selección de Interfaz

Elija la interfaz en la que desea configurar la política de QoS en esta ventana. Aquí se ofrece una lista de las interfaces WAN y las interfaces que no tienen configurada ninguna política de QoS saliente. La lista incluye las interfaces VPN pero no las interfaces que se utilizan para los clientes Easy VPN ni las que ya tienen una política de QoS existente. Los clientes Easy VPN no admiten QoS.

### Botón Detalles

Haga clic para ver los detalles de configuración de la interfaz. La ventana muestra la dirección IP y la máscara de subred de la interfaz, los nombres de las reglas de acceso y de las políticas que se aplican a ella y las conexiones para las que se utiliza dicha interfaz.

### Marcado DSCP (fiable)

Haga clic para usar los marcados Differentiated Services Code Point (DSCP) para clasificar el tráfico. Los dispositivos de la red de Cisco como teléfonos IP y switches agregan marcados DSCP a los paquetes. Configurar DSCP en el router permite usar estos marcados para clasificar el tráfico. Si la imagen de Cisco IOS en el router no admite marcado DSCP, esta opción no aparecerá.

### Descubrimiento de protocolo NBAR (no fiable).

Haga clic para usar descubrimiento de protocolo de Networked Based Application Recognition (NBAR) para clasificar el tráfico. Cuando NBAR reconoce y clasifica una aplicación, una red puede invocar servicios para esa aplicación específica. NBAR garantiza que ese ancho de banda de red se usa eficientemente al clasificar paquetes y aplicar calidad de servicio (QoS) al tráfico clasificado. Si la imagen de Cisco IOS en el router no admite descubrimiento de protocolo de NBAR, esta opción no aparecerá.

# Generación de la política de QoS

Utilice esta ventana para asignar el ancho de banda a los distintos tipos de tráfico que pasan a través de la interfaz seleccionada. El valor del porcentaje que especifica representa 1000 Kbps. Por ejemplo, si especifica 5%, se asigna un ancho de banda de 5000 Kbps. El valor del porcentaje total para todo tipo de tráfico, excepto Mejor esfuerzo, no debe exceder el 75%.

- Voz: tráfico de voz. El valor por defecto es el 33 por ciento del ancho de banda.
- Señalización de llamadas: la señalización necesaria para controlar el tráfico de voz. El valor por defecto es el 5 por ciento del ancho de banda.
- Enrutamiento: tráfico generado por éste y otros routers para administrar el enrutamiento de paquetes. El valor por defecto es el 5 por ciento del ancho de banda.
- Administración: Telnet, SSH y otros tráficos generados para administrar el router. El valor por defecto es el 5 por ciento del ancho de banda.
- Transaccional: por ejemplo, el tráfico generado para aplicaciones comerciales o actualizaciones de base de datos. El valor por defecto es el 5 por ciento del ancho de banda.
- Mejor esfuerzo: ancho de banda restante para otro tráfico, como el tráfico de correo electrónico. El valor por defecto es el 47 por ciento del ancho de banda. El valor de Mejor esfuerzo se actualiza dinámicamente según el porcentaje total para los otros tipos de tráfico.

## Resumen de la configuración de QoS

La ventana Resumen del Asistente para QoS muestra un resumen de la política de QoS creada según sus opciones en el asistente. Este mapa de política se asociará a la interfaz seleccionada. Cada clase que configure el asistente para QoS de SDM se resume en esta pantalla. A continuación, una muestra parcial señala la interfaz a la que está unida la política, el tipo de clasificación (NBAR o DSCP), el nombre de la política y varias de las clases de QoS creadas.

Interfaz: FastEthernet0/0

Clasificación: DSCP

Nombre de la política: SDM-QoS-Policy-1

Detalles de la política

-----  
Nombre de la clase: SDM-Voice-1  
-----

Activado: Sí  
DSCP de coincidencia: ef  
Servicio de cola: LLQ  
Porcentaje de ancho de banda: 33  
-----

Nombre de la clase: SDM-Signalling-1  
-----

Activado: Sí  
DSCP de coincidencia: cs3,af31  
Servicio de cola: CBWFQ  
Porcentaje de ancho de banda: 5  
-----

Nombre de la clase: SDM-Routing-1  
-----

Activado: Sí  
DSCP de coincidencia: cs6  
Servicio de cola: CBWFQ  
Porcentaje de ancho de banda: 5  
-----

Nombre de la clase: clase por defecto  
-----

Activado: Sí  
Protocolos de coincidencia:  
Servicio de cola: Cola regular  
Selección aleatoria: Sí  
-----

Nombre de la clase: SDM-Streaming-Video-1  
-----

Activado: No  
DSCP de coincidencia: cs4

# Editar política de QoS

La ventana **Editar política de QoS** permite ver y cambiar las políticas de [QoS](#) configuradas y asociar políticas con interfaces de router.

## Lista del Nombre de la Política

Elija un nombre de política de QoS en esta lista para ver los detalles de esa política.

## Interfaz

Si la política que aparece está asociada con una interfaz, se muestra el nombre de esa interfaz, por ejemplo, FastEthernet 0/0.

## Asociación

Haga clic para cambiar la asociación de una política de QoS con una interfaz. Si la política está asociada actualmente con una interfaz, puede anular la asociación de la política o cambiar la dirección del tráfico al que se aplica la política. El botón de asociación está desactivado cuando una interfaz de serie frame-relay se muestra en el campo Interfaz.

## Botones de clase de QoS

Los botones sobre el área Lista de clases permiten editar y reordenar la información de la clase para la política

- Botón Agregar: haga clic para agregar una clase de QoS a la política.
- Botón Editar: seleccione una clase y haga clic en este botón para editarla en el diálogo que aparece. El botón Editar se desactiva cuando se selecciona una clase de QoS de sólo lectura.
- Botón Eliminar: seleccione una clase y haga clic en este botón para eliminar una clase de QoS de esta política. El botón Eliminar se desactiva cuando se selecciona una clase de QoS de sólo lectura.
- Botón Cortar: seleccione una clase y haga clic en este botón para eliminarla de su posición actual en la lista. Use el botón Pegar para colocar la clase en la posición que desea. El botón Cortar se desactiva cuando se selecciona una clase de QoS de sólo lectura.

- Botón Copiar: seleccione una clase y haga clic en este botón para copiar la información de la clase. El botón Copiar se desactiva cuando se selecciona una clase de QoS de sólo lectura.
- Botón Pegar: haga clic para editar la información de la clase copiada y proporcionar un nombre nuevo a la clase. Si elige **Agregar esta clase a la política**, la clase se colocará con las políticas activadas en la clase. El botón Pegar se desactiva cuando se selecciona una clase de QoS de sólo lectura.
- Botón Desplazar hacia arriba: elija una clase y haga clic en este botón para desplazar una clase hacia arriba en la lista de clases. Este botón sólo se puede usar para desplazar clases activadas. El botón Desplazar hacia arriba se desactiva cuando se selecciona una clase de QoS de sólo lectura.
- Botón Desplazar hacia abajo: elija una clase y haga clic en este botón para desplazar una clase hacia abajo en la lista de clases. Este botón sólo se puede usar para desplazar clases activadas. El botón Desplazar hacia abajo se desactiva cuando se selecciona una clase de QoS de sólo lectura.

## Pantalla Lista de clases

La ventana Editar política de QoS muestra los detalles de las clases de QoS que forman la política seleccionada.

### Columna Icono

La primera columna puede contener un icono que indica el estado de una política de QoS.



Si este icono aparece al lado de la clase de QoS, ésta es de sólo lectura y no puede editarse, eliminarse o desplazarse hacia otra posición en la lista de clases.

### Nombre de la clase

El nombre de la clase de QoS. Cisco SDM predefine nombres para las clases de QoS.

### Activado

Una marca de verificación verde indica que esta clase está activada. Un icono rojo con una X blanca indica que la clase no se ha activado para esta política. Para activar una clase, haga clic en **Editar** y actívela en la ventana Editar clase de calidad de servicio (QoS).



### Coincidencia

La clase de QoS puede buscar coincidencias con **Cualquiera** o con **Todos** los valores DSCP seleccionados. Si elige **Cualquiera**, el tráfico debe cumplir sólo uno de los criterios de coincidencia. Si elige **Todos**, el tráfico debe cumplir todos los criterios de coincidencia. Los valores DSCP elegidos se muestran en la columna DSCP.

### Clasificación

Esta parte de la pantalla contiene las siguientes columnas:

- DSCP: los valores DSCP que se seleccionan para coincidencias posibles.
- Protocolos: los protocolos que se incluyen en esta clase de QoS. Una clase de QoS de tráfico de vídeo puede incluir protocolos como cuseeme, netshow y vdolive. Una clase de QoS de tráfico de enrutamiento puede incluir protocolos como BGP, EIGRP y OSPF.
- ACL: el nombre o el número de una ACL que especifica el tráfico al que se aplica esta clase de QoS.

### Acción

Esta parte de la pantalla contiene las siguientes columnas:

- Servicio de cola: esta columna muestra el tipo de servicio de cola, Class Based Weighted Fair Queuing (CBWFQ), Low Latency Queuing (LLQ) o Fair Queuing y muestra el ancho de banda asignado a la clase.
- Definir DSCP: el valor de DSCP que proporciona a este tipo de tráfico la clase de QoS.
- Rechazar: esta columna muestra **Sí** cuando este tipo de tráfico debe rechazarse o **No** cuando debe permitirse.

### Botones Aplicar cambios y Descartar cambios

Los cambios realizados en esta ventana no se transmiten inmediatamente al router. Para transmitir los cambios realizados, haga clic en **Aplicar cambios**. Si no desea que los cambios realizados en esta ventana se envíen al router, haga clic en **Descartar cambios**.

## Asociar o anular asociación de la política de QoS

Use esta ventana para cambiar las asociaciones que una política de QoS tiene con interfaces del router.

### Columna Interfaz

Esta columna proporciona una lista de las interfaces del router.



#### Nota

---

Si selecciona la interfaz que SDM utiliza para comunicarse con el router, puede hacer que la conexión entre SDM y el router se rechace.

---

### Columna Entrante

Marque la casilla en esta columna si desea asociar la política de QoS con el tráfico entrante en la interfaz seleccionada.

### Columna Saliente

Marque la casilla en esta columna si desea asociar la política de QoS con el tráfico saliente en la interfaz seleccionada.

## Agregar o editar una clase de QoS

Puede crear y editar clases de tráfico de [QoS](#) y especificar si la clase debe agregarse a la política de QoS.

### Agregar esta clase a la política

Seleccione esta opción para incluir esta clase de [QoS](#) en la política de QoS. Si no selecciona esta opción, la clase de QoS se marcará con el valor Desactivado en la ventana Editar política de QoS.

### Nombre de la clase

El nombre de la clase de QoS se muestra en este campo si está editando una clase existente. Debe ingresar un nombre de clase si está agregando una clase nueva a una política o pegando información desde una clase de QoS que ha copiado.

## Clase por defecto

Esta opción aparece cuando no existe una clase por defecto en la política de QoS. Haga clic en **Clase por defecto** si desea agregar una clase por defecto en lugar de crear una clase nueva. Existen varios parámetros de configuración que no puede configurar para una clase por defecto:

- Casilla Clasificación: no puede especificar los criterios de clasificación.
- Casilla Acción: no puede especificar el rechazo de ese tráfico. Además, sólo puede especificar el uso de ese servicio de cola regular.

## Clasificación

Seleccione los tipos de elementos y valores que desea que el router inspeccione en el tráfico. Si hace clic en Todos, el tráfico debe coincidir con todos los criterios. Si hace clic en Cualquiera, el tráfico sólo necesita coincidir con un criterio. Debe especificar un tipo de valor en la lista y hacer clic en **Editar** para especificar los valores. Para especificar que la clase debe coincidir con http, edonkey y smtp, por ejemplo, seleccione **Protocolo** y haga clic en **Editar**. Luego, seleccione estos protocolos en el diálogo Editar valores de protocolo de coincidencia y haga clic en **Aceptar**. Los protocolos que selecciona aparecen en la columna Valor de la lista Clasificación.

Si desea que la clase coincida con el tráfico definido en una ACL, haga clic en **Regla de acceso** y, luego, en **Editar**. En el diálogo que aparece, puede seleccionar una ACL existente, crear una nueva o borrar asociaciones existentes si está editando una clase de QoS.

## Acción

Seleccione la acción que el router debe realizar cuando encuentra tráfico que coincide con los valores DSCP especificados.

- **Rechazar**: rechazar el tráfico. Si selecciona **Rechazar**, se desactivan otras opciones en el área Acción.
- **Definir DSCP**: seleccione el valor DSCP al que desea que se restablezca el tráfico.
- **Servicio de cola**: el LLQ está disponible si el tráfico utiliza el protocolo RTP o tiene un valor DSCP de EF. Si el tráfico no tiene estos atributos, la opción LLQ no está disponible. Si está agregando o editando la clase por defecto, sólo está disponible el servicio de cola regular.

- **Porcentaje de ancho de banda:** el valor de porcentaje que especifica se utiliza como un porcentaje absoluto del ancho de banda total en la interfaz.
- **Porcentaje de ancho de banda restante:** el valor de porcentaje que especifica se utiliza como un porcentaje relativo del ancho de banda total en la interfaz. Por ejemplo, puede especificar que el 30 por ciento del ancho de banda disponible se asigne a una clase y que el 60 por ciento del ancho de banda se asigne a otra clase de QoS. Para usar esta opción, todas las otras clases deben utilizarla. La opción **Porcentaje de ancho de banda restante** se desactiva si se selecciona **LLQ**.
- **Detección aleatoria:** activa Weighted Random Early Detection (WRED) y Distributed WRED (DWRED) en el router. Esta opción está desactivada si se selecciona **LLQ**. Random Early Detection rechaza paquetes durante períodos de alta congestión. De este modo, le avisa al host de origen que disminuya la velocidad de transmisión.

## Editar valores DSCP de coincidencia

Para agregar un valor DSCP a la lista de coincidencia, seleccione un valor de la columna **Valores DSCP disponibles** a la izquierda, y haga clic en el botón punta de flecha doble hacia arriba para agregarlo a la columna **Valores DSCP seleccionados**. Para eliminar un valor de la columna **Valores DSCP seleccionados**, seleccione el valor y haga clic en el botón punta de flecha doble hacia abajo.

## Editar valores de protocolo de coincidencia

Para agregar un protocolo a una clase, seleccione un protocolo de la columna **Protocolos disponibles**, ubicado a la izquierda, y haga clic en el botón punta de flecha doble hacia arriba para agregarlo a la columna **Protocolos seleccionados**. Para eliminar un protocolo de la columna **Protocolos seleccionados**, elija el protocolo y haga clic en el botón punta de flecha doble hacia abajo.

## Agregar protocolos personalizados

Esta ventana permite agregar protocolos personalizados que no están disponibles en la ventana Editar valores de protocolo de coincidencia. Para definir un protocolo personalizado, haga lo siguiente:

- 
- Paso 1** Seleccione el nombre del protocolo personalizado de la lista Nombre.
  - Paso 2** Seleccione si se usará como protocolo TCP o UDP.
  - Paso 3** Defina los números de puerto que usará este protocolo. Especifique un número de puerto en el campo Nuevo número de puerto y haga clic en **Agregar** para agregarlo a la lista Números de puerto. Para eliminar un número de puerto de la lista, seleccione el número y haga clic en **Eliminar**.
- 

## Editar ACL de coincidencia

Elija **Seleccione una regla existente (ACL)** o **Cree una nueva regla (ACL) y seleccione**. Aparecen diálogos adicionales que permiten crear o seleccionar una regla existente. Si desea borrar asociaciones de reglas existentes, puede seleccionar **Ninguna (borrar asociaciones)**.

## Editar valores DSCP de coincidencia

Para agregar un valor DSCP a la lista de coincidencia, seleccione un valor de la columna **Valores DSCP disponibles** a la izquierda, y haga clic en el botón punta de flecha doble hacia arriba para agregarlo a la columna **Valores DSCP seleccionados**. Para eliminar un valor de la columna **Valores DSCP seleccionados**, seleccione el valor y haga clic en el botón punta de flecha doble hacia abajo.





## CAPÍTULO 27

# Control de Admisión a la Red

---

El Control de Admisión a la Red (NAC) protege las redes de datos contra virus informáticos al evaluar la “vitalidad” de las estaciones de trabajo de los clientes para asegurarse que ellos reciban las últimas actualizaciones de firmas de virus disponibles, y controlar su acceso a la red.

NAC funciona con el software antivirus para evaluar la condición de un cliente, llamada la *postura* del cliente, antes de permitir el acceso del cliente a la red. NAC se asegura de que un cliente de la red tenga instalada una firma de virus actualizada, que no haya sido infectada. Si el cliente requiere una actualización de firmas, NAC lo redirigirá a completar la actualización. Si el cliente se ha comprometido o si se está originando un brote de virus en la red, NAC colocará al cliente en un segmento de cuarentena de la red hasta que se complete la desinfección.

Para obtener más información sobre NAC, haga clic en los enlaces siguientes:

- [http://www.cisco.com/en/US/netsol/ns466/networking\\_solutions\\_package.html](http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html)
- [http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont\\_0900aecd80217e26.pdf](http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf)

# Ficha Crear NAC

Usted usa la ficha Crear NAC y el asistente de NAC para crear una política de NAC y relacionarla a una interfaz. Después de que usted cree la política de NAC, podrá editarla al hacer clic en **Editar NAC** y al escogerla de la lista de políticas.

La configuración de NAC en el router es sólo una parte de la implementación completa de NAC. Haga clic en [Otras Tareas en una Implementación del NAC](#) para conocer las tareas que se deben llevar a cabo en otros dispositivos para implementar el NAC.

## Activar el Botón AAA

La autenticación, autorización, y contabilidad (**AAA**) deben estar activadas en el router antes de que usted pueda configurar NAC. Si AAA no está activada, haga clic en el botón **Activar AAA**. Si AAA ya ha sido configurada en el router, no se desplegará este botón.

## Iniciar el Botón de Asistente del NAC

Haga clic en este botón para iniciar el asistente del NAC. El asistente divide la configuración del NAC en una serie de pantallas en las que usted completará una tarea de configuración sencilla.

## ¿Cómo obtengo una lista?

Si quiere crear una configuración en la cual el asistente no le indique el camino, haga clic en el botón siguiente a esta lista. Este botón lista otras clases de configuraciones que usted podría llevar a cabo. Si quiere aprender a crear una de las configuraciones listadas, elija la configuración y haga clic en **Ir**.



## Otras Tareas en una Implementación del NAC

Una implementación del NAC completa incluye los siguientes pasos de configuración:

- 
- Paso 1** Instalar y configurar el software de Agente de Confianza Cisco (CTA) en los hosts de la red. Esto proporciona a los hosts un agente de gestión de estado capaz de responder a las consultas **EAPoUDP** del router. Vea los vínculos después de estos pasos para obtener el software de CTA y para aprender cómo instalarlo y configurarlo.
  - Paso 2** Instalar y configurar un servidor AAA de autenticación EAPoUDP. Este servidor debe ser un Servidor de Control de Acceso Seguro de Cisco (ACS, Access Control Server) que usa el protocolo **RADIUS**. Se requiere el software del Servidor de Control de Acceso de Cisco, versión 3.3. Vea los vínculos después de estos pasos para conocer más acerca sobre cómo instalar y configurar el ACS.
  - Paso 3** Instalar y configurar el servidor de validación y corrección de gestión de estado
- 

Si usted es un usuario registrado de Cisco.com, podrá descargar el software de Agente de Confianza de Cisco (CTA) desde el vínculo siguiente:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cta>

El documento en el vínculo siguiente explica cómo instalar y configurar el software de CTA en un host.

[http://www.cisco.com/en/US/products/ps5923/products\\_administration\\_guide\\_book09186a008023f7a5.html](http://www.cisco.com/en/US/products/ps5923/products_administration_guide_book09186a008023f7a5.html)

El documento en el vínculo siguiente contiene una visión general del proceso de configuración.

[http://www.cisco.com/application/pdf/en/us/guest/netso1/ns466/c654/cdccont\\_0900aecd80217e26.pdf](http://www.cisco.com/application/pdf/en/us/guest/netso1/ns466/c654/cdccont_0900aecd80217e26.pdf)

Los documentos en el vínculo siguiente explican cómo instalar y configurar el ACS Seguro de Cisco para servidores basados en Windows Versión 3.3.

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_soft/csacs4nt/acs33/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs33/index.htm)

## Bienvenido

El asistente de NAC le permite a usted hacer lo siguiente:

- Seleccionar la interfaz en donde se activará el NAC: los hosts que intenten acceder a la red a través de esta interfaz deberán pasar por el proceso de validación del NAC.
- Configurar los Servidores de Política del NAC: las políticas de admisión se configuran en estos servidores, y el router se comunica con ellos cuando un host de la red intente acceder a la red. Usted puede especificar la información para servidores múltiples. Los servidores de política del NAC usan el protocolo RADIUS.
- Configurar una lista de excepción del NAC: los hosts tales como impresoras, teléfonos IP y los hosts sin agentes de gestión de estado de los NAC instalados, pueden necesitar saltarse el proceso del NAC. Los hosts con direcciones IP estáticas y otros dispositivos pueden identificarse en una lista de excepción, y tratarse al usar una política de excepción relacionada. Los hosts también pueden identificarse por su dirección MAC, o por su tipo de dispositivo.
- Configurar una política de host sin agente: si usted quiere usar una política que resida en un servidor ACS Seguro de Cisco para manejar hosts sin un agente de gestión de estado instalado, podrá hacerlo. Cuando el servidor ACS Seguro de Cisco recibe un paquete de un host sin agente, éste responde al enviar la política del host sin agente. Configurar una política del host sin agente es útil cuando hay hosts sin agentes, a quienes se les atiende dinámicamente, tales como los clientes de DHCP.
- Configurar NAC para acceso remoto: se les debe permitir el acceso a los hosts que usen Cisco SDM para administrar el router. El asistente le permite especificar direcciones IP para administración remota, de manera que Cisco SDM pueda modificar la ACL de NAC para permitir que los hosts que tengan esas direcciones accedan al router.

Configurar NAC en el router es el último paso en una configuración de NAC. Antes de que usted configure el router con esta función, complete los pasos descritos en el vínculo siguiente: [Otras Tareas en una Implementación del NAC](#).

## Servidores de Políticas del NAC

Las políticas de control de admisión de NAC se configuran y guardan en una base de datos de políticas que residen en servidores **RADIUS** que ejecutan Cisco Secure ACS, versión 3.3. El router debe validar las credenciales de los hosts de la red al comunicarse con el servidor RADIUS. Use esta ventana para suministrar la información que el router necesita para comunicarse con los servidores RADIUS. Cada servidor RADIUS que especifique debe tener el software Secure Cisco Access Control Server (**ACS**), versión 3.3, instalado y configurado.

### Escoger la fuente RADIUS del Cliente

Configurar el origen RADIUS le permitirá a usted especificar la dirección IP del origen a enviarse en paquetes RADIUS con destino al servidor RADIUS. Si usted necesita más información sobre una interfaz, escoja la interfaz y haga clic en el botón **Detalles**.

La dirección IP del origen en los paquetes RADIUS enviados desde el router debe configurarse como la dirección IP del NAD versión 3.3 de Cisco ACS o superior.

Si selecciona **El router elige el origen**, la dirección IP del origen en los paquetes RADIUS será la dirección de la interfaz a través de la cual los paquetes RADIUS saldrán del router.

Si usted escoge una interfaz, la dirección IP del origen en los paquetes RADIUS será la dirección de la interfaz que usted escoja como la fuente RADIUS del cliente.



#### Nota

El software de Cisco IOS permite que una interfaz sencilla de origen RADIUS se configure en el router. Si el router ya tiene configurada una origen RADIUS y usted escoge una origen diferente a la dirección IP del origen colocada en los paquetes enviados al servidor RADIUS, se cambiará a la dirección IP del nuevo origen, y podrá no coincidir con la dirección IP del NAD configurada en Cisco ACS.

## Botón Detalles

Si usted necesita una visión rápida de la información sobre una interfaz antes de escogerla, haga clic en **Detalles**. La pantalla le mostrará la dirección IP y la máscara de subred, las reglas de acceso y las reglas de inspección aplicadas a la interfaz, la política de IPSec y la política de QoS aplicadas, y si hay una configuración de Easy VPN en la interfaz.

## Columnas de Servidor IP, Tiempo de inactividad y parámetros

Columnas de Servidor IP, Tiempo de inactividad y parámetros contienen la información que el router usa para comunicarse con un servidor RADIUS. Si no hay información del servidor RADIUS relacionada con la interfaz elegida, estas columnas quedarán en blanco.

## Usar la Casilla de verificación para el NAC

Marque esta casilla si usted quiere usar el servidor RADIUS indicado para el NAC. El servidor debe tener configuradas las políticas de control de admisión requeridas, si el NAC va a estar apto para usar el servidor.

## Botones de Agregar, Editar, y Ping

Para suministrar información a un servidor RADIUS, haga clic en el botón **Agregar** e introduzca la información en la pantalla mostrada. Elija una fila y haga clic en **Editar** para modificar la información para un servidor RADIUS. Escoja una fila y haga clic en **Ping** para probar la conexión entre el router y el servidor RADIUS.



### Nota

Cuando se esté efectuando una prueba de ping, introduzca la dirección IP de la interfaz del origen RADIUS en el campo de origen en el diálogo de ping. Si usted elige **Router escoge el origen**, no necesitará proporcionar ningún valor en el campo de origen del diálogo de ping.

Los botones **Editar** y **Ping** se desactivan cuando no hay ninguna información del servidor RADIUS disponible para la interfaz elegida.

## Selección de Interfaz

Escoja la interfaz con la cual se activará el NAC en esta ventana. Elija la interfaz a través de la cual los hosts de la red se conectan a la red.

Haga clic en el botón **Detalles** para mostrar las políticas y reglas relacionadas con la interfaz que usted elija. La ventana despliega los nombres de las ACLs aplicadas al tráfico de entrada y salida en esta interfaz.

Si una ACL entrante ya está presente en la interfaz, Cisco SDM usará esa ACL para NAC al agregar las declaraciones de permiso apropiadas para el tráfico de EAPoUDP. Si la dirección IP de la interfaz sobre la cual el NAC está siendo aplicado fuera 192.55.22.33, una muestra de declaración de permisos podrá ser la siguiente:

```
access-list 100 permit udp any eq 21862 192.55.22.33
```

La declaración de permiso que Cisco SDM agrega, usa el número de puerto 21862 para el protocolo EAPoUDP. Si los hosts de la red ejecutan EAPoUDP en un número de puerto personalizado, usted deberá modificar esta entrada de ACL para usar el número de puerto que usan los hosts.

Si no se configura ninguna ACL entrante en la interfaz que usted especifica, puede hacer que Cisco SDM aplique un ACL a la interfaz. Usted podrá escoger una política recomendada, o una política que sólo supervise las gestión de estados del NAC monitorizadas.

- **Validación estricta (recomendada):** Cisco SDM aplica una ACL que deniega todo el tráfico (**deny ip any any**). La admisión a la red se determina por el proceso de validación del NAC. Por defecto, todo tráfico se deniega excepto el tráfico que se encontró como legítimo basado en la política configurada en el servidor de política de NAC.
- **Supervisar parámetros NAC:** Cisco SDM aplica una ACL que permite todo el tráfico (**permit ip any any**). Después del proceso de validación del NAC, el router puede recibir políticas del servidor del NAC que niega el acceso a ciertos hosts. Usted puede utilizar la configuración **Supervisar posturas NAC** para determinar el impacto de la configuración de NAC en la red. Después de realizar esta acción, puede modificar las políticas en el servidor de políticas de NAC, y luego reconfigurar NAC en el router para usar la **Validación estricta**, al cambiar la ACL aplicada a la interfaz a **deny ip any any**, utilizando la función de Políticas del Firewall de Cisco SDM.

## Lista de excepción de NAC

Usted puede identificar los hosts a los que se les debe permitir saltar el proceso de validación del NAC. Típicamente, los hosts tales como impresoras, teléfonos IP, y hosts sin el software del Agente de gestión de estados del NAC instalado, se agregan a la lista de excepción.

Si hay hosts sin direcciones estáticas en su red, se recomienda que se incluyan en la política del host sin agente, y no en la lista de excepción del NAC. La política de excepción del NAC no puede operar apropiadamente si cambian las direcciones IP del host.

Si usted está usando el asistente de NAC y no necesita configurar una lista de excepción de NAC, podrá hacer clic en **Siguiente** sin introducir información en esta ventana. Como una alternativa o como complemento para la lista de excepción de NAC, el asistente permite que usted configure una política del host sin agente en otra ventana.

### Columnas de Dirección IP, Dirección MAC, Tipo de dispositivo, Dirección de dispositivo y Políticas

Estas columnas contienen información sobre un host en la lista de excepción. Un host puede identificarse por su dirección IP, dirección MAC, o el tipo de dispositivo que es. Si se identifica por una dirección, la dirección IP o la dirección MAC se muestra en la fila junto con el nombre de la política que gobierna el acceso del host a la red.

### Botones Agregar, Editar y Eliminar

Genere la lista de excepción al hacer clic en **Agregar** e introducir la información sobre un host. Usted puede usar el botón **Agregar** tantas veces como necesite hacerlo.

Elija una fila y haga clic en **Editar** para cambiar la información sobre un host. Haga clic en **Eliminar** para eliminar la información sobre un host, de esta ventana. Los botones Editar y Eliminar se desactivan cuando no hay información en esta lista.

## Agregar o Editar una Entrada de la Lista de Excepción

Agregue o edite información en una entrada de la lista de excepción en esta ventana.

### Tipo de lista

Los hosts se escogen por la manera en que son identificados. Esta lista contiene las selecciones siguientes:

- Dirección IP: seleccione ésta si quiere identificar el host por su dirección IP.
- Dirección MAC: seleccione ésta si desea identificar el host por su dirección MAC.
- Teléfono IP de Cisco: seleccione ésta si quiere incluir los teléfonos IP de Cisco en la lista de excepción en la red.

### Especificar el Campo de Dirección

Si usted escoge dirección IP o dirección MAC como el tipo de host, introdúzcala dirección en este campo. Si usted elige un tipo de dispositivo, este campo se desactiva.

### Campo de Política

Si usted sabe el nombre de la política de excepción, introdúzcala en este campo. Haga clic en el botón con tres puntos a la derecha del campo de política para escoger una política existente o mostrar un cuadro de diálogo en el que usted pueda crear una política nueva.

## Elegir una Política de Excepción

Escoja la política que quiera aplicar al host. Cuando usted escoge una política, la URL de redirección especificada para la política aparecerá en un campo de sólo lectura, y se mostrarán las entradas de la regla de acceso para la política.

SI no hay políticas disponibles en la lista, haga clic en **Cancelar** para regresar a la pantalla del asistente y luego elija la opción que le permita agregar una política.

Elija la política que desee aplicar al host excluido de la lista. Si no hay ninguna política en la lista, haga clic en **Cancelar** para regresar al asistente. Luego seleccione **Crear una nueva política** y elíjala en la ventana Agregar a la lista de excepción.

## URL de redireccionamiento: Campo URL

Este campo de sólo lectura muestra la URL redirigida relacionada con la política que usted elige. Los hosts a los que se les aplica esta política se redirigen a esta URL cuando se hace el intento de acceder a la red.

## Vista Preliminar de la Regla de Acceso

Las columnas de Acción, Origen, Destino y Servicio indican las entradas de ACL en la regla de acceso relacionada con la política. Estas columnas se encuentran vacías si no se configura alguna ACL para esta política.

## Agregar Política de Excepción

Cree una nueva política de excepción en esta ventana.

Para crear una nueva política de excepción, introduzca un nombre para la política y especifique una regla de acceso que defina las direcciones IP de los hosts, en la lista de excepción que pueden acceder, o introduzca una URL de redirección. La URL de redirección debe contener información correctiva que permita a los usuarios actualizar sus archivos de definición de virus. Usted debe suministrar un nombre para la regla de acceso o una URL de redirección. Usted puede especificar ambos.

## Dar Nombre al Campo

introduzca el nombre de la política en este campo. No utilice signos de interrogación (?) o los caracteres de espacio en los nombres de política. Limite cada nombre de política a no más de 256 caracteres.

## Campo de la Regla de Acceso

Introduzca el nombre de la regla de acceso que quiera usar, o haga clic en el botón a la derecha de este campo para buscar una regla de acceso o crear una regla nueva de acceso. La regla de acceso debe contener entradas de permiso que especifiquen las direcciones IP, a las que se pueden conectar los hosts en la lista de excepción. La regla de acceso debe ser una ACL designado; no se soportan las ACLs numeradas.



## Campo de URL de Redirección

Introduzca una URL que contenga la información correctiva para su red. Esta información podría contener instrucciones para descargar archivos de definición de virus.

Una URL de corrección podría tener la apariencia siguiente:

```
http://172.23.44.9/update
```

Las URL de redireccionamiento son generalmente de la forma `http://URL`, o `https://URL`.

## Política de Hosts sin Agentes

Si existe una política para hosts sin agentes en el servidor ACS Seguro de Cisco, el router podrá usar esa política para manejar los hosts sin agentes de gestión de estado instalados. Este método de manejar hosts sin agentes puede usarse como una alternativa o como un complemento para una lista de excepción del NAC. Si usted está utilizando el asistente de NAC y no necesita configurar una política de hosts sin agentes, podrá hacer clic en **Siguiente** sin introducir información en esta ventana.

### Autenticar la Casilla de verificación de Hosts sin Agentes

Marque esta casilla para indicar que quiere usar la política de hosts sin agentes en el servidor ACS Seguro de Cisco.

### Campos de Nombre del Usuario y Contraseña

Algunas imágenes de software de Cisco IOS requieren que se suministre un nombre de usuario y una contraseña junto con la solicitud al servidor ACS Seguro de Cisco. Si se requiere esto, introduzca el nombre del usuario y la contraseña configurada en el servidor ACS Seguro de Cisco para este propósito. Si la imagen del software de Cisco IOS no requiere esta información, estos campos no aparecerán.

## Configurar el NAC para el Acceso Remoto

La configuración de NAC para acceso remoto permite que usted modifique las ACLs que crea la configuración de NAC, de manera que éstas permitirán el tráfico de Cisco SDM. Especifique los hosts que podrán utilizar Cisco SDM para acceder al router.

### Activar administración remota de Cisco SDM

Seleccione esta casilla para activar la administración remota de Cisco SDM en la interfaz designada.

### Campos de Dirección del Host y la Red

Si quiere que Cisco SDM modifique la ACL para permitir el tráfico de Cisco SDM desde un host único, elija **Dirección del host** y especifique la dirección IP de un host. Seleccione **Dirección de red** y especifique la dirección de una red y una máscara de subred para permitir el tráfico de Cisco SDM desde los hosts en esa red. El host o la red deben estar accesibles desde las interfaces que usted especificó. Seleccione **Cualquiera** para permitir tráfico de Cisco SDM desde cualquier host conectado con las interfaces especificadas.

## Modificar el firewall

Cisco SDM comprueba todas las [ACL](#) aplicadas a la interfaz especificada en esta configuración para determinar si bloquea algún tráfico que debe permitirse a través del firewall, de modo que funcione la característica que está configurando.

Todas las interfaces se incluyen en la lista, junto con el servicio que se está bloqueando en esa interfaz y la ACL que lo está bloqueando. Si desea que Cisco SDM modifique la ACL para permitir el tráfico listado, marque la casilla **Modificar** en la fila apropiada. Si desea ver la entrada que Cisco SDM agregará a la ACL, haga clic en el botón **Detalles**.

En la tabla siguiente, FastEthernet0/0 se ha configurado para NAC. Esta interfaz se configura con los servicios mostrados en la columna de servicio.

Interfaz	Servicio	ACL	Acción
FastEthernet0/0	Servidor RADIUS	101 (ENTRANTE)	[ ] Modificar
FastEthernet0/0	DNS	100 (ENTRANTE)	[ ] Modificar
FastEthernet0/0	DHCP	100 (ENTRANTE)	[ ] Modificar
FastEthernet0/0	NTP	101 (ENTRANTE)	[ ] Modificar
FastEthernet0/0	VPN	190 (ENTRANTE)	[ ] Modificar

## Ventana Detalles

Esta ventana muestra las entradas que Cisco SDM agregará a las ACL para permitir los servicios necesarios para el servicio que está configurando. La ventana podrá contener una entrada como la siguiente:

```
permit tcp host 10.77.158.84 eq www host 10.77.158.1 gt 1024
```

En este caso, el tráfico Web cuyo número de puerto es mayor que 1024 se permite desde el host 10.77.158.84 en la red local hasta al host 10.77.158.1

## Resumen de la configuración

Esta ventana resume la información que usted introdujo, y permite que la examine en una única ventana. Usted puede usar el botón Atrás para regresar a cualquier pantalla del asistente para cambiar la información. Haga clic en **Finalizar** para enviar la configuración al router.

He aquí un ejemplo de un resumen de configuración del NAC:

```
Interfaz NAC: FastEthernet0/1.42
Nombre de admisión: SDM_EOU_3
```

```
Interfaz de origen de cliente AAA: FastEthernet0/1.40
Servidor 1 de política del NAC: 10.77.158.54
```

Lista de excepción

```
-----
Dirección/dispositivo Dirección IP (22.22.22.2) recién
agregada
Detalles de la Política:
Nombre de la política: P55
URL de redireccionamiento: http://www.fix.com
Regla de acceso: test11
-----
```

```
Política del Host sin Agente activada
Nombre de usuario: bill
Contraseña: *****
```

En este ejemplo, los paquetes RADIUS tendrán la dirección IP de FastEthernet 0/1.40. El NAC está activado en FastEthernet 0/1.42, y la política del NAC que el asistente aplicó es SDM\_EOU\_3. Un host ha sido identificado en la lista de excepción, y su acceso a la red se controla por la política de excepción P55.

## Ficha Editar NAC

La ficha Editar NAC enumera las políticas del NAC configuradas en el router y permite que usted configure otras funciones del NAC. Una política del NAC debe configurarse para cada interfaz en la cual se llevará a cabo la validación de gestión de estado.

## Botón de Tiempos de inactividad del NAC

El router y el cliente usan el protocolo de Autenticación Extensible sobre el Protocolo de Datos No Formateados (EAPoUDP) para intercambiar información de [gestión de estado](#). Los valores por defecto para las configuraciones de los tiempos de inactividad del EAPoUDP están preconfigurados, pero usted puede cambiar las configuraciones. Este botón se desactiva si no hay política del NAC configurada en el router.

## Botón de Política de Host sin Agente

Si existe una política para hosts sin agentes en el servidor ACS Seguro de Cisco, el router podrá usar esa política para manejar los hosts sin agentes de gestión de estado instalados. Este método de manejar los hosts sin agentes puede usarse cuando tales hosts no tengan direcciones IP estáticas. Este botón se desactiva si no hay política del NAC configurada en el router.

## Botones Agregar, Editar y Eliminar

Estos botones permiten que usted administre la lista de políticas del NAC. Haga clic en **Agregar** para crear una nueva política del NAC. Use los botones de Editar y Eliminar para modificar y de eliminar políticas del NAC. Los botones Editar y Eliminar se desactivan cuando no se ha configurado ninguna política del NAC en el router.

Cuando no hay política configurada en el router, sólo el botón de Agregar está activado. El botón de Agregar se desactivará cuando todas las interfaces del router estén configuradas con una política del NAC.

## Lista de Políticas del NAC

El nombre, la interfaz a la que se aplica la política del NAC, y la regla de acceso que define la política, se incluyen en la lista. Si usted activara NAC en una interfaz al utilizar el asistente de Crear NAC, la política predeterminada NAC SDM\_EOU\_1 aparecerá en esta lista.

## Componentes del NAC

Esta ventana proporciona una breve descripción de los componentes de EAPoUDP que Cisco SDM permite que usted configure.

## Ventana Lista de Excepción

Este tema del marcador de posición se eliminará cuando se desarrolle el sistema de ayuda para NAC. Este tema de ayuda ya ha sido escrito para el modo de asistente. Para verlo, haga clic en el vínculo siguiente:

[Lista de excepción de NAC](#)

## Ventana Políticas de Excepción

Las políticas de excepción del NAC controlan el acceso a la red de los hosts, en la lista de excepción. Una política de excepción del NAC consta de un nombre, una regla de acceso, y/o una URL de redirección. La regla de acceso especifica los destinos a los cuales los hosts gobernados por la política tienen acceso. Si una URL de redirección se especifica en la política, la política podrá dirigir a los clientes de la Web a sitios que contengan información sobre cómo obtener la más reciente protección de virus disponible.

Un ejemplo de una entrada de política del NAC se muestra en la tabla siguiente:

Nombre	Regla de acceso	URL Redirigido
NACLess	Regla del Nac	http://172.30.10/update

Las reglas de acceso relacionadas con las políticas del NAC deben ser ACLs extendidas, y deben nombrarse. Un ejemplo de una regla de acceso que podrá usarse en una política del NAC se muestra en la tabla siguiente:

Acción	Origen	Destino	Servicio	Registro	Atributos
Permiso	Cualquiera	172.30.2.10	Ip		

Esta regla permite que cualquier host controlado por la política envíe el tráfico del IP a la dirección IP 172.30.2.10.

## Botones Agregar, Editar y Eliminar

Haga clic en el botón **Agregar** para crear una política de excepción nueva. Use el botón **Editar** para modificar las políticas de excepción existentes, y el botón **Eliminar** para quitar las políticas de excepción. Los botones Editar y Eliminar se desactivan cuando no hay ninguna política de excepción en la lista.

## Límites de tiempo del NAC

Configure los valores de los límites de tiempo que el router usará para la comunicación **EAPoUDP** con los hosts de la red. Los valores por defecto, mínimos y máximos para todas las configuraciones se muestran en la tabla siguiente.

Valor	Por defecto	Mínimo	Máximo
Tiempo de inactividad del período de retención	180 segundos	60 segundos	86400 segundos
Tiempo de inactividad de retransmisión	3 segundos	1 segundo	60 segundos
Tiempo de inactividad de revalidación	36000 segundos	300 segundos	86400 segundos
Tiempo de inactividad de consulta del estado	300 segundos	30 segundos	1800 segundos

## Selección de Interfaz

Escoja la interfaz a la que las configuraciones del Tiempo de inactividad del NAC se aplicarán.

## Campo Tiempo de inactividad del Período de Retención

Introduzca el número de segundos en que el router ignorará los paquetes de los clientes que acaban de fallar en la autenticación.

### **Campo Tiempo de inactividad de la Retransmisión**

introduzca el número de segundos que el router debe esperar antes de retransmitir los mensajes de EAPoUDP a los clientes.

### **Campo Tiempo de inactividad de la Revalidación**

El router interroga al agente de [gestión de estado](#) periódicamente sobre el cliente para determinar la adherencia del cliente a la política de seguridad. Introduzca el número de segundos que el router debe esperar entre las consultas.

### **Campo Tiempo de inactividad de Consulta del Estado**

introduzca el número de segundos que el router debe esperar entre las consultas para el agente de gestión de estado en el host.

### **Botón Restablecer a Valores Por defecto**

Haga clic en este botón para restablecer todos los tiempos de inactividad del NAC a sus valores por defecto.

### **Casilla de verificación Configurar éstos valores de tiempos de inactividad globalmente**

Haga clic en esta casilla de verificación para que estos valores se apliquen a todas las interfaces.

## **Configurar la Política del NAC**

Una política del NAC activa el proceso de validación de gestión de estado en una interfaz de router y puede usarse para especificar las clases de tráfico que serán excluidos de la validación de gestión de estado en el proceso de control de admisión.

### **Dar Nombre al Campo**

Ingrese un nombre para la política.



## Seleccione una Lista de la Interfaz

Escoja la interfaz a la cual usted quiere aplicarle la política del NAC. Escoja una interfaz que conecte a los clientes de la red al router.

## Campo de Regla de Admisión

Usted puede usar una regla de acceso para eximir tráfico específico de activar el proceso de control de admisión. No se requiere. introduzca el nombre o número de la regla de acceso que usted quiere usar para la regla de admisión. Usted también puede hacer clic en el botón a la derecha de este campo y buscar la regla de acceso, o crear una nueva regla de acceso.

La regla de acceso debe contener declaraciones de negación que especifican el tráfico que va a eximirse del proceso de control de admisión. No ocurre ninguna activación de validación de postura, si la regla de acceso sólo contiene declaraciones de negación.

Un ejemplo de entradas de la ACL para una regla de admisión del NAC es como sigue:

```
deny udp any host 10.10.30.10 eq domain
deny tcp any host 10.10.20.10 eq www
permit ip any any
```

La primera declaración de negación exime el tráfico con destino del puerto 53 (dominio), y la segunda declaración exime el tráfico con destino del puerto 80 (www). La declaración de permiso que termina la ACL, asegura de que ocurra la validación de gestión de estado.

## Cómo...

Los temas siguientes contienen los procedimientos para llevar a cabo las tareas que el asistente de Crear NAC no le ayudará a hacer.

### ¿Cómo Configuro un Servidor de Política del NAC?

El router debe tener conexión a un Servidor de Control de Acceso Seguro de Cisco (ACS, Access Control Server) al ejecutar un software de ACS versión 3.3. El ACS debe configurarse para usar el protocolo RADIUS con el propósito de implementar el NAC. El documento en el vínculo siguiente contiene una visión general del proceso de configuración.

[http://www.cisco.com/application/pdf/en/us/guest/netso/ns466/c654/cdccont\\_0900aec80217e26.pdf](http://www.cisco.com/application/pdf/en/us/guest/netso/ns466/c654/cdccont_0900aec80217e26.pdf)

Los documentos en el vínculo siguiente explican cómo instalar y configurar el ACS Seguro de Cisco para servidores basados en Windows Versión 3.3.

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_soft/csacs4nt/acs33/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs33/index.htm)

### ¿Cómo Instalo y Configuro un Agente de gestión de estado en un Host?

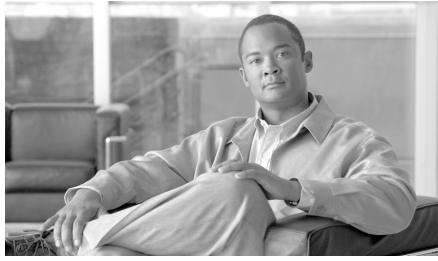
Si usted es un usuario registrado de Cisco.com, podrá descargar el software de Agente de Confianza de Cisco (CTA) desde el vínculo siguiente:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cta>

El documento en el vínculo siguiente explica cómo instalar y configurar el software de CTA en un host.

[http://www.cisco.com/en/US/products/ps5923/products\\_administration\\_guide\\_book09186a008023f7a5.html](http://www.cisco.com/en/US/products/ps5923/products_administration_guide_book09186a008023f7a5.html)

Los procedimientos de instalación específicos requeridos para instalar el software del agente de gestión de estado de terceros, y el servidor de corrección opcional varían dependiendo del software en uso. Consulte la documentación del distribuidor para obtener detalles completos.



# CAPÍTULO 28

## Propiedades del router

---

Las propiedades del router permiten definir los atributos generales del router, como el nombre del router, el nombre de dominio, la contraseña, el estado del Protocolo simple de gestión de redes ([SNMP](#)), la dirección del servidor Sistema de nombre de dominio ([DNS](#)), las cuentas de usuario, los atributos de registro del router, el terminal de tipo virtual (vty), la configuración de [SSH](#) y otros ajustes de seguridad para el acceso al router.

## Propiedades del dispositivo

La pantalla Propiedades – Dispositivo contiene información sobre el host, el dominio y la contraseña para su router.

### Ficha Dispositivo

La ficha Dispositivo contiene los campos siguientes.

#### Host

Especifique el nombre que desee asignar al router en este campo.

#### Dominio

Especifique el nombre de dominio de su empresa. Si no dispone de esta información, la puede obtener del administrador de redes.

**Especifique el texto para el anuncio**

Especifique el texto para el anuncio del router. Este anuncio aparecerá siempre que alguien se conecte al router. Se recomienda que la barra de texto incluya un mensaje que indique que el acceso no autorizado está prohibido.

**Ficha Contraseña**

La ficha Contraseña contiene los campos siguientes.

**Activar la contraseña secreta**

Administrador del dispositivo de seguridad de Cisco (Cisco SDM) admite la activación de la contraseña secreta. La opción Activar contraseña secreta permite controlar quién puede introducir comandos de configuración en este router. Se recomienda el uso de una contraseña secreta. Esta contraseña no se mostrará en la ventana de Propiedades del dispositivo de Cisco SDM y aparecerá cifrada en el archivo de configuración del router. Sugerimos por lo tanto mantener un registro de esta contraseña por si se olvida.

Es posible que la versión de Cisco IOS que ejecuta el router también admita la activación de la contraseña. La activación de la contraseña funciona como la activación de la contraseña secreta, pero se cifra en el archivo de configuración. Si se activa una contraseña mediante la interfaz de línea de comandos (CLI), ésta se ignora si ya existe una contraseña secreta activada.

**Contraseña vigente**

Si ya se ha definido una contraseña, esta área contiene asteriscos (\*).

**Especificar nueva contraseña**

Active la nueva contraseña en este campo.

**Volver a especificar nueva contraseña**

Vuelva a especificar la contraseña exactamente como la especificó en el campo Nueva contraseña.

# Fecha y hora: Propiedades del reloj

Utilice esta ventana para visualizar y editar los ajustes de fecha y hora del router.

## Fecha/Hora

Los ajustes de fecha y hora del router se pueden ver en la parte derecha de la barra de estado de Cisco SDM. Los ajustes de fecha y hora de esta parte de la ventana Propiedades del reloj no están actualizados.

## Fuente de temporización del router

Este campo puede contener los valores siguientes:

- NTP: el router recibe información horaria de un servidor [NTP](#).
- Configuración del usuario: los valores de fecha y hora se ajustan de forma manual mediante Cisco SDM o el CLI.
- Sin fuente de temporización: el router no se ha configurado con ajustes de fecha y hora.

## Cambiar configuración

Haga clic para cambiar los ajustes de fecha y hora del router.

# Propiedades de fecha y hora

Utilice esta ventana para configurar la fecha y hora del router. Puede dejar que Cisco SDM sincronice la configuración con el PC o puede hacerlo manualmente.

## Sincronizar con el reloj de mi equipo local

Marque esta opción Cisco SDM para sincronizar los ajustes de fecha y hora del router con los ajustes de fecha y hora del PC.

## Sincronizar

Haga clic para que Cisco SDM sincronice los ajustes de hora. Cisco SDM realiza los ajustes de fecha y hora de este modo sólo si hace clic en **Sincronizar**. En las sesiones posteriores, Cisco SDM no sincronizará nuevamente estos valores con el equipo de forma automática. Este botón estará desactivado si no ha seleccionado **Sincronizar con el reloj de mi equipo local**.



### Nota

Debe definir los ajustes de zona horaria y de cambios de hora según la luz solar en el equipo antes de iniciar Cisco SDM, de forma que Cisco SDM recibirá los ajustes correctos cuando haga clic en **Sincronizar**.

## Editar fecha y hora

Utilice esta área para definir la fecha y hora de forma manual. Puede elegir el mes y el año en las listas desplegadas y seleccionar el día del mes en el calendario. Los valores de los campos del área Hora deben aparecer en formato de 24 horas. Es posible seleccionar la zona horaria en función del meridiano de Greenwich (GMT) o buscar en la enumera las ciudades principales de su zona horaria.

Si desea que el router defina los ajustes de hora para que ésta cambie en función de las horas de luz y las horas estándar, seleccione **Ajustar el reloj automáticamente para cambios de hora según la luz solar**.

## Aplicar

Haga clic en esta opción para aplicar los ajustes de fecha y hora que ha definido en los campos, Fecha, Hora y Zona horaria.

# NTP

**NTP** (Network Time Protocol) permite que los routers de su red sincronicen sus ajustes de hora con un servidor NTP. Un grupo de clientes NTP que obtiene información sobre la fecha y la hora de una misma fuente tendrá unos ajustes de hora más uniformes. Esta ventana permite visualizar la información del servidor NTP que se ha configurado, añadir información nueva o editar o eliminar la información existente.

**Nota**

---

Si el router no admite los comandos NTP, esta rama no aparecerá en el árbol Propiedades del router.

---

## Dirección IP

La dirección IP de un servidor NTP.

Si su organización no dispone de ningún servidor NTP, tiene la opción de utilizar un servidor disponible públicamente como, por ejemplo, el servidor que se describe en la dirección URL siguiente:

<http://www.eecis.udel.edu/~mills/ntp/clock2a.html>

## Interfaz

La interfaz a través de la cual el router se comunicará con el servidor NTP.

## Preferir

En esta columna aparece **Sí** en el caso que el servidor NTP se haya designado como servidor NTP preferido. Se establecerá contacto con los servidores NTP preferidos antes de hacerlo con los no preferidos. Puede haber más de un servidor NTP preferido.

## Agregar

Haga clic en esta opción para agregar información del servidor NTP.

### Editar

Haga clic para editar una configuración de servidor NTP especificada.

### Eliminar

Haga clic para eliminar una configuración de servidor NTP especificada.

## Agregar/Editar detalles del servidor NTP

Agregue o edite información de un servidor [NTP](#) en esta ventana.

### Dirección IP

Especifique o edite la dirección IP del servidor NTP.

### Preferir

Haga clic en esta casilla si desea que este servidor NTP sea el preferido.

### Interfaz

Seleccione la interfaz del router que proporcionará acceso al servidor NTP. Puede utilizar el comando del CLI **show IP routes** para determinar qué interfaz tiene una ruta hasta este servidor NTP.



#### Nota

---

Se creará una regla de acceso ampliada para el tráfico del puerto 123 y se aplicará a la interfaz que seleccione en esta ventana. Si esta interfaz ya dispone de una regla de acceso, Cisco SDM añadirá declaraciones para permitir el tráfico del puerto 123 en esta interfaz. Si la regla existente es una regla de acceso estándar, Cisco SDM la cambiará por una regla ampliada para poder especificar el tipo de tráfico y su destino.

---



## Clave de autenticación

Marque esta casilla si el servidor NTP utiliza una clave de autenticación y especifique la información requerida en los campos. La información de estos campos debe coincidir con la información de clave del servidor NTP.

### Número de clave

Especifique el número para la clave de autenticación. El intervalo de números de clave es de 0 a 4.294.967.295.

### Valor de clave

Especifique la clave utilizada por el servidor NTP. El valor de clave puede utilizar cualquiera de las letras de la A a la Z, en mayúsculas o minúsculas, y no puede tener más de 32 caracteres.

### Confirmar valor de clave

Vuelva a especificar el valor de la clave para confirmar su exactitud.

## SNTP

Esta ventana aparece en los routers Cisco 830. El protocolo Simple Network Time Protocol (SNTP) es una versión menos compleja del protocolo Network Time Protocol (NTP). NTP permite que los routers de su red sincronicen su configuración horaria con un servidor NTP. Un grupo de clientes NTP que obtiene información sobre la fecha y la hora de una misma fuente tendrá unos ajustes de hora más uniformes. Esta ventana permite visualizar la información del servidor NTP que se ha configurado, añadir información nueva o editar o eliminar la información existente.



### Nota

---

Si el router no admite los comandos NTP, esta rama no aparecerá en el árbol Propiedades del router.

---

## Propiedad

El nombre definido por el sistema para este servidor NTP.

**Valor**

La dirección IP para este servidor NTP.

**Agregar**

Haga clic en esta opción para agregar información del servidor NTP.

**Editar**

Haga clic para editar una configuración de servidor NTP especificada.

**Eliminar**

Haga clic para eliminar una configuración de servidor NTP especificada.

**Agregar detalles del servidor NTP**

Especifique la dirección IP de un servidor [NTP](#) en esta ventana.

**Nota**

---

Se creará una regla de acceso ampliada para el tráfico del puerto 123 y se aplicará a la interfaz que seleccione en esta ventana. Si esta interfaz ya disponía de una regla de acceso, Cisco SDM añadirá declaraciones para permitir el tráfico del puerto 123 en esta interfaz. Si la regla existente era una regla de acceso estándar, Cisco SDM la cambiará por una regla ampliada para poder especificar el tipo de tráfico y su destino.

---

**Dirección IP**

Especifique la dirección IP del servidor NTP en formato de decimales con puntos. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

# Registro

Utilice esta ventana para activar el registro de los mensajes del sistema y especificar los hosts de registro donde se pueden guardar los registros. Se puede especificar el nivel de mensajes de registro que se desea enviar y recibir, y también introducir el nombre de host o la dirección IP de múltiples hosts de registro.

## Dirección IP/Nombre de host

Haga clic en **Agregar** y especifique la dirección IP o nombre de host de un host de red al que desea que el router envíe los mensajes del registro para almacenarlo. Los botones **Editar** y **Eliminar** le permiten modificar la información que ha especificado y eliminar entradas.

Especifique los tipos de mensajes que se envían a hosts de registro eligiendo el nivel de registro desde la lista desplegable **Nivel de registro**. Consulte el apartado [Nivel de registro](#) para obtener más información.

## Nivel de registro

Los siguientes niveles de registro están disponibles en las listas desplegables **Nivel de registro**:

- emergencias (0)
- alertas (1)
- crítico (2)
- errores (3)
- advertencias (4)
- notificaciones (5)
- informativo (6)
- depuración (7)

El registro captura todos los mensajes del nivel que elija más todos los mensajes de los niveles inferiores, o bien el router envía todos los mensajes del nivel que elija más todos los mensajes de niveles inferiores a los hosts de registro. Por ejemplo, si elige notificaciones (5), el registro recupera o envía mensajes de los niveles 0 a 5. Los mensajes de registro del firewall requieren un nivel de registro de depuración (7), mientras que los mensajes de registro de seguridad de la aplicación requieren un nivel informativo (6).

## Registro a un búfer

Si desea que los mensajes de sistema se registren en el búfer del router, seleccione la casilla **Búfer de registro** en el cuadro de diálogo que aparece en Cisco SDM cuando se hace clic en **Editar**, y luego especifique el tamaño del búfer en el campo Tamaño del búfer. Cuanto mayor sea el tamaño del búfer, más entradas se podrán guardar en él antes de eliminar las entradas más antiguas para dejar espacio a las nuevas. Sin embargo, debe encontrar el equilibrio entre las necesidades del registro y el rendimiento del router.

Especifique los tipos de mensajes que se recuperan en el registro eligiendo el nivel de registro de la lista desplegable **Nivel de registro**. Consulte el apartado [Nivel de registro](#) para obtener más información.

## SNMP

Esta ventana le permite activar [SNMP](#), definir las cadenas de comunidad SNMP y especificar información sobre el administrador de interrupciones SNMP.

### Activar SNMP

Marque esta casilla de verificación para activar SNMP. Desmárquela para desactivar SNMP. SNMP está activado por defecto.

### Cadena de comunidad

Las cadenas de comunidad SNMP son contraseñas integradas en las Bases de Información de Gestión (MIB). Las MIB guardan datos acerca de la operación del router y deben estar disponibles para usuarios remotos autenticados. Los dos tipos de cadenas de comunidad son las cadenas de comunidad “públicas”, que proporcionan acceso de sólo-lectura a todos los objetos en la MIB excepto las cadenas de comunidad, y las cadenas de comunidad “privadas”, que proporcionan acceso de lectura-escritura a todos los objetos en la MIB, excepto las cadenas de comunidad.

En la tabla de cadenas de comunidad aparecen todas las cadenas de comunidad configuradas y sus tipos. Utilice el botón **Agregar** para visualizar el cuadro de diálogo Add a Community String (Agregar una cadena de comunidad) y crear nuevas cadenas de comunidad. Haga clic en los botones **Editar** o **Eliminar** para editar o eliminar la cadena de comunidad seleccionada de la tabla.

## Receptor de interrupciones

Especifique direcciones IP y cadenas de comunidad de los receptores de interrupciones, es decir, las direcciones a las que se debe enviar la información sobre las interrupciones. Normalmente, se trata de las direcciones IP de las estaciones de gestión SNMP que supervisan su dominio. Consulte con el administrador de sitios para determinar la dirección si no está seguro de ella.

Haga clic en los botones **Agregar**, **Editar**, o **Eliminar** para administrar la información del receptor de interrupciones.

## Ubicación del servidor SNMP

Campo de texto que puede utilizar para especificar la ubicación del servidor SNMP. No se trata de ningún parámetro de configuración que afecte al funcionamiento del router.

## Contacto del servidor SNMP

Campo de texto que puede utilizar para especificar la información de contacto para una persona que gestiona el servidor SNMP. No se trata de ningún parámetro de configuración que afecte al funcionamiento del router.

# Netflow

Esta ventana muestra cómo está configurado el router para supervisar usuarios principales (top talkers) de Netflow en interfaces que tienen Netflow configurado. Para obtener más información acerca de los elementos que se muestran, consulte [Usuarios de Netflow](#)

Usted puede supervisar los parámetros de Netflow en el router y ver las estadísticas de los usuarios principales en **Monitor > Estado de interfaz** y en **Monitor > Estado de tráfico > N Flujos de tráfico principales**. Si *no* activa los usuarios principales de Netflow, se les supervisará.

## Usuarios de Netflow

En esta ventana podrá configurar la supervisión de Netflow y ver los usuarios principales.

### Activar usuarios principales

Marque la casilla de verificación **Activar usuarios principales** para activar la supervisión de los usuarios principales en las interfaces que poseen configuración Netflow.

### Usuarios principales

Establezca la cantidad de usuarios principales en el cuadro de cantidad de **Usuarios principales**. Escoja un número entre 1 y 200. Cisco SDM rastreará y registrará datos hasta la cantidad de usuarios principales que establezca.

### Límite de tiempo de caché

Establezca el límite de tiempo, en milisegundos, para el caché de usuarios principales en el cuadro numérico **Tiempo límite de caché**. Escoja un número entre 1 y 3.600.000. El caché de usuarios principales se actualizará cuando se alcance el límite de tiempo.

### Ordenar por

Elija cómo ordenar los usuarios principales escogiendo bytes o paquetes de la lista desplegable **Ordenar por**.

# Acceso a router

En esta ventana se explican las funciones que se incluyen en el acceso al router.

## Cuentas de usuario: Configurar cuentas de usuario para el acceso al router

Desde esta ventana se pueden definir cuentas y contraseñas que permitirán a los usuarios autenticarse cuando se registren al router por medio de [HTTP](#), [Telnet](#), [PPP](#) o algún otro medio.

### Nombre de usuario

Nombre de cuenta de usuario.

### Contraseña

Contraseña de cuenta de usuario, mostrada con asteriscos (\*).



#### Nota

---

La contraseña de usuario no es lo mismo que la activación de la contraseña secreta configurada en la ficha Contraseña, dentro de Propiedades del dispositivo. La contraseña de usuario permite que es usuario especificado se registre en el router para acceder a un conjunto limitado de comandos.

---

### Nivel de privilegio

Nivel de privilegio para el usuario.

## Nombre de la vista

Si se ha asociado una vista del CLI con la cuenta de usuario, el nombre de la vista aparece en esta columna. Las vistas definen el acceso del usuario a Cisco SDM según la función del usuario. Para obtener más información, haga clic en [Asociar una vista al usuario](#).



### Nota

Si Cisco SDM se inicia con una vista definida por el usuario o con una vista alterada definida por Cisco SDM, Cisco SDM funcionará en modo Supervisión y el usuario tendrá privilegios de sólo lectura. Las funciones de Cisco SDM que se pueden supervisar dependen de los comandos que estén presentes en la vista. No todas las funciones estarán disponibles para que el usuario las supervise.

## ¿Qué desea hacer?

Para:	Haga lo siguiente:
Agregar una nueva cuenta de usuario.	Haga clic en <b>Agregar</b> . A continuación, agregue la cuenta en la ventana Agregar una cuenta de usuario.
Editar una cuenta de usuario.	Seleccione la cuenta de usuario y haga clic en <b>Editar</b> . A continuación, edite la cuenta en la ventana Editar un nombre de usuario.
Eliminar una cuenta de usuario.	Seleccione la cuenta de usuario y haga clic en <b>Eliminar</b> . A continuación, confirme la eliminación en la casilla de alerta que aparecerá.

## Agregar/Editar un nombre de usuario

Agregue o edite una cuenta de usuario en los campos que contiene esta ventana.

### Nombre de usuario

En este campo especifique o edite el nombre de usuario.

### Contraseña

En este campo especifique o edite la contraseña.



## Confirmar contraseña

Especifique nuevamente la contraseña en este campo. Si la contraseña y la contraseña de confirmación no corresponden entre sí, aparecerá una ventana de error al hacer clic en **Aceptar**.

Al hacer clic en **Aceptar** aparecerá la información de la cuenta nueva o editada en la ventana Configurar cuentas de usuario para Telnet/SSH.

## Casilla de verificación Cifrar contraseña mediante el algoritmo hash MD5

Marque esta casilla si desea que la contraseña se cifre mediante el algoritmo MD5 (Message Digest 5) unidireccional, que proporciona una protección de cifrado de gran seguridad.



### Nota

Los protocolos que requieren la recuperación de contraseñas de texto plano, como **CHAP**, no se pueden utilizar con contraseñas cifradas por MD5. El cifrado de MD5 no es reversible. Para recuperar la contraseña de texto plano, deberá eliminar la cuenta de usuario y crearla nuevamente sin marcar la opción **Cifrar contraseña**.

## Nivel de privilegio

Especifique el nivel de privilegio para el usuario. Si se aplica a un comando del CLI, ese comando sólo podrá ser utilizado por usuarios con un nivel de privilegio igual o superior al nivel definido para el comando.

## Asociar una vista al usuario

Este campo se muestra cuando configura cuentas de usuario para acceso al router. Es posible que no sea visible si trabaja en un área diferente de Cisco SDM.

Seleccione la opción **Asociar una vista al usuario** si desea restringir el acceso del usuario a una vista en particular. Si asocia una vista con cualquier usuario por primera vez, se le pedirá que especifique la contraseña de vista. Esta opción sólo se encuentra disponible en el nodo Acceso a router del árbol Tareas adicionales.

**Nombre de la vista:**

Seleccione la vista que desee asociar con este usuario de la siguiente lista:

- **SDM\_Administrator:** un usuario asociado con el tipo de vista **SDM\_Administrator** posee acceso ilimitado a Cisco SDM y puede realizar todas las operaciones permitidas por Cisco SDM.
- **SDM\_Monitor:** un usuario asociado a un tipo de vista **SDM\_Monitor** puede supervisar todas las funciones admitidas en Cisco SDM. El usuario no puede enviar configuraciones por medio de Cisco SDM. El usuario puede desplazarse por las distintas áreas de Cisco SDM, como Interfaces y conexiones, Firewall y VPN. Sin embargo, los componentes de la interfaz de usuario de estas áreas estarán desactivados.
- **SDM\_Firewall:** un usuario asociado al tipo de vista **SDM\_Firewall** puede usar las funciones Firewall y Supervisión de Cisco SDM. El usuario puede configurar firewalls y ACL mediante el Asistente para firewall, la Vista de política del firewall y el Editor ACL. Los componentes de la interfaz de usuario de las otras áreas estarán desactivados para este usuario.
- **SDM\_EasyVPN\_Remote:** un usuario asociado al tipo de vista **SDM\_EasyVPN\_Remote** puede utilizar las funciones de Easy VPN remoto de Cisco SDM. El usuario puede crear conexiones de Easy VPN remoto y editarlas. Los componentes de la interfaz de usuario de las otras áreas estarán desactivados para este usuario.

**Detalles**

El área **Asociar una vista al usuario** muestra detalles acerca de la vista especificada. Haga clic en el botón **Detalles** para obtener información más detallada acerca de la vista especificada.

## Contraseña de la vista

Al asociar una vista con cualquier usuario por primera vez, se le pedirá que especifique la contraseña de vista para las vistas definidas por Cisco SDM. Utilice esta contraseña para cambiar a otras vistas.

**Especifique la contraseña de la vista**

Especifique la contraseña de vista en el campo Ver Contraseña.

# Configuración VTY

En esta ventana se muestra la configuración del terminal virtual (vty) del router. La columna Propiedad contiene intervalos de línea configurados y propiedades configurables para cada intervalo. Los ajustes para estas propiedades aparecen en la columna Valor.

En esta tabla se muestran los ajustes vty del router y se incluyen las siguientes columnas:

- Intervalo de líneas: muestra el intervalo de conexiones vty a las que se aplican el resto de los ajustes de la fila.
- Protocolos de entrada permitidos: muestra los protocolos configurados para la entrada. Puede tratarse de [Telnet](#), [SSH](#) o de ambos.
- Protocolos de salida permitidos: muestra los protocolos configurados para la salida. Puede tratarse de Telnet, SSH o de ambos.
- Límite de tiempo EXEC: el número de segundos de inactividad tras el que finalizará una sesión.
- Clase de acceso entrante: nombre o número de la regla de acceso aplicada a la dirección de entrada del intervalo de línea.
- Clase de acceso saliente: nombre o número de la regla de acceso aplicada a la dirección de salida del intervalo de línea.
- ACL: si se configura, muestra la [ACL](#) asociada con las conexiones vty.
- Política de autenticación: la política de autenticación [AAA](#) asociada con esta línea vty. Este campo es visible si AAA está configurado en el router.
- Política de autorización: la política de autorización AAA asociada con esta línea vty. Este campo es visible si AAA está configurado en el router.

**Nota**

Para utilizar SSH como protocolo de entrada o de salida, debe activarlo haciendo clic en **SSH** del árbol Tareas adicionales y generando una clave RSA.

## Editar líneas vty

Esta ventana le permite editar la configuración del terminal virtual (vty) del router.

### Intervalo de líneas

Especifique el intervalo de líneas vty a las que se aplicarán los ajustes realizados en esta ventana.

### Límite de tiempo

Especifique el número de segundos de inactividad que se permiten antes de que se cierre una conexión inactiva.

### Protocolo de entrada

Seleccione los protocolos de entrada haciendo clic en las casillas correspondientes.

#### Casilla de verificación Telnet

Seleccione esta casilla para activar el acceso Telnet al router.

#### Casilla de verificación SSH

Seleccione esta casilla para permitir que clientes SSH inicien sesión en el router.

### Protocolo de salida

Seleccione los protocolos de salida haciendo clic en las casillas correspondientes.

#### Casilla de verificación Telnet

Seleccione esta casilla para activar el acceso Telnet al router.

#### Casilla de verificación SSH

Marque esta casilla para permitir que el router establezca comunicación con clientes SSH.

## Regla de acceso

Puede asociar las reglas de acceso para filtrar el tráfico entrante o saliente a las líneas vty del intervalo.

### Entrante

Escriba el nombre o número de la regla de acceso que filtra el tráfico saliente, o haga clic en el botón y busque la regla de acceso.

### Saliente

Especifique el nombre o número de la regla de acceso para filtrar el tráfico saliente, o haga clic en el botón y busque la regla de acceso.

## Autenticación/Autorización

Estos campos están visibles cuando AAA está activado en el router. AAA se puede activar haciendo clic en **Tareas Adicionales > AAA > Activar**.

### Política de autenticación

Seleccione la política de autenticación que desea utilizar para esta línea vty.

### Política de autorización

Seleccione la política de autorización que desea utilizar para esta línea vty.

## Configurar políticas de acceso a la gestión

Utilice esta ventana para revisar las políticas de acceso a la gestión existentes y para seleccionar las políticas que desee editar. Las políticas de acceso a la gestión especifican las redes y hosts que podrán acceder a la interfaz de línea de comandos del router. En la política, es posible especificar los protocolos que pueden utilizar el host o la red y la interfaz del router que llevará el tráfico de gestión.

## Host/red

Una dirección de red o dirección IP de un host. Si se determina una dirección de red, la política se aplica a todos los hosts que contiene dicha red. Si se determina una dirección de host, la política se aplica a ese host.

Una dirección de red se muestra en el formato número de red/bits de red, como en el ejemplo que aparece a continuación.

```
172.23.44.0/24
```

Para obtener más información acerca de este formato y acerca del uso de las direcciones IP y las máscaras de subred, consulte [Direcciones IP y máscaras de subred](#).

## Interfaz de gestión

La interfaz del router por la que se transmitirá el tráfico de gestión.

## Protocolos permitidos

En esta columna aparece una lista de los protocolos que pueden utilizar los hosts especificados cuando establecen comunicación con el router. Se pueden configurar los protocolos siguientes:

- **Cisco SDM**: los hosts especificados pueden utilizar Cisco SDM.
- **Telnet**: los hosts especificados pueden utilizar Telnet para acceder al CLI del router.
- **SSH**: los hosts especificados pueden utilizar Secure Shell para acceder al CLI del router.
- **HTTP**: los hosts especificados pueden utilizar HTTP (Hypertext Transfer Protocol) para acceder al router. Si se especifica Cisco SDM, también se deberá especificar HTTP o HTTPS.
- **HTTPS**: los hosts especificados pueden utilizar HTTPS (Hypertext Transfer Protocol Secure) para acceder al router.
- **RCP**: los hosts especificados pueden utilizar RCP (Remote Copy Protocol) para gestionar archivos del router.
- **SNMP**: los hosts especificados pueden utilizar SNMP (Simple Network Management Protocol) para gestionar el router.

### Botón Agregar

Haga clic para agregar una política de gestión y especifique la política en la ventana Agregar una política de gestión.

### Botón Editar

Haga clic para editar una política de gestión y especifique la política en la ventana Editar una política de gestión.

### Botón Eliminar

Haga clic para eliminar una política de gestión específica.

### Botón Aplicar

Haga clic en este botón para aplicar los cambios efectuados en la ventana Agregar/Editar una política de gestión a la configuración del router.

### Botón Descartar cambios

Haga clic en este botón para descartar los cambios efectuados en la ventana Agregar/Editar una política de gestión a la configuración del router. De este modo se descartarán los cambios realizados y se quitarán de la ventana Configurar políticas de acceso a la gestión.

## Agregar/Editar una política de gestión

Utilice esta ventana para agregar o editar una política de gestión.

### Tipo

Especifique si la dirección que proporciona es la dirección de un host específico o de una red.

### Dirección IP/máscara de subred

Si ha especificado **Red** en el campo Tipo, escriba la dirección IP de un host o la dirección de la red y la máscara de subred. Para obtener más información, consulte [Direcciones IP y máscaras de subred](#).

## Interfaz

Seleccione la interfaz por la que desea que pase el tráfico de gestión. La interfaz debe ser la ruta más directa desde el host o la red hasta el router local.

## Protocolos de gestión

Especifique los protocolos de gestión permitidos para el host o la red.

### Permitir SDM

Marque esta opción para permitir que el host o la red especificados accedan a Cisco SDM. Si marca esta casilla, se seleccionarán automáticamente los protocolos siguientes: Telnet, SSH, HTTP, HTTPS y RCP. Aunque seleccione esta opción también podrá dar permiso a protocolos adicionales.

Si desea que los usuarios utilicen protocolos seguros cuando se conecten a Cisco SDM, marque la opción **Permitir sólo protocolos seguros**. Si marca esta casilla, se seleccionarán automáticamente los protocolos siguientes: SSH, HTTPS y RCP. Si, a continuación, selecciona un protocolo no seguro, como Telnet, Cisco SDM anulará la selección de **Permitir sólo protocolos seguros**.

### Puede especificar protocolos de gestión de forma individual

Si desea especificar protocolos individuales que puedan utilizar el host o la red, puede marcar cualquiera de estas casillas: [Telnet](#), [SSH](#), [HTTP](#), [RCP](#), o [SNMP](#).

Si los protocolos Telnet y SSH no están activados (marcados) en la ventana VTYs y SNMP no lo está en la ventana Propiedades de SNMP, Cisco SDM le solicitará que active estos protocolos cuando los especifique en esta ventana.



#### Nota

---

Las opciones **Permitir sólo protocolos seguros** y **HTTPS** se desactivarán si la imagen de Cisco IOS del router no admite HTTPS.

---



## Mensajes de error de acceso a la gestión

La función Acceso a la gestión puede generar los mensajes de error siguientes.

### Mensaje de error

Alerta de SDM: ANY Not Allowed (ANY no permitido)

**Explicación** Una política de gestión será de “sólo lectura” si cualquiera de sus reglas de origen o destino contienen la palabra clave “any”. Estas políticas no se pueden editar en la ventana Acceso a la gestión. Cualquier política que contenga la palabra “cualquiera” puede constituir un riesgo de seguridad debido a las siguientes razones:

- Si se asocia “any” al origen, se permite el tráfico desde cualquier red hacia el router.
- Si se asocia “any” al destino, se permite al acceso a cualquier nodo de la red admitido por el router.

**Acción recomendada** Se puede eliminar la entrada de acceso que origina este mensaje al seleccionar la regla en la ventana Reglas y hacer clic en **Editar**. De otro modo, se puede desasociar la regla de la interfaz a la cual se aplica desde la ventana Interfaces y Conexiones.

### Mensaje de error

Alerta de SDM: Unsupported Access Control Entry (Entrada de control de acceso no admitida)

**Explicación** Una política de gestión será de sólo lectura si las entradas de acceso no admitidas (ACE) se asocian con la interfaz o línea vty a la que ha aplicado la política de gestión. Puede utilizar el CLI para quitar las ACE no admitidas. Estas ACE no admitidas son las que contienen palabras clave o sintaxis que Cisco SDM no admite.

**Mensaje de error**

Alerta de SDM: SDM Not Allowed (SDM no permitido)

**Explicación** Este mensaje aparece si aún no ha configurado ninguna política de acceso a la gestión para permitir que un host o red acceda a Cisco SDM en este router.

**Acción recomendada** Deberá proporcionar una política de este tipo para poder acceder a Cisco SDM en este router. No es posible desplazarse a otras funciones ni enviar comandos al router hasta que configure una política de acceso de gestión para permitir el acceso de un host o una red a Cisco SDM.

**Mensaje de error**

Alerta de SDM: Current Host Not Allowed (Host vigente no permitido)

**Explicación** Este mensaje aparece si no ha configurado ninguna política de acceso a la gestión para permitir que el host o la red vigentes accedan a Cisco SDM en este router.

**Acción recomendada** Debe crear una política de este tipo para poder acceder a Cisco SDM en este router desde el host o la red vigentes. De lo contrario, perderá la conexión con el router al enviarle la configuración. Haga clic en **Sí** para agregar una política de acceso a la gestión del host o la red vigentes. Haga clic en **No** para continuar sin añadir ninguna política para el host o la red vigentes. Perderá el contacto con el router durante el envío del comando y se deberá conectar a Cisco SDM por medio de un host o una red distintos.

# SSH

Este router implementa el servidor SSH (Secure Shell), una función que permite a un cliente SSH establecer una conexión segura y cifrada con un router de Cisco. Esta conexión proporciona una funcionalidad similar a la de una conexión Telnet entrante pero permite utilizar un cifrado potente con autenticación del software Cisco IOS. El servidor SSH en el software Cisco IOS funcionará con clientes SSH disponibles de forma comercial y pública. Esta función estará desactivada si el router no utiliza ninguna imagen de Cisco IOS IPsec DES o 3DES y si la rama SSH del árbol Tareas adicionales no aparece..

El SSH utiliza una clave criptográfica para codificar los datos transmitidos entre el router y el cliente SSH. La generación de la clave criptográfica RSA en esta ventana permite establecer una comunicación SSH entre el router y los clientes SSH.

## Mensajes de estado

### **Crypto key is not set on this device (La clave criptográfica no está definida en este dispositivo)**

Aparece si no se ha configurado ninguna clave criptográfica para el dispositivo. Si no hay ninguna clave configurada, puede especificar un tamaño de módulo y generar una clave.

### **La clave RSA está definida en este router**

Aparece si se ha generado una clave criptográfica. SSH está activado en este router.

## Botón Tamaño del módulo clave

Es visible si no se ha generado una clave criptográfica. Haga clic en este botón y especifique el tamaño del módulo al que desea asignar la clave. Si desea un valor de módulo de 512 a 1.024, especifique un valor entero que sea múltiplo de 64. Si desea un valor mayor que 1.024, puede especificar 1.536 ó 2.048. Si especifica un valor mayor que 512, es posible que la generación de la clave tarde un minuto o más.

## Botón Generar clave RSA

Haga clic para generar una clave criptográfica para el router con el tamaño del módulo que haya especificado. Si se ha creado una clave criptográfica, este botón se desactiva.

# Configuración DHCP

Esta ventana explica cómo se gestionan las configuraciones DHCP en el router.

## Conjuntos DHCP

Esta ventana muestra los conjuntos DHCP configurados en el router.

### Nombre del conjunto

El nombre del conjunto DHCP.

### Interfaz

Interfaz donde se ha configurado el conjunto DHCP. Los clientes asociados a esta interfaz recibirán direcciones IP desde este conjunto DHCP.

### Detalles del conjunto DHCP *nombre*

Esta área proporciona los siguientes detalles acerca del conjunto identificado en *nombre*:

- **Intervalo del conjunto DHCP:** intervalo de direcciones IP que se pueden conceder a los clientes.
- **Dirección IP del router por defecto:** si el router dispone de una dirección IP en la misma subred que el conjunto DHCP, aparecerá aquí.
- **Servidores DNS:** la dirección IP de los servidores DNS que el router proporcionará a los clientes DHCP.
- **Servidores WINS:** la dirección IP de los servidores WINS que el router proporcionará a los clientes DHCP.
- **Nombre de dominio:** el nombre de dominio configurado en el router.
- **Tiempo de concesión:** tiempo durante el que el router concede una dirección IP a un cliente.
- **Importar todo:** indica si el router importa parámetros de opciones de DHCP a la base de datos del servidor DHCP y si envía esta información a los clientes DHCP en la LAN cuando solicitan direcciones IP.

## Agregar

Elija esta opción para crear un nuevo conjunto DHCP. El usuario debe especificar el nombre del conjunto DHCP, la red del conjunto DHCP, el rango de direcciones IP del conjunto DHCP, y el tiempo de concesión. También existe la opción de configurar los servidores DNS, el servidor WINS, el nombre de dominio y el router por defecto desde el conjunto DHCP.

## Editar

Seleccione esta opción para editar un conjunto DHCP existente.

## Eliminar

Seleccione esta opción para eliminar un conjunto DHCP.

## Estado del conjunto DHCP

Haga clic en este botón para ver las direcciones de IP concedidas por el conjunto especificado. Si un conjunto DHCP contiene parámetros distintos a la red de conjuntos, el rango de direcciones IP, el tiempo de concesión, los servidores DNS, los servidores WINS, el nombre de dominio y el router por defecto, Cisco SDM muestra este conjunto como de “sólo lectura”. Si un conjunto contiene un rango de direcciones IP discontinuo, también se muestra como de “sólo lectura”.

# Agregar o Editar conjunto DHCP

Utilice esta ventana para agregar o editar un conjunto DHCP. Los conjuntos por defecto de Cisco SDM no se pueden editar.

## Nombre del conjunto DHCP

Proporcione un nombre para el conjunto DHCP en este campo.

## Red del conjunto DHCP

Ingrese la red desde la que se obtendrán las direcciones IP del conjunto; por ejemplo, 192.168.233.0. No puede ser la dirección IP de un host individual.

## Máscara de subred

Especifique el número de máscara de subred. La máscara de subred 255.255.255.0 proporciona la dirección IP 255.

## Conjunto DHCP

Especifique las direcciones IP inicial y final para el conjunto. Por ejemplo, si la red es 192.168.233.0 y la máscara de subred es 255.255.255.0, la dirección inicial es 192.168.233.1 mientras que la dirección final es 192.168.233.254.

## Longitud de concesión

Especifique el tiempo durante el que las direcciones se concederán a los clientes. Es posible especificar que las concesiones de las direcciones no venzan o especificar el tiempo de concesión en días, horas y minutos. Recuerde no exceder 365 días, 23 horas o 59 minutos.

## Opciones de DHCP

Especifique información sobre los servidores DNS, los servidores WINS, el nombre de dominio y el router por defecto en los campos de las opciones DHCP. Estos valores se enviarán a los clientes DHCP cuando requieran una dirección IP.

### **Importar todas las opciones de DHCP en la base de datos del servidor DHCP**

Haga clic en esta opción si desea importar los parámetros de opción de DHCP a la base de datos del servidor DHCP y también envía esta información a los clientes DHCP en la LAN cuando solicitan direcciones IP.

## Asociaciones DHCP

Esta ventana muestra las asociaciones DHCP manuales existentes. Una asociación DHCP manual le permite asignar la misma dirección IP a un cliente específico cada vez que el cliente solicite una dirección IP de los conjuntos DHCP disponibles.

También puede agregar nuevas asociaciones, editar o eliminar asociaciones ya existentes.

**Nombre de la asociación**

Nombre asignado a la asociación DHCP.

**Máscara de host/IP**

Dirección IP y máscara asociadas al cliente.

**Dirección MAC**

Dirección MAC del cliente.

**Tipo**

El tipo de dirección MAC corresponde a uno de los siguientes:

- Ethernet  
El cliente posee una dirección de hardware.
- IEEE802  
El cliente posee una dirección de hardware.
- <Ninguno>  
El cliente posee un identificador de cliente.

**Nombre de cliente**

Nombre opcional asignado al cliente.

**Botón Agregar**

Haga clic para agregar una nueva asociación manual DHCP.

**Botón Editar**

Haga clic para editar la asociación manual DHCP especificada.

**Botón Eliminar**

Haga clic para eliminar la asociación manual DHCP especificada.

## Agregar o Editar la Asociación DHCP

Esta ventana permite agregar asociaciones manuales DHCP o editar las ya existentes.

### Nombre

Especifique el nombre que desea dar a la asociación DHCP. Si se está editando la asociación DHCP, el campo de nombre es de “sólo lectura”.

### IP del host

Especifique la dirección IP que desea asociar al cliente. La dirección debe ser parte del conjunto DHCP disponible para el cliente. No especifique una dirección utilizada por otra asociación DHCP.

### Máscara

Especifique la máscara utilizada para la dirección IP del host.

### Identificador

Desde el menú desplegable seleccione una forma para identificar al cliente con una dirección MAC.

### Dirección MAC

Especifique la dirección MAC del cliente. No especifique una dirección utilizada por otra asociación DHCP.

### Tipo

Si seleccionó **Dirección de hardware** del menú Identificador, elija **Ethernet** o **IEEE802** para configurar el tipo de dirección MAC del cliente.

### Nombre del cliente (Opcional)

Especifique un nombre para identificar al cliente. El nombre debe ser un nombre de host únicamente, no un nombre tipo dominio. Por ejemplo, se acepta el nombre *router*, pero no el nombre *router.cisco.com*.



# Propiedades de DNS

**DNS** (Domain Name System) es una base de datos de nombres de host de Internet con sus direcciones IP correspondientes distribuida por los servidores DNS designados. Permite a los usuarios de la red referirse a los hosts por el nombre en lugar de por la dirección IP, que resulta más difícil de recordar. Utilice esta ventana para activar el uso de los servidores DNS para la traducción de nombres de host en direcciones.

## Casilla de verificación Activar el nombre de host basado en DNS para la traducción de direcciones

Marque esta casilla para que el router utilice DNS. Desmárquela si no desea utilizar DNS.

## Dirección IP DNS

Especifique las direcciones IP de los servidores DNS a los que desea que el router envíe solicitudes de DNS.

Haga clic en los botones **Agregar**, **Editar** o **Eliminar** para administrar la información de la dirección IP DNS.

# Métodos DNS dinámicos

Esta ventana muestra una lista de métodos DNS dinámicos.

Cada método DNS dinámico que se muestra enviará con su actualización el nombre de host y el nombre de dominio configurados en **Configurar > Tareas adicionales > Propiedades del router**. Sin embargo, si se crea un método DNS dinámico al momento de configurar una interfaz WAN, se puede dejar sin efecto el nombre de host y el nombre de dominio configurados en **Configurar > Tareas adicionales > Propiedades del router**. El nuevo nombre de host y de dominio será válido únicamente para ese método DNS dinámico.

Algunos métodos DNS dinámicos son de “sólo lectura”. Fueron configurados en el software Cisco IOS mediante el CLI y, por lo tanto, no pueden ser editados o eliminados. Para poder editar estos métodos de “sólo lectura”, use el CLI para cambiar el caché interno o las opciones de grupo de host a HTTP o IETF.

### Botón Agregar

Haga clic en el botón **Agregar** para crear un nuevo método DNS dinámico.

### Botón Editar

Para editar un método DNS dinámico, elíjalo de la lista de métodos DNS dinámicos existentes y luego haga clic en el botón **Editar**.

### Botón Eliminar

Para eliminar un método DNS dinámico, elíjalo de la lista de métodos DNS dinámicos existentes y luego haga clic en el botón **Eliminar**.

**Nota**

---

Si intenta eliminar un método DNS dinámico asociado a una o más interfaces aparecerá una advertencia.

---

## Agregar o Editar un método DNS dinámico

Esta ventana permite agregar o editar un método DNS manual. Configure el tipo de método eligiendo entre **HTTP** o **IETF**.

### HTTP

HTTP es un tipo de método DNS dinámico que actualiza un proveedor de servicio DNS con cambios en la dirección IP de la interfaz asociada.

### Servidor

Si se usa HTTP, elija la dirección de dominio del proveedor de servicio DNS desde el menú desplegable.

### Nombre de usuario

Si se usa HTTP, especifique un nombre de usuario para acceder al proveedor de servicio DNS.

## Contraseña

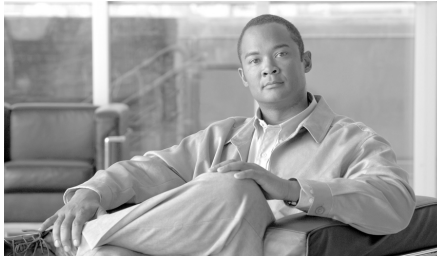
Si se usa HTTP, especifique una contraseña para acceder al proveedor de servicio DNS.

## IETF

IETF es un tipo de método DNS dinámico que actualiza un servidor DNS con cambios en la dirección IP de la interfaz asociada.

Si usa IETF, configure un servidor DNS para el router en **Configurar > Tareas adicionales > DNS**.





# CAPÍTULO 29

## Editor ACL

---

Las reglas definen cómo responderá el router a un tipo de tráfico en particular. Mediante Cisco SDM, puede crear reglas de acceso que obliguen al router a bloquear determinados tipos de tráfico a la vez que permite otros, reglas NAT que definan el tráfico que debe someterse a la traducción de direcciones y reglas [IPSec](#) que especifiquen el tráfico que debe cifrarse. Además, Cisco SDM proporciona reglas por defecto que se utilizan en las configuraciones guiadas y que el usuario puede revisar y utilizar al crear sus propias reglas de acceso. También permite ver las reglas que no se han creado mediante Cisco SDM, denominadas reglas externas, y las reglas con una sintaxis no compatible con Cisco SDM, denominadas reglas no admitidas.

Utilice la pantalla Reglas para ver un resumen de las reglas en la configuración del router y para navegar hacia otras ventanas y crear, editar o eliminar reglas.

### Categoría

Un tipo de regla. Uno de los siguientes:

- |                            |   |
|----------------------------|---|
| Reglas de acceso           | Reglas que rigen el tráfico que puede entrar y salir de la red. Estas reglas las utilizan las interfaces de router y las líneas VTY que permiten a los usuarios conectarse al router. |
| Reglas <a href="#">NAT</a> | Reglas que determinan cómo las direcciones IP privadas se traducen en direcciones IP de Internet válidas.   |

Reglas <b>IPSec</b>	Reglas que determinan qué tráfico se cifrará en las conexiones seguras.
Reglas <b>NAC</b>	Reglas que especifican las direcciones IP que serán admitidas hacia la red o bloqueadas desde la red.
Reglas de firewall	Reglas que pueden especificar las direcciones de origen y destino, el tipo de tráfico y si el tráfico debe permitirse o denegarse.
Reglas <b>QoS</b>	Reglas que especifican el tráfico que debe pertenecer a la clase de QoS con la que está asociada la regla.
Reglas no admitidas	Reglas que no se han creado mediante Cisco SDM y que no son compatibles con Cisco SDM. Estas reglas son de sólo lectura y no pueden modificarse mediante Cisco SDM.
Reglas definidas externamente	Reglas que no se han creado mediante Cisco SDM pero que son compatibles con Cisco SDM. Estas reglas no pueden asociarse con ninguna interfaz.
Reglas de Cisco SDM por defecto	Éstas son reglas predefinidas que utilizan los asistentes para Cisco SDM y que se pueden aplicar en las ventanas Tareas adicionales>Editor ACL.

## Nº de reglas

El número de reglas de este tipo.

## Descripción

Una descripción de la regla, si se ha especificado una.

### Para configurar reglas:

Haga clic en la categoría de la regla en el árbol de reglas para ver la ventana para ese tipo de regla. Cree y modifique las reglas en dicha ventana.

El tema de ayuda para estas ventanas contiene procedimientos generales que podrán ser de gran utilidad. [Procedimientos útiles para las reglas de acceso y firewalls](#) incluye procedimientos detallados paso por paso para otras tareas.

# Procedimientos útiles para las reglas de acceso y firewalls

En esta sección se incluyen procedimientos que podrán ser de gran utilidad.

- [¿Como se visualiza la actividad en el firewall?](#)
- [¿Cómo se configura un firewall en una interfaz no compatible?](#)
- [¿Cómo se configura un firewall después de configurar una VPN?](#)
- [¿Cómo se puede permitir que pase determinado tráfico por una interfaz DMZ?](#)
- [¿Cómo se modifica un firewall existente para permitir el tráfico procedente de una nueva red o host?](#)
- [¿Cómo se configura el paso de NAT \(NAT Passthrough\) para un firewall?](#)
- [¿Cómo se permite que el tráfico llegue al concentrador Easy VPN a través del firewall?](#)
- [¿Cómo se asocia una regla a una interfaz?](#)
- [¿Cómo se anula la asociación de una regla de acceso con una interfaz?](#)
- [¿Cómo se elimina una regla que esté asociada a una interfaz?](#)
- [¿Cómo se crea una regla de acceso para una lista Java?](#)

# Ventanas de reglas

Estas ventanas permiten examinar, crear, modificar y eliminar reglas.

- Ventana Reglas de acceso: normalmente, las reglas de acceso definen el tráfico cuya entrada a la LAN o salida de la LAN se desea permitir o denegar. Sin embargo, también se pueden utilizar para otros propósitos.
- Ventana Reglas NAT: las reglas NAT se utilizan para especificar un conjunto de direcciones que se deben traducir.
- Ventana Reglas IPSec: las reglas IPSec son reglas ampliadas que se utilizan en las políticas IPSec para especificar el tráfico que se cifrará para las conexiones VPN.
- Ventana Reglas NAC: reglas que especifican las direcciones IP que serán admitidas hacia la red o bloqueadas desde la red.
- Ventana Reglas de firewall: reglas que pueden especificar las direcciones de origen y destino, el tipo de tráfico, y si el tráfico debe permitirse o denegarse.
- Ventana Reglas de QoS: reglas que especifican el tráfico que debe pertenecer a la clase de QoS con la que está asociada la regla.
- Ventana Reglas no admitidas: las reglas no admitidas contienen sintaxis o palabras clave no compatibles con Cisco SDM. Estas reglas pueden afectar el funcionamiento del router, pero Cisco SDM las marca como de sólo lectura.
- Ventana Reglas definidas externamente: las reglas definidas externamente son reglas que se han creado sin utilizar Cisco SDM.
- Ventana Reglas de Cisco SDM por defecto: las reglas de Cisco SDM por defecto son reglas de acceso previamente definidas, que se utilizan en las configuraciones iniciales guiadas y que se pueden utilizar en las configuraciones creadas por el usuario.
- Ventana Reglas NAC: las reglas NAC se usan en la política de excepción NAC con el fin de especificar hosts que se encuentran exentos del proceso de validación NAC. También se usan para definir los hosts o redes de control de admisión.



La parte superior de la pantalla proporciona una lista de las reglas de acceso que se han configurado en el router. Esta lista no incluye las reglas de Cisco SDM por defecto. Para ver estas reglas de Cisco SDM por defecto, haga clic en la rama **Reglas de SDM por defecto** del árbol Reglas.

La parte inferior de la ventana proporciona una lista de las entradas de regla asociadas con la regla seleccionada. Una entrada de regla consta de criterios contra los cuales se compara el tráfico entrante y saliente. Asimismo, también indica la acción que se debe llevar a cabo en el tráfico que satisface dichos criterios. Todo tráfico que no satisface los criterios de cualquiera de las entradas incluidas en este cuadro se abandona.

### Primera columna

Esta columna puede contener iconos que indican el estado de una regla.



Si la regla es de sólo lectura, en esta columna aparecerá el icono correspondiente.

### Nombre/Número

El nombre o número de la regla de acceso.

Los números del 1 al 99 se utilizan para identificar listas de acceso estándar. Los números del 100 al 199 se utilizan para identificar listas de acceso ampliadas. Los nombres, que contienen caracteres alfabéticos, permiten ampliar el intervalo de las listas de acceso estándar más allá del 99 y el de las listas de acceso ampliadas más allá del 199.

### Usado por

El nombre de la interfaz o los números VTY a los que se ha aplicado la regla.

### Tipo

El tipo de regla, estándar o ampliada.

Las reglas estándar comparan la dirección IP de origen de un paquete con sus criterios de dirección IP para determinar si coinciden. Los criterios de dirección IP de la regla pueden ser una sola dirección IP o partes de una dirección IP, definidas mediante una máscara inversa.



Las reglas ampliadas pueden examinar una mayor variedad de campos del paquete para determinar una coincidencia. Las reglas ampliadas pueden examinar el origen de un paquete y las direcciones IP, el tipo de protocolo, los puertos de origen y de destino y otros campos del paquete.

Las reglas de acceso pueden ser reglas estándar o ampliadas. Las reglas IPSec deben ser reglas ampliadas, ya que deben poder especificar un tipo de servicio. Las reglas definidas externamente pueden ser reglas estándar o ampliadas.

## Descripción

Una descripción de la regla, si se ha especificado alguna.

## Primera columna (área de entrada de reglas)

-  Permitir tráfico.
-  Denegar tráfico.

## Acción

La acción que se debe llevar a cabo cuando un paquete que satisface los criterios de esta entrada llega a la interfaz. Puede ser “Permit” o “Deny”:

- Permit: permitir el tráfico que satisface los criterios de esta fila.
- Deny: no permitir el tráfico que satisface los criterios de esta fila.

Haga clic en [Significados de las palabras clave “permit” y “deny”](#) para obtener más información acerca de las acciones de permitir y denegar dentro del contexto de un tipo específico de regla.

## Origen

Criterios de dirección IP de origen que el tráfico debe cumplir. Esta columna puede contener los elementos siguientes:

- Una dirección IP y una [máscara comodín](#). La dirección IP especifica una red y la máscara inversa especifica la parte de la dirección IP de la regla que la dirección IP del paquete debe cumplir.
- La palabra clave **any**. “Any” indica que la dirección IP de origen puede ser cualquier dirección IP.
- Un nombre de host.

## Destino

En el caso de las reglas ampliadas, los criterios de la dirección IP de destino que el tráfico debe cumplir. La dirección puede ser para una red o un host específico. Esta columna puede contener los elementos siguientes:

- Una dirección IP y una **máscara comodín**. La dirección IP especifica una red y la máscara inversa especifica la parte de la dirección IP de la regla que la dirección IP del paquete debe cumplir.
- La palabra clave **any**. “Any” indica que la dirección IP de origen puede ser cualquier dirección IP.
- Un nombre de host.

## Servicio

En el caso de las **reglas ampliadas**, el servicio especifica el tipo de tráfico que deben contener los paquetes que cumplen la regla. Esto se ve mostrando el servicio como, por ejemplo, echo-reply, seguido por un protocolo como ICMP. Una regla que permita o deniegue varios servicios entre los mismos puntos finales deberá contener una entrada para cada servicio.

## Atributos

Este campo puede contener información adicional acerca de esta entrada como, por ejemplo, si se ha activado el inicio de sesión.

## Descripción

Una breve descripción de la entrada.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Agregar una regla.	Haga clic en el botón <b>Agregar</b> y cree la regla en las ventanas que aparecen.
Editar una regla o una entrada de regla.	Seleccione la regla de acceso y haga clic en <b>Editar</b> . A continuación, modifique la regla en la ventana Editar una regla que aparece.

Si desea:	Haga lo siguiente:
Asociar una regla con una interfaz.	Consulte <a href="#">¿Cómo se asocia una regla a una interfaz?</a>
Eliminar una regla que no se ha asociado con ninguna interfaz.	Seleccione la regla de acceso y haga clic en <b>Eliminar</b> .
Eliminar una regla que se ha asociado con una interfaz.	Cisco SDM no permite eliminar reglas que se han asociado con una interfaz. Para eliminar este tipo de regla, primero debe anular su asociación con la interfaz. Consulte <a href="#">¿Cómo se elimina una regla que esté asociada a una interfaz?</a>
Lo que deseo hacer no se describe aquí.	El enlace siguiente contiene procedimientos que se pueden consultar: <a href="#">Procedimientos útiles para las reglas de acceso y firewalls</a> .

## Agregar/Editar una regla

Esta ventana permite agregar o editar una regla seleccionada en la ventana Reglas. Se puede cambiar el nombre o el número de la regla, agregar, cambiar, reordenar o eliminar entradas de la regla y agregar o cambiar la descripción de ésta.

### Nombre/Número

Permite agregar o editar el nombre o número de la regla.

La numeración de las reglas estándar debe oscilar entre 1 y 99, o entre 1.300 y 1.999.

La numeración de las reglas ampliadas debe oscilar entre 100 y 199, o entre 2.000 y 2.699.

Los nombres, que pueden contener caracteres alfabéticos, permiten asociar una etiqueta representativa a la regla de acceso.

### Tipo

Permite seleccionar el tipo de regla que se desea agregar. Las reglas estándar permiten que el router examine la red o el host de origen en el paquete. Las reglas ampliadas permiten que el router examine la red o el host de origen, la red o el host de destino y el tipo de tráfico que el paquete contiene.

## Descripción

En este campo puede especificar una descripción de la regla. Dicha descripción debe tener menos de 100 caracteres.

## Lista Entrada de regla

Esta lista muestra las entradas que forman la regla. Se puede agregar, editar o eliminar entradas. Asimismo, se pueden reordenar entradas, a fin de cambiar su orden de evaluación.

Siga las directrices siguientes cuando vaya a crear entradas para una regla:

- La lista debe contener, como mínimo, una declaración de permiso; de lo contrario, se denegará todo el tráfico.
- La última entrada debe ser un permiso para todo o una denegación para todo.
- En la misma regla no se pueden mezclar entradas estándar y entradas ampliadas.
- Una misma regla no puede contener entradas duplicadas.

## Clonar

Haga clic en este botón para utilizar la entrada seleccionada como plantilla de una nueva entrada. Esta función le permite ahorrar tiempo y minimizar errores. Por ejemplo, si desea crear varias entradas de reglas ampliadas con el mismo origen y destino pero protocolos o puertos diferentes, cree la primera entrada mediante el botón **Agregar**. Una vez creada la primera entrada, podrá copiarla mediante el botón **Clonar** y cambiar el campo de protocolo o el de puerto para crear una entrada nueva.

## Asociación de interfaces

Haga clic en el botón **Asociar** para aplicar la regla a una interfaz.



### Nota

El botón **Asociar** sólo estará activado si se está agregando una regla a partir de la ventana Reglas de acceso.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
Agregar o editar una entrada de regla.	Haga clic en <b>Agregar</b> y cree la entrada en la ventana que aparece. O haga clic en <b>Editar</b> y cambie la entrada en la ventana mostrada.
Agregar una regla utilizando como plantilla una entrada ya existente.	<p>Seleccione la entrada que desee utilizar como plantilla y haga clic en <b>Clonar</b>. A continuación, cree la entrada en el cuadro de diálogo que aparece.</p> <p>El cuadro de diálogo mostrará el contenido de la entrada seleccionada para que pueda editarla y crear una entrada nueva.</p>
Reordenar las entradas de una regla para asegurarse de que el router evalúa determinadas entradas.	Seleccione la entrada de la regla y haga clic en el botón <b>Desplazar hacia arriba</b> o <b>Desplazar hacia abajo</b> para mover la entrada hasta el punto que desee.
Asociar una regla con una interfaz.	<p>Haga clic en <b>Asociar</b> y seleccione la interfaz y la dirección en la ventana Asociar con una interfaz.</p> <p>Si el botón <b>Asociar</b> no está activado, puede asociar la regla con una interfaz haciendo doble clic en la interfaz en la ventana Interfaces y conexiones y utilizando la ficha Asociar.</p>
Eliminar una entrada de regla.	Seleccione la entrada de la regla y haga clic en <b>Eliminar</b> . A continuación, confirme la eliminación en la ventana Alerta que aparezca.
Más detalles acerca de las reglas.	<p>Explore los recursos disponibles en Cisco.com. El enlace siguiente contiene información acerca de las listas de acceso de IP:</p> <p><a href="http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml">http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml</a></p>
Lo que deseo hacer no se describe aquí.	El enlace siguiente contiene procedimientos que se pueden consultar: <a href="#">Procedimientos útiles para las reglas de acceso y firewalls</a>

## Asociar con una interfaz

Esta ventana se puede utilizar para asociar una regla que se ha creado desde la ventana Reglas de acceso con una interfaz y para especificar si dicha regla se aplica a tráfico saliente o entrante.

### Seleccionar una interfaz

Seleccione la interfaz a la que desea aplicar esta regla.


### Especificar una dirección

Si desea que el router compruebe los paquetes que entran en la interfaz, haga clic en **Entrante**. El router buscará una coincidencia con la regla antes de enrutar el paquete; el router acepta o abandona dicho paquete en función de si la regla indica “permitir” o “denegar”. Si desea que el router envíe el paquete a la interfaz saliente antes de compararlo con las entradas de la regla de acceso, haga clic en **Saliente**.

### Si hay otra regla ya asociada con la interfaz

Si aparece un cuadro informativo que indica que existe otra regla de acceso asociada con la interfaz y dirección especificadas, puede cancelar la operación; o bien, puede continuar anexando las entradas de la regla a la regla que ya se aplica a la interfaz o anulando la asociación de la regla con la interfaz y asociando la regla nueva.

## ¿Qué desea hacer?

Si desea:	Haga lo siguiente:
<p>Cancelar la operación y conservar la asociación entre la interfaz y la regla existente.</p>	<p>Haga clic en <b>No</b>. Se conserva la asociación entre la regla existente y la interfaz y se guarda la regla creada en la ventana Agregar una regla.</p> <p>Puede examinar la regla existente y la nueva y decidir si desea sustituir la regla existente o combinar las entradas de la regla nueva a la existente.</p>
<p>Continuar y combinar las entradas de la regla creada con las entradas de la regla existente.</p>	<p>Haga clic en <b>Sí</b>. A continuación, cuando aparezca la ventana que le solicita si desea combinar o sustituir la regla existente, haga clic en <b>Combinar</b>.</p> <p>Las entradas creadas para la nueva regla se anexan tras la última entrada de la regla existente.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p><b>Nota</b> Si la regla que desea combinar no es compatible con la regla existente, sólo podrá sustituir la regla existente.</p> </div>
<p>Continuar y sustituir la regla existente con la regla que ha creado.</p>	<p>Haga clic en <b>Sí</b>. A continuación, cuando aparezca la ventana que le solicita si desea combinar o sustituir la regla existente, haga clic en <b>Sustituir</b>.</p> <p>La regla que está sustituyendo no se borra, Fue anulada su asociación con la interfaz y la dirección.</p>

## Agregar una entrada de regla estándar

Una entrada de regla estándar permite autorizar o denegar el tráfico que proviene de un origen especificado. El origen puede ser una red o un host de una red específica. En esta ventana puede crear una entrada de regla única, aunque puede regresar a la ventana para crear entradas adicionales para la regla, si es preciso.



**Nota**

Todo tráfico que no cumpla los criterios de alguna de las entradas de regla que cree, será denegado implícitamente. Para asegurarse de que se permite el tráfico que no desea denegar, deberá anexar entradas de permiso explícitas a la regla que está configurando.

**Acción**

Seleccione la acción que desee que el router ejecute cuando un paquete cumpla los criterios de la entrada de la regla. Las opciones son **“Permit”** y **“Deny”**. El funcionamiento de dichas opciones depende del tipo de regla en la que se utilizan. En Cisco SDM, las entradas de regla estándar se pueden utilizar en reglas de acceso, en reglas NAT y en las listas de acceso asociadas con un [mapa de ruta](#). Haga clic en [Significados de las palabras clave “permit” y “deny”](#) para obtener más información acerca de las acciones Permitir y Denegar en el contexto de un tipo de regla específico.

**Red/host de origen**

Criterios de dirección IP de origen que el tráfico debe cumplir. Los campos de esta área de la ventana cambian en función del valor indicado en el campo Tipo.

**Tipo**

Seleccione uno de los siguientes:

- Una red. Seleccione esta opción si desea que la acción se aplique a todas las direcciones IP de una red.
- Un nombre de host o dirección IP. Seleccione esta opción si desea que la acción se aplique a un host específico o una dirección IP.
- Cualquier dirección IP. Seleccione esta opción si desea que la acción se aplique a cualquier dirección IP.

**Dirección IP**

Si ha seleccionado **Una Red o Un nombre de host o dirección IP**, escriba la dirección IP en este campo. Si la dirección que escribe es una dirección de red, especifique una [máscara comodín](#) para indicar las partes de la dirección de la red que deben coincidir.

**Máscara**

Si ha seleccionado **Una Red o Un nombre de host o dirección IP**, seleccione la máscara comodín en la lista o bien especifique una máscara comodín personalizada. Un 0 binario en una máscara inversa significa que el bit correspondiente de la dirección IP de un paquete debe coincidir exactamente. Un 1 binario en una máscara comodín significa que no es preciso que el bit correspondiente de la dirección IP de un paquete coincida.

**Nombre de host/IP**

Si ha seleccionado **Un nombre de host o dirección IP** en el campo Tipo, especifique el nombre o la dirección IP del host. Si introduce un nombre de host, se debe configurar el router para que use un servidor DNS.

**Descripción**

En este campo puede especificar una breve descripción de la entrada. Dicha descripción debe tener menos de 100 caracteres.

**Coincidencias de registro con esta entrada**

Si ha especificado syslog en Propiedades del sistema, puede marcar esta casilla; las coincidencias quedarán registradas en el registro del sistema.

**Agregar una entrada de regla ampliada**

Una entrada de regla ampliada permite autorizar o denegar tráfico basándose en su origen y destino y en el protocolo y el servicio especificados en el paquete.

**Nota**


---

Todo tráfico que no cumpla los criterios de alguna de las entradas de regla que cree, será denegado implícitamente. Para asegurarse de que se permite el tráfico que no desea denegar, deberá anexar entradas de permiso explícitas a la regla que está configurando.

---

## Acción

Seleccione la acción que desee que el router ejecute cuando un paquete cumpla los criterios de la entrada de la regla. Las opciones son **“Permit”** y **“Deny”**. Si está creando una entrada para una regla IPsec, las opciones son **Proteger el tráfico** y **No proteger el tráfico**.

El funcionamiento de dichas opciones depende del tipo de regla en la que se utilizan. En Cisco SDM, las entradas de regla ampliadas se pueden utilizar en reglas de acceso, reglas NAT, reglas IPsec y en las listas de acceso asociadas con un [mapa de ruta](#). Haga clic en [Significados de las palabras clave “permit” y “deny”](#) para obtener más información acerca de la acción de Permitir y de Denegar en el contexto de un tipo de regla específico.

## Red/host de origen

Criterios de dirección IP de origen que el tráfico debe cumplir. Los campos de esta área de la ventana cambian en función del valor indicado en el campo Tipo.

### Tipo

Seleccione uno de los siguientes:

- Una dirección IP específica. Puede ser la dirección de una red o bien la dirección de un host específico.
- Un nombre de host.
- Cualquier dirección IP.

### Dirección IP

Si ha seleccionado **Una dirección IP específica**, escriba la **Dirección IP** en este campo. Si la dirección que escribe es una dirección de red, especifique una [máscara comodín](#) para indicar las partes de la dirección de la red que deben coincidir.

**Máscara**

Si ha seleccionado **Una dirección IP específica**, seleccione la máscara comodín en la lista o especifique una máscara comodín personalizada. Un 0 binario en una máscara inversa significa que el bit correspondiente de la dirección IP de un paquete debe coincidir exactamente. Un 1 binario en una máscara inversa significa que no es preciso que el bit correspondiente de la dirección IP de un paquete coincida.

**Nombre de host**

Si ha seleccionado **Un nombre de host** en el campo Tipo, especifique el nombre del host.

**Red/host de destino**

Criterios de dirección IP de origen que el tráfico debe cumplir. Los campos de esta área de la ventana cambian en función del valor indicado en el campo Tipo.

**Tipo**

Seleccione uno de los siguientes:

- Una dirección IP específica. Puede ser la dirección de una red o bien la dirección de un host específico.
- Un nombre de host.
- Cualquier dirección IP.

**Máscara**

Si ha seleccionado **Una dirección IP específica**, seleccione la máscara comodín en la lista o especifique una máscara comodín personalizada. Un 0 binario en una máscara inversa significa que el bit correspondiente de la dirección IP de un paquete debe coincidir exactamente. Un 1 binario en una máscara inversa significa que no es preciso que el bit correspondiente de la dirección IP de un paquete coincida.

**Nombre de host**

Si ha seleccionado **Un nombre de host** en el campo Tipo, especifique el nombre del host.

## Descripción

En este campo puede especificar una breve descripción de la entrada. Dicha descripción debe tener menos de 100 caracteres.

## Protocolo y servicio

Seleccione el protocolo y el servicio, si es pertinente, a los que desea que se aplique la entrada. La información suministrada varía en función del protocolo. Haga clic en el protocolo para ver qué información debe suministrar.

### Puerto de origen

Disponible cuando se selecciona TCP o UDP. Si configura este campo, el router filtrará según el puerto de origen del paquete. En el caso de una conexión TCP, en raras ocasiones es preciso especificar un valor de puerto de origen. Si no está seguro de si necesita utilizar este campo, déjelo con el valor = **any**.

### Puerto de destino

Disponible cuando se selecciona TCP o UDP. Si configura este campo, el router filtrará en el puerto de destino de un paquete.

Si selecciona este protocolo:	Puede especificar lo siguiente en los campos Puerto de origen y Puerto de destino:
TCP o UDP	<p>Puede especificar el puerto de origen o de destino por nombre o número. Si no recuerda el nombre o el número, haga clic en el botón ... y seleccione el valor que desee en la ventana Servicio. Este campo acepta números de protocolo del 0 al 65535.</p> <ul style="list-style-type: none"> <li>• =. La entrada de la regla se aplica al valor especificado en el campo situado a la derecha.</li> <li>• !=. La entrada de la regla se aplica a cualquier valor, salvo al que se ha especificado en el campo situado a la derecha.</li> <li>• &lt;. La entrada de la regla se aplica a todos los números de puerto inferiores al número especificado.</li> <li>• &gt;. La entrada de la regla se aplica a todos los números de puerto superiores al número especificado.</li> <li>• intervalo. La entrada se aplica al intervalo de números de puerto especificado en los campos situados a la derecha.</li> </ul>
ICMP	<p>Puede especificar <b>cualquier</b> tipo de ICMP o bien especificar un tipo por nombre o por número. Si no recuerda el nombre o el número, haga clic en el botón ... y seleccione el valor que desee. Este campo acepta números de protocolo del 0 al 255.</p>
IP	<p>Puede especificar <b>cualquier</b> protocolo IP o bien especificar un protocolo por nombre o por número. Si no recuerda el nombre o el número, haga clic en el botón ... y seleccione el valor que desee. Este campo acepta números de protocolo del 0 al 255.</p>

Consulte [Servicios y puertos](#) para ver una tabla que contiene los nombres y números de puerto disponibles en Cisco SDM.

### Coincidencias de registro con esta entrada

Si se ha configurado el registro para mensajes de firewall, se puede seleccionar esta casilla, y las correspondencias serán grabadas en el archivo de registro que se envía al servidor syslog. Si desea obtener más información, consulte este enlace: [Registro de firewall](#).

## Seleccionar una regla

Utilice esta ventana para seleccionar la regla que va a utilizar.

### Categoría de regla

Seleccione la categoría de la regla en la que desee efectuar la selección. Las reglas de la categoría que seleccione aparecerán en el cuadro situado bajo la lista. Si no aparece ninguna regla en el cuadro, significa que no se ha definido ninguna regla para esa categoría.

### Nombre/Número

El nombre o número de la regla.

### Usado por

Cómo se utiliza la regla. Por ejemplo, si la regla se ha asociado a una interfaz, el nombre de dicha interfaz. Si se está utilizando la regla en una política IPsec, el nombre de dicha política. O bien, si NAT ha utilizado la regla, esta columna contendrá el valor NAT.

### Descripción

Descripción de la regla.

### Vista previa

Esta área de la pantalla muestra las entradas de la regla seleccionada.

### Acción

Puede ser **Permitir** o **Denegar**. Consulte [Significados de las palabras clave “permit” y “deny”](#) para obtener más información acerca de la acción de Permitir y de Denegar dentro del contexto de un tipo específico de regla.

### Origen

Criterios de dirección IP de origen que el tráfico debe cumplir. Esta columna puede contener los elementos siguientes:

- Una dirección IP y una **máscara comodín**. La dirección IP especifica una red y la máscara inversa especifica la parte de la dirección IP de la regla que la dirección IP del paquete debe cumplir.
- La palabra clave **any**. “Any” indica que la dirección IP de origen puede ser cualquier dirección IP.
- Un nombre de host.

### Destino

En el caso de las reglas ampliadas, los criterios de la dirección IP de destino que el tráfico debe cumplir. La dirección puede ser para una red o un host específico. Esta columna puede contener los elementos siguientes:

- Una dirección IP y una **máscara comodín**. La dirección IP especifica una red y la máscara inversa especifica la parte de la dirección IP de la regla que la dirección IP del paquete debe cumplir.
- La palabra clave **any**. “Any” indica que la dirección IP de origen puede ser cualquier dirección IP.
- Un nombre de host.

### Servicio

En el caso de las **reglas ampliadas**, el servicio especifica el tipo de tráfico que deben contener los paquetes que cumplen la regla. Esto se ve mostrando el servicio como, por ejemplo, echo-reply, seguido por un protocolo como ICMP. Una regla que permita o deniegue varios servicios entre los mismos puntos finales deberá contener una entrada para cada servicio.





# CAPÍTULO 30

## Asignación puerto a aplicación

---

La Asignación puerto a aplicación (PAM) permite personalizar los números de puertos TCP y UDP para los servicios y aplicaciones de la red. El PAM utiliza esta información para admitir entornos de red que ejecuten servicios utilizando puertos que no sean los puertos registrados o conocidos asociados con una aplicación.

La información de PAM mantiene activa los servicios admitidos por el Control de acceso basado en contexto (CBAC) para que se ejecuten en puertos no estándar. Previamente, el CBAC se limitaba a inspeccionar el tráfico utilizando sólo los puertos conocidos o registrados asociados con una aplicación. Ahora, PAM permite que los administradores de redes personalicen el control de acceso a la red para aplicaciones y servicios específicos.

## Asignaciones puerto a aplicación

Esta ventana muestra las asignaciones puerto a aplicación configuradas en el router y permite que se agreguen, editen y eliminen entradas [PAM](#). Cada fila de la ventana muestra una entrada PAM, las que se encuentran agrupadas según tipo.

### Botones Agregar, Editar y Eliminar

Utilice estos botones para crear, editar o eliminar las entradas PAM. Si se hace clic en el botón **Agregar** es posible crear entradas que asignan los números de puerto a los nombres de protocolo. Si se hace clic en el botón **Editar** es posible hacer cambios en las entradas definidas por el usuario. Las entradas con el valor *Definido por sistema* en la columna Tipo de protocolo no pueden editarse ni eliminarse.

## Columna Protocolo de aplicación

Esta columna contiene el nombre del protocolo de aplicación, y los nombres de los tipos de protocolos. Por ejemplo, las entradas FTP y TFTP se encuentran bajo el tipo de protocolo Transferencia de archivos.

## Columna Tipo de puerto

Esta lista aparece si el router está ejecutando una imagen de Cisco IOS que permita especificar si esta entrada de asignación de puerto se aplica al tráfico TCP o al UDP.

## Columna Puerto

Esta columna contiene el número del puerto. Por ejemplo, la entrada definida por el usuario para http tendría el número de puerto 80 en esta columna. Una entrada definida por el usuario para http podría tener el número de puerto 8080 u otro número personalizado de esta columna.

## Columna Tipo de protocolo

Una fila de esta columna muestra uno de los siguientes valores:

- **Definido por usuario:** la entrada contiene una asignación no estándar entre un protocolo y un número de protocolo. La entrada podría asociarse a una dirección IP del host identificado por la lista de control de acceso (ACL), cuyo número aparece en la columna Lista de acceso.
- **Definido por sistema:** la entrada contiene una asignación estándar y registrada entre el protocolo y el número del protocolo, como *tftp 69*, o *sntp 25*. Las entradas definidas por sistema no pueden editarse ni eliminarse. Las entradas definidas por sistema no contienen valor en la columna Lista de acceso porque se aplican a todos los hosts de la red.

## Columna Lista de acceso

Una entrada PAM se aplica a un solo host, definido por medio de una ACL estándar. Esta columna muestra el número de la ACL utilizada para identificar al host al que se aplica la entrada PAM. Si desea visualizar la ACL que identifica al host, vaya a **Tareas adicionales > Editor de ACL > Reglas de acceso**. Luego, haga clic en el número de la ACL que se observó en esta ventana.

## Columna Descripción

Si se ha creado una columna de la entrada PAM, la descripción se muestra en esta columna.

## Agregar o editar entrada de asignación de puerto

Es posible agregar y editar las entradas de asignación de puertos para los protocolos estándar o personalizados.

### Campo Protocolo

Si se está agregando una entrada, especifique el protocolo haciendo clic en el botón (...) de la lista, ubicado a la derecha y seleccione un protocolo definido por sistema, o especificando el nombre de un protocolo personalizado. No es posible especificar nombres de protocolos personalizados para los que ya existe una asignación de puertos.

Si se está editando una entrada, se desactiva el campo protocolo. Si se necesita cambiar el protocolo, elimine la entrada PAM y vuelva a crearla usando la información de protocolo que necesite.

### Campo Descripción

Este campo aparece si se está ejecutando una imagen de Cisco IOS que permita especificar si esta entrada de asignación de puerto se aplica al tráfico TCP o al UDP. En forma opcional, especifique una descripción de la entrada de asignación de puertos. Las descripciones son útiles cuando se está agregando entradas para protocolos personalizados o aplicaciones especiales. Por ejemplo, si se creó una entrada para una aplicación de bases de datos personalizada llamada “orville” ejecutándose en el host sf-5, se podría especificar “orville-sf-5”.

### Lista Tipo de puerto

Esta lista aparece si el router está ejecutando una imagen de Cisco IOS que permita especificar si esta entrada de asignación de puerto se aplica al tráfico TCP o al UDP. Seleccione **TCP** o bien **UDP**. Es TCP por defecto.

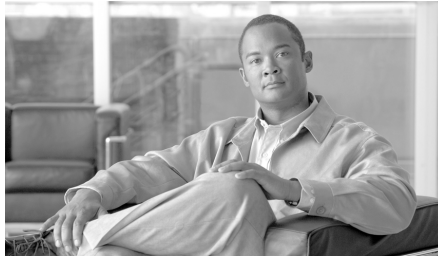
## Campo Número de puerto

Especifique el número de puerto que desea asignar al protocolo que especificó. Si el router está ejecutando una imagen de Cisco IOS que permite especificar si esta entrada de asignación de puertos al tráfico TCP o UDP, es posible especificar múltiples números de puertos separados por comas, o intervalos de números de puertos indicados con un guión. Por ejemplo, se podría especificar tres números de puertos no contiguos, como 310, 313, 318; o se podría introducir el intervalo 415-419.

Si el router no ejecuta una imagen de Cisco IOS que permita especificar si esta entrada de asignación de puerto se aplica al tráfico TCP o al UDP, puede especificar un número de puerto individual.

## Campo Servicio del host

Especifique la dirección IP del host al que se aplicará esta asignación de puertos. Si se necesita la misma asignación para otro host, debe crear una entrada PAM diferente para ese nuevo host.



# CAPÍTULO 31

## Firewall de política basado en zonas

---

El firewall de política basado en zonas (también conocido como “firewall de política de zonas” o “ZPF”) cambia el firewall del modelo basado en la interfaz anterior a un modelo de configuración basada en zonas más flexible y de mejor comprensión. Las interfaces se asignan a las zonas y se aplica una política de inspección al tráfico que se produce entre las zonas. Las políticas entre zonas ofrecen flexibilidad y granularidad considerable para que se puedan aplicar distintas políticas de inspección a grupos de host múltiples conectados a la misma interfaz de router.

Las políticas de firewall se configuran con el Lenguaje de política de clasificación común de Cisco (**C3PL**), que utiliza una estructura jerárquica para definir la inspección de protocolos de red y los grupos de host en que se aplicará la inspección.

Para obtener una descripción detallada de la forma en que se puede implementar el firewall de política basado en zonas, lea la *Guía de diseño de firewall de política basado en zonas* disponible en [cisco.com](http://www.cisco.com) en **Support (Soporte) > Product Support (Soporte de productos) > Cisco IOS Software (Software Cisco IOS) > Cisco IOS Software Releases 12.4 Mainline (Línea principal de software Cisco IOS versión 12.4) > Configure (Configurar) > Feature Guides (Guías de funciones)** y haga clic en *Zone-Based Policy Firewall Design Guide (Guía de diseño de firewall de política basado en zonas)*. Este documento también está disponible en el siguiente enlace:

[http://www.cisco.com/en/US/products/ps6350/products\\_feature\\_guide09186a008072c6e3.html](http://www.cisco.com/en/US/products/ps6350/products_feature_guide09186a008072c6e3.html)

## Orden de tareas de configuración

Se puede seguir el siguiente orden de tareas para configurar el firewall de política basado en zonas:

1. Definir las zonas.
2. Definir los pares de zonas.
3. Definir los mapas de clase que describen el tráfico que se debe aplicar a la política cuando cruza un par de zonas.
4. Definir los mapas de política para aplicar acciones al tráfico del mapa de clase.
5. Aplicar mapas de política a los pares de zonas.
6. Asignar interfaces a las zonas.

La secuencia de tareas no es importante, pero algunos eventos deben realizarse en orden. Por ejemplo, debe configurar un mapa de clase antes de asignarlo a un mapa de política. De manera similar, no puede asignar un mapa de política a un par de zonas hasta que haya configurado la política. Si trata de realizar una tarea basada en otra parte de la configuración que no ha configurado, SDM no permite realizar dicha acción.

## Ventana de zona

Una zona, o [zona de seguridad](#), es un grupo de interfaces en las que se puede aplicar una política de seguridad. Las interfaces de una zona deben compartir funciones o características comunes. Por ejemplo, dos interfaces que se conectan a la LAN local podrían colocarse en una zona de seguridad y las interfaces conectadas a Internet podrían colocarse en otra zona de seguridad.

Para que el tráfico fluya entre todas las interfaces de un router, todas las interfaces deben ser miembro de una zona de seguridad u otra. No es necesario que todas las interfaces de router sean miembros de zonas de seguridad.

Las reglas generales de la política basada en zonas describen las reglas que rigen el comportamiento de la interfaz y el flujo de tráfico entre las interfaces que son miembros de la zona.

Esta ventana muestra el nombre de cada zona de seguridad, las interfaces que contiene y cualquier par de zonas asociado del que sea miembro la zona. Una zona puede ser miembro de múltiples pares de zonas.

Haga clic en **Agregar** para crear una zona nueva.

Haga clic en **Editar** para elegir interfaces diferentes para una zona existente.

Haga clic en **Eliminar** para eliminar una zona. No se puede eliminar una zona que es miembro de un par de zonas.

## Agregar o editar una zona

Para agregar una nueva zona, también denominada [zona de seguridad](#), especifique un nombre de zona y elija las interfaces que se incluirán en ésta. La lista de interfaces muestra los nombres de interfaces disponibles. Dado que las interfaces físicas sólo pueden colocarse en una zona, no aparecen en la lista si ya se colocaron en una zona. Las interfaces virtuales, como, por ejemplo, las interfaces de marcación o interfaces de plantilla virtual pueden colocarse en zonas múltiples y siempre aparecerán en la lista.



### Nota

- El tráfico que fluye desde o hacia esta interfaz se rige por el mapa de política asociado con la zona.
- La interfaz que asocie con esta zona puede utilizarse para un [VPN](#) sitio a sitio, [DMVPN](#), [Easy VPN](#), [SSL VPN](#) u otro tipo de conexión cuyo tráfico podría bloquearse con un firewall. Cuando asocia una interfaz con una zona en este cuadro de diálogo, SDM no crea ninguna [ACL](#) de paso que permita dicho tráfico. Puede configurar el paso necesario para el mapa de política de dos formas.
  - Vaya a **Configurar > Firewall y ACL > Editar política de firewall > Regla para nuevo tráfico**. En el cuadro de diálogo que aparece, proporcione la información de dirección IP de origen y destino, además del tipo de tráfico que se debe permitir que pase por el firewall. En el campo Acción, seleccione **Permitir ACL**.
  - Vaya a **Configurar > C3PL > Mapa de política > Inspección de protocolo**. Proporcione un mapa de política de inspección de protocolo que permitirá que el tráfico necesario pase por el firewall.

Después de crear una zona, puede cambiar las interfaces asociadas con ésta, pero no puede cambiar el nombre de la zona.

## Reglas generales de la política basada en zonas

La suscripción de interfaces de red de router en zonas está sujeta a varias reglas que rigen el comportamiento de la interfaz al igual que el tráfico entre las interfaces que son miembros de la zona.

- Una zona debe configurarse antes de que se le puedan asignar las interfaces.
- Una interfaz se puede asignar a una sola zona de seguridad.
- Todo el tráfico desde y hacia una interfaz determinada se encuentra bloqueado implícitamente cuando la interfaz se asigna a una zona, con excepción del tráfico desde y hacia otras interfaces de la misma zona y del tráfico de cualquier interfaz del router.
- Se permite implícitamente que el tráfico fluya por defecto entre las interfaces que son miembro de la misma zona.
- Para permitir el tráfico desde y hacia una interfaz que pertenece a la zona, se debe configurar una política que permita o inspeccione el tráfico entre esa zona y cualquier otra.
- La zona automática es la única excepción de la política de denegación total por defecto. Se permite todo el tráfico dirigido a cualquier interfaz de router hasta que éste se deniega explícitamente.
- El tráfico no puede fluir entre una interfaz que es miembro de la zona y cualquier interfaz que no lo es.
- Las acciones de aprobación, inspección y rechazo sólo se pueden aplicar entre dos zonas.
- Es posible que las interfaces que no se asignaron a una función de zona como puertos de router clásicos todavía utilicen la inspección completa de estado clásica/configuración CBAC.
- Si se requiere que una interfaz en el cuadro no forme parte de la política de zonas/firewall, aún podría ser necesario colocar esa interfaz en una zona y configurar una política de aprobación total (un tipo de política de prueba) entre esa zona y cualquier otra hacia la que se desee el flujo de tráfico.



- De lo anterior se desprende que, si el tráfico debe fluir entre todas las interfaces de un router, todas las interfaces deben formar parte del modelo de zonas (cada interfaz debe ser miembro de una zona u otra).
- La única excepción del enfoque por defecto de la denegación anterior es el tráfico desde y hacia el router que se permitirá por defecto. Se puede configurar una política explícita para restringir dicho tráfico.

Este conjunto de reglas se obtuvo de la *Guía de diseño de firewall de política basado en zonas* que se encuentra disponible en el siguiente enlace:

[http://www.cisco.com/en/US/products/ps6350/products\\_feature\\_guide09186a008072c6e3.html](http://www.cisco.com/en/US/products/ps6350/products_feature_guide09186a008072c6e3.html)

## Pares de zonas

Un par de zonas le permite especificar una política de firewall unidireccional entre dos zonas de seguridad. La dirección del tráfico se especifica con una [zona de seguridad](#) de origen y destino. La misma zona no se puede definir como origen y destino.

Si desea que el tráfico fluya en ambas direcciones entre dos zonas, debe crear un par de zonas para cada dirección. Si desea que el tráfico fluya libremente entre todas las interfaces, cada interfaz debe configurarse en una zona.

La siguiente tabla muestra un ejemplo de cuatro pares de zonas.

Par de zonas	Origen	Destino	Política
LAN-salida	zona-VLAN1	zona-FE1	mapa política inspección-a
LAN-entrada	zona-FE1	zona-VLAN1	mapa política inspección-b
Reserva-salida	Automático	zona-BR10	mapa política inspección-c
Reserva-entrada	zona-BR10	automático	mapa política inspección-c

LAN-salida y LAN-entrada son pares de zonas configurados para el tráfico que fluye entre la interfaz LAN, VLAN1 y FastEthernet 1. Cada par de zonas se controla mediante una política de zona separada. Reserva-salida y Reserva-entrada se configuran para el tráfico que genera el router. La misma política controla el tráfico enviado desde zona-BR10 como tráfico enviado por el router, representado por la zona automática.

Haga clic en **Agregar** para crear un par de zonas.

Haga clic en **Editar** para cambiar la política asociada con un par de zonas.

Haga clic en **Eliminar** para eliminar un par de zonas.

## Agregar o editar un par de zonas

Para configurar un nuevo par de zonas, asigne un nombre al par de zonas, una zona de origen a partir de la cual se originará el tráfico, una zona de destino a la que se enviará el tráfico y la política que determinará el tráfico que se podrá enviar entre las zonas. La lista de zona de origen y zona de destino contiene las zonas configuradas en el router y la zona automática. La zona automática se puede usar cuando configure pares de zonas para el tráfico que se origina en el router o se destina a éste, como, por ejemplo, un par de zonas configurado para el tráfico SNMP. La lista de políticas contiene el nombre de cada [mapa de política](#) configurado en el router.

Si está editando un par de zonas, puede cambiar el mapa de política, pero no puede cambiar el nombre ni las zonas de origen o destino.

## Agregar una zona

Puede configurar una interfaz como miembro de una [zona de seguridad](#) desde la ficha Interfaces and Connections Association (Asociación de interfaces y conexiones). La zona que agregue incluirá la interfaz que esté editando como miembro de zona.



### Nota

- El tráfico que fluye desde o hacia esta interfaz se rige por el mapa de política asociado con la zona.
- Una interfaz que asocie con esta zona puede utilizarse para un [VPN](#) sitio a sitio, [DMVPN](#), [Easy VPN](#), [SSL VPN](#) u otro tipo de conexión cuyo tráfico podría bloquearse con un firewall. Cuando asocia una interfaz con una zona en este cuadro de diálogo, SDM no crea ninguna [ACL](#) de paso que permita dicho tráfico. Puede configurar el paso necesario para el mapa de política de dos formas.

- Vaya a **Configurar > Firewall y ACL > Editar política de firewall > Regla para nuevo tráfico**. En el cuadro de diálogo que aparece, proporcione la información de dirección IP de origen y destino, además del tipo de tráfico que se debe permitir que pase por el firewall. En el campo Acción, seleccione **Permitir ACL**.
  - Vaya a **Configurar > C3PL > Mapa de política > Inspección de protocolo**. Proporcione un mapa de política de inspección de protocolo que permitirá que el tráfico necesario pase por el firewall.
- 

## Nombre de zona

Especifique el nombre de la zona que desea agregar.

## Seleccionar una zona

Si se ha configurado una [zona de seguridad](#) en el router, puede agregar la interfaz que esté configurando como un miembro de esa zona.

### Seleccionar una zona para la interfaz

Seleccione la zona en que desea incluir la interfaz y haga clic en **Aceptar**.





## CAPÍTULO **32**

# Authentication, Authorization and Accounting (AAA)

---

“Cisco IOS Authentication, Authorization, and Accounting” (AAA) es una estructura de arquitectura para configurar un conjunto de tres funciones de seguridad independientes en forma congruente. AAA entrega una forma modular de realizar los servicios de autenticación, autorización y contabilidad.

AAA de Cisco IOS ofrece las ventajas siguientes:

- Mayor control y flexibilidad
- Escalabilidad
- Métodos de autenticación estandarizados. Cisco SDM permite configurar los métodos de autenticación Remote Authentication Dialing User Service (RADIUS) y Terminal Access Controller Access Control System Plus (TACACS+).

# Ventana principal de AAA

Esta ventana proporciona una vista de resumen de la configuración de AAA en el router. Para ver información más detallada o editar dicha configuración, haga clic en el nodo apropiado del árbol de AAA.

## Activar/Desactivar AAA

La aplicación AAA está activada por defecto. Si hace clic en **Desactivar**, Cisco SDM muestra un mensaje indicando que se realizarán cambios en la configuración para garantizar el acceso al router. Si se desactiva AAA, el usuario no podrá configurar el router como servidor Easy VPN ni asociar las cuentas de usuario a vistas de interfaz de línea de comandos (CLI).

## Grupos y servidores AAA

Este campo de sólo lectura muestra un recuento de los servidores y grupos de servidores de AAA. El router transmite las solicitudes de autenticación, autorización y cuentas a los servidores de AAA, los cuales se organizan en grupos para brindar al router la posibilidad de contactar servidores alternativos si el primer servidor contactado no está disponible.

## Políticas de autenticación

Este campo de sólo lectura muestra una lista de las políticas de autenticación configuradas, las cuales definen cómo se identifican los usuarios. Para editar dichas políticas, haga clic en el subnodo **Conexión** de **Políticas de autenticación** del árbol AAA.

## Políticas de autorización

Este campo de sólo lectura muestra una lista de las políticas de autorización configuradas, **las cuales definen los métodos que se utilizan para autorizar o denegar la conexión de un usuario**. Para editar dichas políticas, haga clic en **Políticas de autorización** del árbol AAA.

Para editar las políticas de autorización (Autorización de red y autorización Exec), haga clic en los subnodos **Exec** y **Red** respectivamente, en el nodo **Políticas de autorización** del árbol Reglas de AAA.

# Grupos y servidores AAA

Esta ventana ofrece una descripción de los servidores de AAA y grupos de servidores de AAA.

## Ventana Servidores AAA

Esta ventana permite ver una instantánea de la información acerca de los servidores de AAA que el router puede utilizar según la configuración correspondiente. Para cada servidor se muestra la dirección IP, el tipo de servidor y otros parámetros.

### Configuración global

Haga clic en este botón para establecer la configuración global de los servidores TACACS+ y RADIUS. En la ventana Editar configuración global, puede especificar el tiempo durante el cual se intentará contactar con el servidor AAA antes de pasar al siguiente servidor, la clave que se utilizará al contactar con los servidores TACACS+ o RADIUS y la interfaz en la cual se recibirán los paquetes TACACS+ o RADIUS. Esta configuración se aplicará a todos los servidores para los cuales no se haya establecido una configuración específica de servidor.

### Agregar...

Haga clic en este botón para agregar un servidor TACACS+ o RADIUS a la lista.

### Editar...

Haga clic en este botón para editar la información relativa al servidor AAA.

### Eliminar...

Haga clic en este botón para eliminar la información relativa al servidor AAA seleccionado.

### IP del servidor

La dirección IP del servidor AAA.

**Tipo**

El tipo de servidor, TACACS+ o RADIUS.

**Parámetros**

Esta columna muestra una lista del límite de tiempo, clave y otros parámetros de cada servidor.

**Agregar o editar un servidor TACACS+**

Agregue o modifique información acerca de un servidor TACACS+ en esta ventana.

**Host o IP de servidor**

Especifique el nombre de host o la dirección IP del servidor. Si el router no se ha configurado para utilizar un servidor DNS (Domain Name Service), especifique una dirección IP.

**Única conexión al servidor**

Marque esta casilla si desea que el router mantenga una única conexión abierta con el servidor TACACS+, en lugar de abrir y cerrar una conexión TCP cada vez que se comunica con el servidor. Una única conexión abierta resulta más eficaz porque permite al servidor TACACS+ procesar un mayor número de operaciones TACACS+.

**Nota**


---

Esta opción sólo se admite si el servidor TACACS+ ejecuta CiscoSecure versión 1.0.1 o posterior.

---



## Configuración específica de servidor

Marque esta casilla si desea anular la configuración global de los servidores de AAA e indicar un valor de tiempo límite específico de servidor y una clave de cifrado.

### Límite de tiempo (seg.)

Especifique los segundos durante los que el router intentará contactar con este servidor antes de pasar al siguiente servidor de la lista de grupo. Si no especifica ningún valor, el router utilizará el valor configurado en la ventana de configuración global de servidores de AAA.

### Configurar clave

Opcional. Especifique la clave que se utilizará para cifrar el tráfico entre el router y este servidor. Si no especifica ningún valor, el router utilizará el valor configurado en la ventana de configuración global de servidores de AAA.

### Clave nueva/Confirmar clave

Especifique la clave y, a continuación, especifíquela de nuevo para confirmarla.

## Agregar o editar un servidor RADIUS

Agregue o modifique información acerca de un servidor RADIUS en esta ventana.

### Host o IP de servidor

Especifique el nombre de host o la dirección IP del servidor. Si el router no se ha configurado para utilizar un servidor DNS (Domain Name Service), especifique una dirección IP.

### Puerto de autorización

Especifique el puerto del servidor que se utilizará para las solicitudes de autorización. El valor por defecto es 1645.

### Puerto de cuentas

Especifique el puerto del servidor que se utilizará para las solicitudes de cuentas. El valor por defecto es 1646.

**Límite de tiempo (seg.)**

Opcional. Especifique los segundos durante los que el router intentará contactar con este servidor antes de pasar al siguiente servidor de la lista de grupo. Si no especifica ningún valor, el router utilizará el valor configurado en la ventana de configuración global de servidores de AAA.

**Configurar clave**

Opcional. Especifique la clave que se utilizará para cifrar el tráfico entre el router y este servidor. Si no especifica ningún valor, el router utilizará el valor configurado en la ventana de configuración global de servidores de AAA.

**Clave nueva/Confirmar clave**

Especifique la clave y, a continuación, especifíquela de nuevo para confirmarla.

**Editar configuración global**

Esta ventana permite especificar los parámetros de comunicación que se aplicarán a todas las comunicaciones que se establezcan entre el router y los servidores de AAA. Todos los parámetros de comunicación que se configuren para un determinado router anularán los parámetros establecidos en esta ventana.

**Servidor TACACS+/Servidor RADIUS**

Haga clic en el botón correspondiente para especificar el tipo de servidor para el cual se dispone a configurar los parámetros globales. Si selecciona el primer tipo de servidor, los parámetros se aplicarán a todas las comunicaciones que se establezcan con los servidores TACACS+ que no tengan parámetros específicos de servidor definidos. Si selecciona el segundo tipo de servidor, los parámetros se aplicarán a todas las comunicaciones que se establezcan con los servidores RADIUS que no tengan parámetros específicos de servidor definidos.

**Límite de tiempo (seg.)**

Especifique el número de segundos que se esperará la respuesta del servidor RADIUS o TACACS+.

## Clave

Especifique la clave de cifrado para todas las comunicaciones que se establezcan entre el router y los servidores TACACS+ o RADIUS.

## Seleccione la interfaz de origen

Marque esta casilla si desea especificar una única interfaz en la que el router recibirá los paquetes TACACS+ o RADIUS.

### Interfaz

Seleccione la interfaz del router en la que éste recibirá los paquetes TACACS+ o RADIUS. Si la casilla **Seleccione la interfaz de origen** no está seleccionada, este campo se desactivará.

# Ventana Grupos de servidores AAA

Esta ventana muestra los grupos de servidores de AAA configurados en este router. Si no se ha configurado ningún servidor AAA, esta ventana estará vacía.

## Botones Agregar, Editar y Eliminar

Haga clic en el botón **Agregar** para crear un grupo de servidores RADIUS. Después de crear este grupo, el nombre y los miembros del grupo se muestran en esta ventana. Haga clic en **Editar** para modificar la información para el grupo de servidores resaltado. Haga clic en **Eliminar** para eliminar el grupo de servidores resaltado.

## Nombre del grupo

El nombre del grupo de servidores. Los nombres de grupo de servidores le permiten utilizar un nombre único para referirse a varios servidores.

## Tipo

El tipo de servidores del grupo seleccionado, ya sea TACACS+ o RADIUS.

## Miembros del grupo

Especifique los nombres de host o direcciones IP de los servidores de AAA de este grupo.

## Agregar o editar grupo de servidores AAA

Cree o modifique un grupo de servidores AAA en esta ventana.

### Nombre del grupo

Ingrese un nombre para el grupo.

### Tipo de servidor

Seleccione el tipo de servidor, RADIUS o TACACS+.

**Nota**

---

Este campo puede estar protegido y establecido en un tipo específico, de acuerdo con la configuración que está realizando.

---

## Seleccione los servidores que necesitan colocarse en este grupo de servidores AAA

Esta área enumera las direcciones IP de todos los servidores AAA configurados en el router del tipo seleccionado, junto con los puertos de Autorización y Cuentas utilizados. Marque la casilla **Seleccionar** junto a los servidores que desea agregar.

## Políticas de Autenticación y Autorización

Las ventanas correspondientes a las Políticas de Autenticación y Autorización resumen la información sobre la política de autenticación en el router.

### Tipo de autenticación

El tipo de política de autenticación.

## Número de políticas

El número de políticas de este tipo.

## Uso

La descripción del uso de estas políticas.

## Ventanas de Autenticación y Autorización

Las ventanas de Registro y Autorización de Exec y Red muestran las listas de métodos usadas para autenticar los registros, las solicitudes NAC y las solicitudes de autorización de redes y niveles de comando Exec. Es posible revisar y gestionar estas listas de métodos desde estas ventanas.

## Botones Agregar, Editar y Eliminar

Utilice estos botones para crear, editar y eliminar listas de métodos.

## Nombre de lista

Nombre de la lista de métodos. Una lista de métodos consiste en una lista secuencial que describe los métodos de autenticación solicitados con el fin de autenticar un usuario.

## Método 1

El método que el router probará en primer lugar. Si uno de los servidores en este método autentica al usuario (es decir envía una respuesta PASS), la autenticación se realizará de manera exitosa. Si el servidor entrega la respuesta FALLA, la autenticación fracasará. Si no hay respuesta de ninguno de los servidores al primer método, el router utilizará el método que sigue en la lista. Es posible ordenar los métodos en el momento de crear o editar una lista de métodos.

## Método 2,3 y 4

Métodos que el router utilizará en caso de que los servidores mencionados en el método 1 no respondan. Si existen menos de cuatro métodos, las posiciones para las cuales no se ha configurado una lista se mantienen vacías.

## Autenticación de NAC

La ventana Autenticación NAC muestra el método **EAPoUDP** configurado en el router. Si el asistente NAC ha sido utilizado para crear una configuración NAC en el router, la ventana contendrá el texto siguiente:

Nombre de lista	Método 1
valor por defecto	grupo SDM_NAC_Group

Es posible especificar listas de métodos adicionales en esta ventana si desea que el router intente con los métodos especificados antes de recurrir a la lista de métodos por defecto.

### Botones Agregar, Editar y Eliminar

Utilice estos botones para crear, editar y eliminar listas de métodos.

### Columna Nombre de la lista

Nombre de la lista de métodos. Una lista de métodos consiste en una lista secuencial que describe los métodos de autenticación solicitados con el fin de autenticar un usuario.

### Columna de Método 1

El método que el router probará en primer lugar. Si uno de los servidores en este método autentica al usuario (es decir envía una respuesta PASS), la autenticación se realizará de manera exitosa. Si el servidor entrega la respuesta FALLA, la autenticación fracasará. Si no hay respuesta de ninguno de los servidores al primer método, el router utilizará el método que sigue en la lista. Es posible ordenar los métodos en el momento de crear o editar una lista de métodos.

### Columnas de Método 2,3 y 4

Métodos que el router utilizará en caso de que los servidores mencionados en el método 1 no respondan. Si existen menos de cuatro métodos, las posiciones para las cuales no se ha configurado una lista se mantienen vacías.

## Autenticación de 802.1x

La ventana Autenticación 802.1x muestra la lista de métodos configurados para autenticación 802.1. Si el asistente para LAN se ha utilizado para crear una configuración 802.1x, esta ventana contiene la entrada siguiente:

Nombre de lista	Método 1
valor por defecto	group radius



**Nota**

No puede especificar listas de métodos adicionales para configuración 802.1x.

### Botones Agregar, Editar y Eliminar

Utilice estos botones para crear, editar y eliminar listas de métodos.

### Columna Nombre de la lista

Nombre de la lista de métodos. Una lista de métodos consiste en una lista secuencial que describe los métodos de autenticación solicitados con el fin de autenticar un usuario.

### Columna de Método 1

El método que el router probará en primer lugar. Si uno de los servidores en este método autentica al usuario (es decir envía una respuesta PASS), la autenticación se realizará de manera exitosa. Si el servidor entrega la respuesta FALLA, la autenticación fracasará. Si no hay respuesta de ninguno de los servidores al primer método, el router utilizará el método que sigue en la lista. Es posible ordenar los métodos en el momento de crear o editar una lista de métodos.

### Columnas de Método 2,3 y 4

Métodos que el router utilizará en caso de que los servidores mencionados en el método 1 no respondan. Si existen menos de cuatro métodos, las posiciones para las cuales no se ha configurado una lista se mantienen vacías.

## Agregar o Editar una lista de métodos para autenticar o autorizar

Una lista de métodos consiste en una lista secuencial que describe los métodos de autenticación solicitados con el fin de autenticar un usuario. Estas listas permiten designar uno o varios protocolos de seguridad que se utilizarán para la autenticación, con lo cual se garantiza un sistema de reserva para la autenticación en caso de que el método inicial fallara.

El software Cisco IOS utiliza el primer método que figura en la lista para autenticar los usuarios. Si dicho método no responde, el software Cisco IOS selecciona el siguiente método de autenticación que figura en la lista de métodos. Este proceso continúa hasta que se logra una comunicación correcta con un método de autenticación de la lista, o bien hasta que se agotan todos los métodos definidos en la lista de métodos.

Cabe destacar que el software Cisco IOS prueba la autenticación con el siguiente método de autenticación de la lista sólo cuando no existe respuesta del método anterior. Si la autenticación falla en algún punto de este ciclo, lo que significa que el servidor de seguridad o base de datos con nombre de usuario local responde con la denegación del acceso al usuario, el proceso de autenticación se detiene y no se prueba ningún otro método de autenticación.

### Nombre/Especificar

Seleccione el nombre Por defecto de la lista Nombre, o bien seleccione Definido por el usuario, y especifique un nombre de la lista de métodos en el campo Especificar.

### Métodos

Un método es un grupo de servidores configurado. Se pueden especificar y colocar en la lista hasta cuatro métodos, en el orden que desee que los utilice el router. El router probará el primer método de la lista. Si con la solicitud de autenticación se recibe una respuesta PASS o FAIL, el router ya no realizará ninguna otra consulta. Si el router no recibe ninguna respuesta con el primer método, utilizará el siguiente, y así sucesivamente hasta que reciba una respuesta PASS o FAIL.



## Agregar

Haga clic en este botón para agregar un método a la lista. Si no existe ningún grupo de servidores configurado para agregar, podrá configurar uno en la ventana que aparece.

## Eliminar

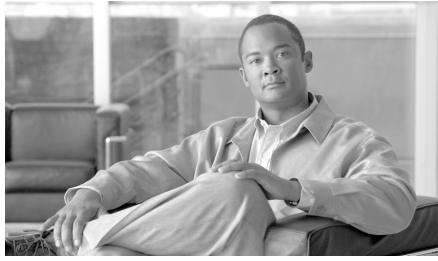
Haga clic en este botón para eliminar un método de la lista.

## Desplazar hacia arriba/abajo

El router prueba los métodos en el orden en que figuran en la lista de esta ventana. Haga clic en **Hacia arriba** para desplazar un método una posición hacia arriba en la lista. Haga clic en **Hacia abajo** para desplazar un método una posición hacia abajo en la lista.

El método “ninguno” siempre ocupará la última posición en la lista. Debajo de él no podrá colocarse ningún otro. Se trata de una restricción del IOS, el cual no aceptará ningún nombre de método una vez que en la lista de métodos se haya agregado el nombre de método “ninguno”.





## CAPÍTULO **33**

# Provisionamiento del router

---

Usted puede provisionar el router utilizando un dispositivo USB conectado directamente al router, o bien mediante Secure Device Provisioning (SDP). SDP debe ser compatible con su versión de Cisco IOS para estar disponible en Cisco SDM.

## Secure Device Provisioning

Esta ventana le permite utilizar Secure Device Provisioning (SDP) para realizar tareas como suscribir el router con un servidor de CA y configurar el router. Haga clic en el botón **Iniciar SDP** para transferirse a la aplicación Web SDP para completar el proceso.

Si está obteniendo certificados, Cisco SDM muestra la ventana Certificados en la que puede ver los certificados después de que se han obtenido de la CA.

Si desea saber lo que tiene que hacer para preparar la suscripción SDP, consulte [Sugerencias para la resolución de problemas SDP](#).

Si desea más información acerca de SDP, haga clic en el siguiente enlace:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products\\_feature\\_gui\\_de09186a008028afbd.html#wp1043332](http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_gui_de09186a008028afbd.html#wp1043332)



### Nota

---

Si el botón **Iniciar SDP** está ausente, la versión de Cisco IOS del router no es compatible con SDP. Si el botón **Iniciar SDP** está desactivado, usted inició sesión en Cisco SDM como usuario sin vista raíz.

---

# Provisionamiento del router desde el USB

Esta ventana le indica si Cisco SDM ha detectado un token USB o un dispositivo flash USB conectado a su router. Se puede hacer clic en el botón

**Provisionamiento del router** para elegir un archivo de configuración desde el token USB o el dispositivo flash USB.

Si elige cargar su router de esta forma, el archivo de configuración del token USB o del dispositivo flash USB se fusiona con el archivo de ejecución del router para crear un nuevo archivo de configuración de ejecución.

## Provisionamiento del router desde USB (cargar archivo)

Esta ventana le permite cargar un archivo de configuración desde un token USB o un dispositivo flash USB conectado a su router. El archivo será fusionado con su archivo de configuración de ejecución para crear un nuevo archivo de configuración de ejecución.

Para cargar un archivo de configuración, siga los pasos siguientes:

- 
- Paso 1** Seleccione el tipo de dispositivo del menú desplegable.
  - Paso 2** Especifique el nombre del archivo de configuración, incluida la ruta completa, o bien haga clic en **Examinar** y elija el archivo en la ventana Selección de archivos.
  - Paso 3** Si el tipo de dispositivo es un token USB, especifique la contraseña para ingresar al token en Token PIN.
  - Paso 4** Si desea previsualizar el archivo, haga clic en **Vista Previa** para mostrar el contenido del archivo en el panel de detalles.
  - Paso 5** Haga clic en **Aceptar** para cargar el archivo elegido.
-

# Sugerencias para la resolución de problemas SDP

Utilice esta información antes de realizar la suscripción mediante Secure Device Provisioning (SDP) para preparar la conexión entre el router y el servidor de certificados. Si se producen problemas durante la suscripción, puede consultar estas tareas para determinar dónde se encuentra el problema.

## Directrices

- Al iniciar SDP, deberá minimizar la ventana del explorador que muestra este tema de ayuda para poder ver la aplicación Web SDP.
- Si tiene planeado configurar el router mediante SDP, deberá hacerlo inmediatamente después de configurar la conexión WAN.
- Cuando haya terminado de efectuar los cambios en la configuración de SDP, deberá regresar a Cisco SDM y hacer clic en Actualizar, en la barra de herramientas, para ver el estado de los puntos de confianza en la ventana Certificados de router del árbol Componentes VPN.

## Sugerencias para la resolución de problemas

Las siguientes recomendaciones implican realizar preparativos en el router local y en el servidor de la CA. Deberá comunicar los requisitos siguientes al administrador del mencionado servidor. Asegúrese de los puntos siguientes:

- El router local y el servidor de la CA disponen de interconectividad IP. El router local debe poder realizar un ping correctamente en el servidor de certificados y este último debe poder hacer lo propio en el router local.
- El administrador del servidor de la CA utiliza un explorador Web compatible con JavaScript.
- El administrador del servidor de la CA dispone de privilegios de activación en el router local.
- El firewall del router local permitirá tráfico al servidor de certificados y desde el mismo.
- Si se ha configurado un firewall en el equipo solicitante y/o en el equipo de registro, debe asegurarse de que el firewall permita tráfico HTTP o HTTPS desde el PC en el cual se invoca la aplicación Cisco SDM o SDP.

Para obtener más información acerca de SDP, consulte la página Web siguiente:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products\\_feature\\_gui\\_de09186a008028afbd.html#wp1043332](http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_gui_de09186a008028afbd.html#wp1043332)

■ Sugerencias para la resolución de problemas SDP



# CAPÍTULO 34

## Lenguaje de política de clasificación común de Cisco

---

El Lenguaje de política de clasificación común de Cisco ([C3PL](#)) es un reemplazo estructurado para comandos de configuración específicos de la función. C3PL le permite crear políticas de tráfico basándose en eventos, condiciones y acciones. SDM utiliza C3PL para crear el [mapa de política](#) y el [mapa de clase](#) que describen los siguientes temas de ayuda.

### Mapa de política

Los mapas de política especifican las acciones que se deben tomar cuando el tráfico coincide con los criterios definidos. Los tipos de tráfico y criterios se definen en mapas de clase asociados con un mapa de política. Para que un router utilice la información de un mapa de política y sus mapas de clases asociados, el mapa de política debe estar asociado con un [par de zonas](#). Para obtener más información sobre la configuración de zonas y pares de zonas, consulte [Firewall de política basado en zonas](#).

## Ventanas de mapa de política

Utilice las ventanas de mapa de política para revisar, crear y editar mapas de política para QoS, HTTP y otros tipos de tráfico. La parte superior de la ventana indica los mapas de política configurados, y la parte inferior muestra los detalles del mapa de política resaltado. Si necesita editar un mapa de política o ver más detalles, haga clic en **Editar** para mostrar un cuadro de diálogo que le permita ver información y realizar cambios.

Este tema de ayuda proporciona una descripción general para las ventanas de mapa de política y algunos datos de ejemplo.

### Agregar

Haga clic en **Agregar** para mostrar un cuadro de diálogo donde pueda configurar un mapa de política.

### Editar

Haga clic en **Editar** para mostrar un cuadro de diálogo donde pueda editar el mapa de política seleccionado. El botón **Editar** se desactiva si no se han configurado mapas de política.

### Eliminar

Haga clic en **Eliminar** para eliminar el mapa de política seleccionado.

### Área de lista de mapa de política

Esta área enumera los mapas de política configurados para el protocolo o la función particular. Seleccione un mapa de política para mostrar detalles en la parte inferior de la pantalla. Los ejemplos siguientes muestran dos políticas de IM.

Nombre del mapa de política	Descripción
im-pmap-g	política de invitado
im-pmap-e	política de empleado



## Detalles del mapa de política

Los detalles del mapa de política seleccionado muestran la configuración del mapa de política. Los detalles que se muestran varían de acuerdo con el tipo de mapa de política.

[HTTP](#), [IM](#), [P2P](#), [IMAP](#) y [POP3](#) muestran un nombre de clase coincidente, una acción y una columna de registro. La siguiente tabla muestra detalles de un mapa de política de IM. El router bloquea el tráfico AOL, pero permite todos los otros tipos de tráfico IM.

Coincidir nombre de clase	Acción	Registro
aol-cmap	Desactivada	Desactivada
clase por defecto	Activada	Desactivada

Inspección de protocolo, [SMTP](#) y los detalles del mapa de política de [SUNRPC](#) incluyen las columnas Coincidir nombre de clase y Acción. La tabla siguiente muestra detalles de un mapa de política SUNRPC.

Coincidir nombre de clase	Acción
cmap-sunrpc1	Permitir
cmap-sunrpc2	Ninguno

## Agregar o editar un mapa de política de QoS

Utilice esta información como ayuda para agregar o editar un mapa de política de QoS.

### Nombre y descripción de política

Si está creando un nuevo mapa de política, especifique un nombre y una descripción para él en estos campos. Si está editando un mapa de política, estos campos son sólo para presentación.

## Columnas Mapa de clase, Servicio de cola, Definir DSCP y Rechazo

Estas columnas resumen la información acerca de cada mapa de clase en el mapa de política. El siguiente ejemplo corresponde a un mapa de clase de voz:

```
Voice-FastEthernet0/1 LLQ 70% ef No
```

Este mapa de clase utiliza Low Latency Queuing y 70% del ancho de banda para esta interfaz. El valor DSCP está definido en ef, y los paquetes de este tipo no se rechazan.

Los botones **Agregar**, **Editar**, **Eliminar**, **Desplazar hacia arriba** y **Desplazar hacia abajo** se pueden utilizar para modificar la información del mapa de clase en esta lista.

## Agregar un mapa de política de inspección

Los mapas de política de inspección especifican la acción que debe realizar el router para que el tráfico coincida con los criterios en los mapas de clase asociados. El router puede permitir que el tráfico pase, rechazarlo y, opcionalmente, registrar el evento o inspeccionar el tráfico.

El nombre y la descripción que especifique se verán en la ventana Mapas de política de inspección. Las columnas Mapa de clase y Acción muestran los mapas de clase asociados con este mapa de política y la acción que el router debe realizar para el tráfico que describe el mapa de clase. Haga clic en **Agregar** para agregar un nuevo mapa de clase a la lista y configurar la acción. Haga clic en **Editar** para modificar la configuración de un mapa de clase. Utilice los botones **Desplazar hacia arriba** y **Desplazar hacia abajo** para cambiar el orden de evaluación de los mapas de clase.

## Mapa de política de capa 7

Esta ventana le permite seleccionar un mapa de política de capa 7 que se utiliza para inspeccionar una aplicación que ha seleccionado. La ventana muestra los mapas de política disponibles para esa aplicación. Seleccione un mapa de política y haga clic en **Aceptar**.

## Inspección de aplicación

Las políticas de inspección de aplicación se aplican en la capa 7 del modelo OSI, donde las aplicaciones de usuario envían y reciben mensajes que permiten a las aplicaciones ofrecer capacidades útiles. Algunas aplicaciones pueden ofrecer capacidades no deseadas o vulnerables, de modo que los mensajes asociados con estas capacidades se deben filtrar para limitar las actividades en los servicios de la aplicación.

El firewall de política de zona del software Cisco IOS ofrece inspección y control de aplicación en los siguientes servicios de la aplicación: Aplicaciones [HTTP](#), [SMTP](#), [POP3](#), [IMAP](#), [SUNRPC](#), [P2P](#) y [IMAP](#). Para obtener más información, consulte los enlaces siguientes

- [Agregar un mapa de clase de inspección HTTP](#)
- [Agregar o editar un mapa de clase SMTP](#)
- [Agregar o editar un mapa de clase de POP3](#)
- [Agregar o editar un mapa de clase IMAP](#)
- [Agregar o editar un mapa de clase SUNRPC](#)
- [Agregar o editar un mapa de clase punto a punto](#)
- [Agregar o editar un mapa de clase de mensajería instantánea](#)

## Configurar inspección profunda de paquetes

La inspección de capa 7 (aplicación) aumenta la inspección de capa 4 con la capacidad para reconocer y aplicar acciones específicas del servicio, como, por ejemplo, bloquear y permitir selectivamente las capacidades de búsqueda de archivos, transferencia de archivos y chat de texto. Las capacidades específicas del servicio varían de acuerdo con el servicio.

Si está creando un nuevo mapa de política, especifique un nombre en el campo **Nombre de mapa de política**. También puede agregar una descripción. Haga clic en **Agregar > nuevo mapa de clase** para crear un nuevo mapa de clase punto a punto. [Agregar o editar un mapa de clase punto a punto](#) contiene información sobre cómo crear este tipo de mapa de clase. Haga clic en **Agregar > clase por defecto** para agregar el mapa de clase por defecto.

Cuando el mapa de clase aparezca en la tabla, especifique la acción que desea realizar cuando se encuentra una coincidencia y si desea que se registren las coincidencias. Puede especificar <Ninguna>, **Restablecer** o **Permitir**. En el ejemplo siguiente, hay **P2P** mapas de clase para gnutella y para eDonkey.

Coincidir nombre de clase	Acción	Registro
gnutellaCMap	Permitir	
eDonkeyCMap	Restablecer	X

## Mapas de clase

Los mapas de clase definen el tráfico que un Firewall basado en política de zonas (ZPF) selecciona para la aplicación de políticas. Los mapas de clase de capa 4 ordenan el tráfico de acuerdo con los siguientes criterios:

- Grupo de acceso: una lista de control de acceso estándar, ampliada o denominada puede filtrar tráfico de acuerdo con la dirección IP de origen y destino, y con el puerto de origen y destino
- Protocolo: los protocolos de capa 4 (TCP, UDP y ICMP) y los servicios de aplicación, como, por ejemplo, HTTP, SMTP, DNS, etc. Se puede especificar cualquier servicio conocido o definido por el usuario que sea conocido para PAM
- Mapa de clase: un mapa de clase subordinado que proporciona criterios de coincidencia adicionales se puede establecer dentro de otro mapa de clase
- Not: el criterio ‘not’ especifica que el tráfico que no coincida con un servicio (protocolo), grupo de acceso o mapa de clase subordinado especificado se seleccionará para el mapa de clase.

Los mapas de clase pueden aplicar operadores “coincidir con cualquiera” o “coincidir con todos” para determinar cómo aplicar los criterios de coincidencia. Si se especifica “coincidir con cualquiera”, el tráfico debe cumplir sólo con uno de los criterios de coincidencia en el mapa de clase. Si se especifica “coincidir con todos”, el tráfico debe coincidir con todos los criterios del mapa de clase para pertenecer a esa clase en particular.

## Asociar mapa de clase

Para asociar un mapa de clase con un mapa de política de inspección, realice las siguientes tareas.

- 
- Paso 1** Especifique un nombre de mapa de clase haciendo clic en el botón a la derecha del campo de nombre y seleccionando **Agregar un mapa de clase**, **Seleccionar un mapa de clase** o **clase por defecto**.
- Paso 2** En la casilla Acción, haga clic en **Pasar**, **Rechazar** o **Inspeccionar**. Si hace clic en **Rechazar**, opcionalmente puede hacer clic en **Registrar** para registrar el evento de rechazo. Si hace clic en **Inspeccionar**, haga clic en **Opciones avanzadas** para especificar los mapas de parámetros, las políticas de inspección o la supervisión que desea para el tráfico en esta clase.
- Paso 3** Haga clic en **Aceptar** para cerrar este cuadro de diálogo y volver al cuadro de diálogo Agregar o Editar un mapa de política de inspección.
- 

## Opciones avanzadas del mapa de clase

Cuando selecciona la acción de inspección para tráfico, puede especificar mapas de parámetros, inspección de aplicación y [ZPF](#) supervisión.

### Mapa de parámetros de inspección

Los mapas de parámetros de inspección especifican límites de tiempo y parámetros de control de sesión de TCP, DNS y UDP. Puede seleccionar un mapa de parámetros existente. Si no se configura un mapa de parámetros, este campo estará desactivado. Haga clic en **Ver** para mostrar el mapa de parámetros seleccionado sin salir de este cuadro de diálogo.

### Mapa de parámetros de filtrado de URL

Los mapas de parámetros de filtrado de URL pueden especificar servidores de filtrado de URL y listas de URL locales. Puede seleccionar un mapa de parámetros existente. Si no se configura un mapa de parámetros, este campo estará desactivado. Haga clic en **Ver** para mostrar el mapa de parámetros seleccionado sin salir de este cuadro de diálogo.

## Activar inspección de aplicación

Una política de inspección de aplicación especifica los tipos de datos para inspeccionar en paquetes de una aplicación especificada. Puede seleccionar una política de inspección de aplicación existente. Si no se configura una política de inspección de aplicación, este campo estará desactivado. Haga clic en **Ver** para mostrar la política de inspección de aplicación seleccionada sin salir de este cuadro de diálogo.

## Velocidad de supervisión y ráfaga

Puede limitar el tráfico a una velocidad específica y especificar un valor de ráfaga. La velocidad de supervisión puede ser un valor entre 8.000 y 2.000.000.000 de bits por segundo. La velocidad de ráfaga puede ser un valor entre 1.000 y 512.000.000 bytes.

## Mapa de clase de QoS

Utilice esta ventana para mostrar y editar información de mapa de clase de QoS. Los mapas de clase de QoS se utilizan en mapas de política de QoS para definir tipos de tráfico.

Haga clic en un nombre de mapa de clase para mostrar detalles acerca de ese mapa de clase en el área **Detalles de mapa de clase**.

Los detalles de un mapa de clase muestran los protocolos que coinciden para definir el tráfico. El siguiente ejemplo muestra detalles de un mapa de clase de señalización de voz.

Detalles de mapa de clase:SDMSignal-FastEthernet0/1

Nombre del elemento	Valor del elemento
Protocolos de coincidencia	h323,rtcp

H.323 y RTCP son los protocolos de señalización de voz que deben coincidir.

## Agregar o editar un mapa de clase de QoS

Utilice esta información como ayuda para agregar o editar un mapa de clase de QoS. Si está agregando un nuevo mapa de clase de QoS, haga clic en el botón a la derecha del campo y seleccione **Agregar un mapa de clase** o **Seleccionar un mapa de clase** desde el menú contextual.

Consulte la información que se incluye en [Acción](#) para obtener información sobre las opciones **Rechazar**, **Definir DSCP** y **Servicio de cola**.

## Agregar o editar un mapa de clase de QoS

Especifique un nombre y una descripción del mapa de clase de QoS que está creando de modo que sea fácil identificarlo y utilizarlo. Haga clic en [Clasificación](#) para obtener una descripción de los botones **Cualquiera**, **Todos** y **Editar** que aparecen en la casilla Clasificación.

## Seleccionar un mapa de clase

Haga clic en el nombre del mapa de clase que desea seleccionar y luego en **Aceptar**. La entrada del mapa de clase se agrega a la ventana desde la cual invocó este cuadro de diálogo.

## Inspección profunda

La inspección profunda le permite crear mapas de clase para parámetros específicos de una aplicación. Por ejemplo, puede crear mapas de clase para la aplicaciones [P2P](#) comunes, como, por ejemplo [eDonkey](#), [gnutella](#) y [kazaa2](#).

## Ventanas Mapa de clase y Grupos de servicio de aplicación

Utilice las ventanas de mapa de clase para revisar, crear y editar mapas de clase para protocolos, tales como [HTTP](#), [SMTP](#) y [POP3](#). El área Mapa de clase de la ventana indica los mapas de clase configurados, y la parte inferior muestra los detalles del mapa de clase seleccionado. Si necesita editar un mapa de clase o ver más detalles, haga clic en **Editar** para mostrar un cuadro de diálogo que le permita ver información y realizar cambios.

■ Mapas de clase

### Agregar

Haga clic en **Agregar** para crear un nuevo mapa de clase del tipo que seleccionó y especifique la configuración en el cuadro de diálogo que se despliega.

### Editar

Haga clic en **Editar** para cambiar la configuración del mapa de clase seleccionado.

### Eliminar

Haga clic en **Eliminar** para eliminar el mapa de clase seleccionado. Cisco SDM puede mostrar cuadros de diálogo si hay dependencias asociadas con esta configuración, como, por ejemplo, mapas de clase subordinados o mapas de parámetros que pueden ser utilizados por otros mapas de clase.

### Área Mapa de clase

Esta área muestra los mapas de clase configurados para el protocolo que seleccionó. Contiene los nombres de los mapas de clase configurados y otra información pertinente.

#### Mapas de clase de QoS

Los mapas de clase de QoS se muestran en una tabla con una columna Nombre de mapa de clase y una columna Descripción. La siguiente es una tabla de ejemplo.

Nombre de mapa de clase	Descripción
CMAP-DMZ	Mapa de clase de QoS de FTP y HTTP
CMAP-3	Prueba



### Mapas de clase de inspección, HTTP, SMTP, SUN RPC, IMAP y POP3

Estos tipos de mapas de clase tienen una columna Nombre de mapa de clase y Usado. La siguiente es una tabla de ejemplo para HTTP.

Nombre de mapa de clase	Usado por
http-rqst	pmap-5
http-rsp-body	pmap-5

### Grupos de servicio de mensajería instantánea y grupos de servicio de aplicación Par a Par

Los grupos de servicio de mensajería instantánea y los grupos de servicio de aplicación par a par (**P2P**) tienen una columna adicional, porque los mapas de clase se configuran para una aplicación específica, como, por ejemplo, Yahoo! La aplicación de mensajería instantánea de Messenger o la aplicación P2P de [gnutella](#). La siguiente tabla muestra datos de ejemplo para grupos de servicio de la aplicación P2P

Nombre de mapa de clase	Usado por	Tipo de mapa de clase
cmap-gnutella	pmap-7	gnutella
cmap-edonkey	pmap-7	edonkey
cmap-bittorrent	pmap-7	bittorrent

### Detalles del mapa de clase

El área Detalles del mapa de clase muestra la configuración de un mapa de clase en particular. Tiene dos columnas: Nombre de elemento y Valor de elemento.

#### Nombre de elemento

El nombre del ajuste de configuración. Por ejemplo, un mapa de clase HTTP puede tener ajustes para Encabezado de solicitud, Uso incorrecto del puerto e Infracción del protocolo.

### Valor de elemento

El valor del ajuste de configuración. Por ejemplo, el valor de la configuración Encabezado de solicitud HTTP puede ser Longitud > 500, y el indicador Uso incorrecto del puerto puede estar desactivado.

### Más información acerca de los detalles del mapa de clase

Para obtener más información acerca de los detalles del mapa de clase que se muestran en estas ventanas, haga clic en cualquiera de los enlaces siguientes:

- [Agregar o editar un mapa de clase de QoS](#)
- [Agregar o editar un mapa de clase de inspección](#)
- [Agregar un mapa de clase de inspección HTTP](#)
- [Agregar o editar un mapa de clase de mensajería instantánea](#)
- [Agregar o editar un mapa de clase punto a punto](#)
- [Agregar o editar un mapa de clase SMTP](#)
- [Agregar o editar un mapa de clase SUNRPC](#)
- [Agregar o editar un mapa de clase IMAP](#)
- [Agregar o editar un mapa de clase de POP3](#)

## Agregar o editar un mapa de clase de inspección

Crear un mapa de clase de inspección le permite poner a disposición para inspección una amplia variedad de tráfico. Especifique un nombre para identificar este mapa de clase en el campo **Nombre de clase**. También puede especificar una descripción. Si está editando un mapa de clase, no puede cambiar el nombre. Cuando haya especificado las condiciones que desea que asigne la clase, haga clic en **Aceptar**.

### Especificar si desea que la clase coincida con cualquiera o con todas las condiciones

Haga clic en **Cualquiera** si es necesario que la clase coincida con una o más condiciones que usted elige. Haga clic en **Todas** si la clase debe coincidir con todas las condiciones.

## Seleccionar lo que desea que coincida con el mapa de clase de inspección

Examine en la columna izquierda lo que desea que coincida con el mapa de clase. Haga clic en el signo más (+) junto a un nodo para mostrar los nodos secundarios. Por ejemplo, haga clic en **HTTP** para mostrar los nodos secundarios http y https. Para seleccionar un elemento, haga clic en él y luego en **Agregar>>**. Para eliminar un elemento que agregó a la columna de la derecha, haga clic en él y luego en **<<Quitar**.

## Cambiar el orden de coincidencia

Si elige que coincida cualquiera de las condiciones, es probable que desee cambiar el orden de coincidencia de los elementos en la columna derecha. Para mover un artículo hacia arriba de la lista, haga clic en él y luego en **Subir**. Para mover un artículo hacia abajo de la lista, haga clic en él y luego en **Bajar**. El botón **Subir** se desactiva cuando hace clic en el elemento en la parte superior de la lista. El botón **Bajar** se desactiva cuando hace clic en el elemento en la parte inferior de la lista.

## Asociar mapa de parámetro

Este cuadro de diálogo muestra los mapas de parámetro que puede asociar con el mapa de clase. Haga clic en la casilla **Seleccionar** junto al mapa de parámetro que desea asociar con el mapa de clase.

## Agregar un mapa de clase de inspección HTTP

Los mapas de clase de inspección HTTP le permiten poner a disposición para inspección una amplia variedad de datos de Solicitud, Respuesta y Respuesta a Solicitud HTTP.

Para crear un mapa de clase de inspección HTTP, haga lo siguiente:

- Paso 1** Especifique un nombre de clase para identificar el mapa de clase. También puede especificar una descripción que será visible en la ventana Mapas de clase HTTP.
- Paso 2** Haga clic en la rama del árbol HTTP que contiene el tipo de datos que desea poner a disposición para inspección. Puede crear un mapa de clase para solicitudes, respuestas y respuestas a solicitudes HTTP.

- Paso 3** Haga clic en la subrama correspondiente para especificar el tipo de datos que desea incluir.
- Paso 4** Configure los datos del mapa de clase en los campos que se muestran.
- Paso 5** Especifique condiciones de coincidencia haciendo clic en **Alguna de las siguientes condiciones** si el mapa de clase debe coincidir con una o más condiciones. Haga clic en **Todas las condiciones especificadas a continuación** si el mapa de clase debe coincidir con todas las condiciones que usted especifica.
- 

## Encabezado de solicitud HTTP

Especifique criterios del mapa de clase para atributos de encabezado de solicitud HTTP.

### Longitud mayor que

Haga clic en esta casilla si desea especificar una longitud de encabezado de solicitud global que un paquete no debe superar y especifique el número de bytes.

### Recuento mayor que

Haga clic en esta casilla si desea especificar un límite para el número total de campos de encabezado de solicitud que un paquete no debe superar y especifique el número de campos.

### Expresiones regulares

Haga clic en esta casilla para especificar expresiones regulares con las cuales coincidir. Elija un mapa de clase de expresión regular existente o cree uno nuevo que coincida con las cadenas que está inspeccionando. Para obtener más información acerca de cómo crear expresiones regulares, consulte [Agregar o editar expresión regular](#). Para examinar un mapa existente sin salir de este cuadro de diálogo, selecciónelo en la lista **Seleccionar un mapa existente** y haga clic en **Ver**.

### Nombre de campo y opciones de configuración

Puede incluir campos dentro del encabezado para los criterios de inspección y especificar longitud, recuento y cadenas para inspeccionar. Haga clic en **Agregar** para incluir un campo y especifique criterios en el cuadro de diálogo que se muestra.

## Campos de encabezado de solicitud HTTP

Elija el tipo de campo de encabezado desde la lista y especifique los criterios de inspección para él.

### Longitud mayor que

Haga clic en esta casilla si desea especificar una longitud que este campo no debe superar y especifique el número de bytes. Por ejemplo, puede bloquear una solicitud cuyo campo de cookies superó los 256 bytes o cuyo campo de agente usuario superó los 128 bytes.

### Recuento mayor que

Haga clic en esta casilla si desea especificar la cantidad de veces que se puede repetir este campo en el encabezado y especifique un número. Por ejemplo, puede bloquear una solicitud que tenga varias líneas de encabezado de longitud de contenido especificando el valor 1. Este ejemplo es una medida efectiva para evitar el tráfico clandestino de sesiones

### Expresiones regulares

Haga clic en esta casilla para especificar expresiones regulares con las cuales coincidir. Elija un mapa de clase de expresión regular existente o cree uno nuevo que coincida con las cadenas que está inspeccionando. Para obtener más información acerca de cómo crear expresiones regulares, consulte [Agregar o editar expresión regular](#). Para examinar un mapa existente sin salir de este cuadro de diálogo, selecciónelo en la lista **Seleccionar un mapa existente** y haga clic en **Ver**.

### Campo de coincidencias

Marque esta casilla si desea que el mapa de clase coincida con el tipo de campo que eligió.

### Otros campos de este cuadro de diálogo

De acuerdo con el campo de encabezado HTTP que elija, este cuadro de diálogo puede mostrar campos adicionales, lo que permite especificar criterios adicionales. Por ejemplo, si elige el campo **tipo de contenido**, puede inspeccionar faltas de coincidencia de tipo de contenido entre la solicitud y la respuesta, tipos de contenido desconocidos e infracciones de protocolo para el tipo de contenido particular. Si selecciona el campo **codificación de transferencia**, puede inspeccionar varios tipos de compresión y codificación.

## Cuerpo de solicitud HTTP

Puede inspeccionar la longitud y las cadenas de caracteres de un cuerpo de solicitud HTTP.

### Longitud

Marque esta casilla y seleccione **Mayor que (>)** para especificar un límite superior para la longitud del cuerpo de la solicitud. Seleccione **Menor que (<)** para especificar un límite inferior.

### Expresiones regulares

Si desea inspeccionar cadenas, haga clic en esta casilla y elija un mapa de clase de expresión regular existente o cree un nuevo mapa que coincida con las cadenas que está inspeccionando. Para obtener más información acerca de cómo crear expresiones regulares, consulte [Agregar o editar expresión regular](#). Para examinar un mapa existente sin salir de este cuadro de diálogo, selecciónelo en la lista **Seleccionar un mapa existente** y haga clic en **Ver**.

## Argumentos de encabezado de solicitud HTTP

Puede inspeccionar la longitud de los argumentos enviados en una solicitud e inspeccionar cadenas que coinciden con las expresiones regulares que ha configurado.

### Longitud mayor que

Haga clic en esta casilla y especifique el número de bytes que la longitud total de los argumentos del encabezado de solicitud no debe superar.

### Expresiones regulares

Haga clic en esta casilla para especificar expresiones regulares con las cuales coincidir. Elija un mapa de clase de expresión regular existente o cree uno nuevo que coincida con las cadenas que está inspeccionando. Para obtener más información acerca de cómo crear expresiones regulares, consulte [Agregar o editar expresión regular](#). Para examinar un mapa existente sin salir de este cuadro de diálogo, selecciónelo en la lista **Seleccionar un mapa existente** y haga clic en **Ver**.

## Método HTTP

Los métodos HTTP indican el propósito de una solicitud HTTP. Elija los métodos HTTP en la columna **Lista de métodos** que desea inspeccionar y marque la casilla **Seleccionar** junto al método.

## Uso incorrecto del puerto de solicitud

El puerto 80 HTTP es utilizado algunas veces por **IM**, **P2P**, arquitectura en túneles y otras aplicaciones. Marque los tipos de usos incorrectos de puertos que desea inspeccionar. Puede inspeccionar cualquier tipo de uso incorrecto del puerto, uso incorrecto del puerto por aplicaciones IM, uso incorrecto del puerto de la aplicación P2P y uso incorrecto por aplicaciones de arquitectura en túneles

## URI de solicitud

Especifique los criterios del Identificador de recurso universal (**URI**) que desea incluir en el mapa de clase.

## Longitud mayor que

Haga clic en esta casilla si desea especificar una longitud de URI que un paquete no debe superar y especifique el número de bytes.

## Expresiones regulares

Haga clic en esta casilla para especificar expresiones regulares con las cuales coincidir. Elija un mapa de clase de expresión regular existente o cree uno nuevo que coincida con las cadenas que está inspeccionando. Para obtener más información acerca de cómo crear expresiones regulares, consulte [Agregar o editar expresión regular](#). Para examinar un mapa existente sin salir de este cuadro de diálogo, selecciónelo en la lista **Seleccionar un mapa existente** y haga clic en **Ver**.

### Caso de ejemplo

Configure un mapa de clase HTTP para bloquear una solicitud cuyo URI coincida con cualquiera de las siguientes expresiones regulares:

“.\*cmd.exe”

“.\*sex”

“.\*gambling”

## Encabezado de respuesta

Especifique los criterios de los encabezados de respuesta HTTP que desea incluir en el mapa de clase.

### Longitud mayor que

Haga clic en esta casilla si desea especificar una longitud de encabezado de respuesta global que un paquete no debe superar y especifique el número de bytes.

### Recuento mayor que

Haga clic en esta casilla si desea especificar un límite para el número total de campos de encabezado de respuesta que un paquete no debe superar y especifique el número de campos.

### Expresiones regulares

Haga clic en esta casilla para especificar expresiones regulares con las cuales coincidir. Elija un mapa de clase de expresión regular existente o cree uno nuevo que coincida con las cadenas que está inspeccionando. Para obtener más información acerca de cómo crear expresiones regulares, consulte [Agregar o editar expresión regular](#). Para examinar un mapa existente sin salir de este cuadro de diálogo, selecciónelo en la lista **Seleccionar un mapa existente** y haga clic en **Ver**.

## Campos de encabezado de respuesta

Elija el tipo de campo de encabezado desde la lista y especifique los criterios de inspección para él.

### Longitud mayor que

Haga clic en esta casilla si desea especificar una longitud de campo que un paquete no debe superar y especifique el número de bytes.

### Recuento mayor que

Haga clic en esta casilla si desea especificar un límite para el número total de campos de este tipo que un paquete no debe superar y especifique el número de campos.



## Expresiones regulares

Haga clic en esta casilla para especificar expresiones regulares con las cuales coincidir. Elija un mapa de clase de expresión regular existente o cree uno nuevo que coincida con las cadenas que está inspeccionando. Para obtener más información acerca de cómo crear expresiones regulares, consulte [Agregar o editar expresión regular](#). Para examinar un mapa existente sin salir de este cuadro de diálogo, selecciónelo en la lista **Seleccionar un mapa existente** y haga clic en **Ver**.

## Otros campos de este cuadro de diálogo

De acuerdo con el campo de encabezado HTTP que elija, este cuadro de diálogo puede mostrar campos adicionales, lo que permite especificar criterios adicionales. Por ejemplo, si elige el campo **tipo de contenido**, puede inspeccionar faltas de coincidencia de tipo de contenido entre la solicitud y la respuesta, tipos de contenido desconocidos e infracciones de protocolo para el tipo de contenido particular. Si selecciona el campo **codificación de transferencia**, puede inspeccionar varios tipos de compresión y codificación.

## Campo de coincidencias

Marque esta casilla si desea que el mapa de clase coincida con el tipo de campo que eligió.

## Cuerpo de respuesta HTTP

Especifique los criterios del cuerpo de respuesta HTTP según los cuales inspeccionar.

## Subprogramas Java en respuesta HTTP

Marque esta casilla si desea inspeccionar subprogramas Java en la respuesta HTTP. De acuerdo con las acciones configuradas en el mapa de política

## Longitud

Marque esta casilla y seleccione **Mayor que (>)** para especificar un límite superior para la longitud del cuerpo de la respuesta. Seleccione **Menor que (<)** para especificar un límite inferior.

## Expresiones regulares

Haga clic en esta casilla para especificar expresiones regulares con las cuales coincidir. Elija un mapa de clase de expresión regular existente o cree uno nuevo que coincida con las cadenas que está inspeccionando. Para obtener más información acerca de cómo crear expresiones regulares, consulte [Agregar o editar expresión regular](#). Para examinar un mapa existente sin salir de este cuadro de diálogo, selecciónelo en la lista **Seleccionar un mapa existente** y haga clic en **Ver**.

## Línea de estado de respuesta HTTP

Haga clic en esta casilla y especifique expresiones regulares para que coincidan con las líneas de estado de respuesta. Elija un mapa de clase de expresión regular existente o cree uno nuevo que coincida con las cadenas que está inspeccionando.

### Caso de ejemplo

Configure el router para que registre una alarma cada vez que se intente acceder a una página prohibida. Una página prohibida generalmente contiene un código de estado 403 y la línea de estado se ve similar a ésta “HTTP/1.0 403 page forbidden\r\n.”

La expresión regular para esto es la siguiente:

```
[Hh][Tt][Tt][Pp][/] [0-9][. ] [0-9][ \t ]+403
```

El registro se especifica en el mapa de política con el cual se asocia el mapa de clase HTTP.

Para obtener más información acerca de cómo crear expresiones regulares, consulte [Agregar o editar expresión regular](#). Para examinar un mapa existente sin salir de este cuadro de diálogo, selecciónelo en la lista **Seleccionar un mapa existente** y haga clic en **Ver**.

## Criterios de encabezado de solicitud/respuesta

Especifique criterios del mapa de clase para encabezados de solicitud/respuesta HTTP.

### Longitud mayor que

Haga clic en esta casilla si desea especificar una longitud de encabezado de solicitud/respuesta global que un paquete no debe superar y especifique el número de bytes.

### Recuento mayor que

Haga clic en esta casilla si desea especificar un límite para el número total de campos de encabezado de solicitud/respuesta que un paquete no debe superar y especifique el número de campos.

### Expresiones regulares

Haga clic en esta casilla para especificar expresiones regulares con las cuales coincidir. Elija un mapa de clase de expresión regular existente o cree uno nuevo que coincida con las cadenas que está inspeccionando. Para obtener más información acerca de cómo crear expresiones regulares, consulte [Agregar o editar expresión regular](#). Para examinar un mapa existente sin salir de este cuadro de diálogo, selecciónelo en la lista **Seleccionar un mapa existente** y haga clic en **Ver**.

## Campos de encabezado de solicitud/respuesta HTTP

Elija el campo de encabezado de solicitud/respuesta HTTP que desea incluir en el mapa de clase.

### Longitud mayor que

Haga clic en esta casilla si desea especificar una longitud de campo que un paquete no debe superar y especifique el número de bytes.

## Recuento mayor que

Haga clic en esta casilla si desea especificar un límite para el número total de campos de este tipo que un paquete no debe superar y especifique el número de campos.

## Expresiones regulares

Haga clic en esta casilla para especificar expresiones regulares con las cuales coincidir. Elija un mapa de clase de expresión regular existente o cree uno nuevo que coincida con las cadenas que está inspeccionando. Para obtener más información acerca de cómo crear expresiones regulares, consulte [Agregar o editar expresión regular](#). Para examinar un mapa existente sin salir de este cuadro de diálogo, selecciónelo en la lista **Seleccionar un mapa existente** y haga clic en **Ver**.

## Otros campos de este cuadro de diálogo

De acuerdo con el campo de encabezado HTTP que elija, este cuadro de diálogo puede mostrar campos adicionales, lo que permite especificar criterios adicionales. Por ejemplo, si elige el campo **tipo de contenido**, puede inspeccionar faltas de coincidencia de tipo de contenido entre la solicitud y la respuesta, tipos de contenido desconocidos e infracciones de protocolo para el tipo de contenido particular. Si selecciona el campo **codificación de transferencia**, puede inspeccionar varios de tipos de compresión y codificación.

## Campo de coincidencias

Marque esta casilla si desea que el mapa de clase coincida con el tipo de campo que eligió.

## Cuerpo de solicitud/respuesta

El router puede inspeccionar la longitud del cuerpo de solicitud/respuesta y cadenas de texto específicas dentro del cuerpo de la solicitud/respuesta.

## Longitud

Marque esta casilla y seleccione **Mayor que (>)** para especificar un límite superior para la longitud del cuerpo de la solicitud/respuesta. Seleccione **Menor que (<)** para especificar un límite inferior.

## Expresiones regulares

Haga clic en esta casilla para especificar expresiones regulares con las cuales coincidir. Elija un mapa de clase de expresión regular existente o cree uno nuevo que coincida con las cadenas que está inspeccionando. Para obtener más información acerca de cómo crear expresiones regulares, consulte [Agregar o editar expresión regular](#). Para examinar un mapa existente sin salir de este cuadro de diálogo, selecciónelo en la lista **Seleccionar un mapa existente** y haga clic en **Ver**.

## Infracción del protocolo de solicitud/respuesta

Para inspeccionar infracciones del protocolo en solicitudes/respuestas de HTTP, haga clic en **Infracción del protocolo**.

## Agregar o editar un mapa de clase IMAP

Crear un mapa de clase para inspección de Internet Message Access Protocol (**IMAP**) puede ayudar a los usuarios que están usando mecanismos seguros de autenticación para impedir el compromiso de las credenciales del usuario.

Especifique un nombre para identificar este mapa de clase en el campo **Nombre de clase**. También puede especificar una descripción. Si está editando un mapa de clase, no puede cambiar el nombre.

Haga clic en **Cadena de inicio de sesión en texto no cifrado** para hacer que el router inspeccione inicios de sesión que no son seguros en el tráfico IMAP.

Haga clic en **Comando de protocolo no válido** para hacer que el router inspeccione comandos no válidos en el tráfico IMAP.

## Agregar o editar un mapa de clase SMTP

Los mapas de clase de Simple Mail Transfer Protocol (**SMTP**) le permiten limitar la longitud del contenido e imponer el cumplimiento del protocolo.

Especifique un nombre para identificar este mapa de clase en el campo **Nombre de clase**. También puede especificar una descripción en el campo proporcionado.

Especifique la **Transferencia de datos máxima permitida** en la casilla **Criterios de coincidencia**.

## Agregar o editar un mapa de clase SUNRPC

Los mapas de clase de SUN Remote Procedure Call (**SUNRPC**) le permiten especificar el número de los programas cuyo tráfico desea que el router inspeccione.

Especifique un nombre para identificar este mapa de clase en el campo **Nombre de clase**. También puede especificar una descripción. Si está editando un mapa de clase, no puede cambiar el nombre.

Haga clic en **Agregar** en la casilla **Número de programa de coincidencia** para agregar un número de programa.

## Agregar o editar un mapa de clase de mensajería instantánea

Los mapas de clase de Mensajería instantánea (**IM**) le permiten especificar el tipo de mensajería instantánea y si desea que se inspeccione el tráfico para todos los servicios IM o sólo el tráfico para el servicio de chat de texto.

En el campo **Tipo de mapa de clase**, seleccione **aol** para America Online, **msnmsgr** para Microsoft Networks Messenger, o bien, **ymsgr** para Yahoo! Messenger.

En la casilla Criterios de coincidencia, haga clic en **Todos los servicios** o en **Servicios de chat de texto** si sólo desea que se inspeccione el tráfico de chat de texto.

## Agregar o editar un mapa de clase punto a punto

Un mapa de clase **P2P** especifica una aplicación P2P y los criterios de coincidencia. Sólo se puede especificar una aplicación por mapa de clase.

## Nombre de la clase

Especifique un nuevo nombre de clase para crear un nuevo mapa de clase. Si hace clic en el botón a la derecha del campo puede seleccionar los mapas de clase existentes para edición. Puede editar los criterios de coincidencia para un mapa de clase, pero no puede cambiar el tipo de mapa de clase.

## Tipo de mapa de clase

Puede crear un mapa de clase P2P para los siguientes tipos de servicios P2P:

- [eDonkey](#)
- [fasttrack](#)
- [gnutella](#)
- [kazaa2](#)

## Criterios y valor de coincidencia

Haga clic en **Agregar** para introducir criterios de coincidencia y poder especificar el tipo de conexión que se va a identificar mediante la clase de tráfico.

Introduzca criterios de coincidencia para especificar el tipo de conexión que se va a identificar mediante la clase de tráfico. Puede especificar que las conexiones de transferencia de archivos se identifiquen mediante la clase de tráfico para fasttrack, gnutella y kazaa2. Para eDonkey, puede especificar que las conexiones de transferencia de archivos, las solicitudes de nombre de archivo (buscar nombre de archivo) y los chats de texto se identifiquen mediante la clase de tráfico.

El valor para el criterio de coincidencia puede ser cualquier expresión regular. Por ejemplo, para especificar que se identifiquen todas las conexiones de transferencia de archivos, introduzca \*.

## Agregar regla P2P

Introduzca criterios de coincidencia para especificar el tipo de conexión que se va a identificar mediante la clase de tráfico. Puede especificar que las conexiones de transferencia de archivos se identifiquen mediante la clase de tráfico para fasttrack, gnutella y kazaa2. Para eDonkey, puede especificar que las conexiones de transferencia de archivos, las solicitudes de nombre de archivo (buscar nombre de archivo) y los chats de texto se identifiquen mediante la clase de tráfico. El valor para el criterio de coincidencia puede ser cualquier expresión regular. Por ejemplo, para especificar que se identifiquen todas las conexiones de transferencia de archivos, introduzca \*.

## Agregar o editar un mapa de clase de POP3

Crear un mapa de clase para inspección de Post Office Protocol, versión 3, (POP3) puede ayudar a los usuarios que están usando mecanismos seguros de autenticación para impedir el compromiso de las credenciales del usuario.

Especifique un nombre para identificar este mapa de clase en el campo **Nombre de clase**. También puede especificar una descripción. Si está editando un mapa de clase, no puede cambiar el nombre.

Haga clic en **Cadena de inicio de sesión en texto no cifrado** para hacer que el router inspeccione inicios de sesión que no son seguros en el tráfico POP3.

Haga clic en **Comando de protocolo no válido** para hacer que el router inspeccione comandos no válidos en el tráfico POP3.

## Mapas de parámetros

Los mapas de parámetros especifican el comportamiento de inspección para firewall de política de zona, para parámetros como, por ejemplo, protección de denegación de servicio, temporizadores de sesión y conexión, y configuración de registro. Los mapas de parámetros también se pueden aplicar a los mapas de clase y política de capa 7 para definir el comportamiento específico de la aplicación, como objetos HTTP, requisitos de autenticación POP3 e IMAP, y otra información específica de la aplicación.



## Ventanas de mapa de parámetros

Las ventanas de mapa de parámetros listan los mapas de parámetros configurados para información de protocolo, filtrado de URL, expresiones regulares y otros tipos de mapas de parámetros. Si el mapa de parámetro se ha asociado con un mapa de clase, el nombre del mapa de clase aparece en la columna Usado por. Los detalles del mapa de parámetro seleccionado se muestran en la mitad inferior de la ventana. Puede agregar, editar y eliminar mapas de parámetros. SDM le informa si intenta eliminar un mapa de parámetro que está siendo usado por un mapa de clase.

Para obtener más información acerca de los mapas de parámetros que se muestran en estas ventanas, haga clic en cualquiera de los enlaces siguientes:

- [Tiempos de inactividad y umbrales para mapas de parámetros de inspección y CBAC](#)
- [Agregar o editar un mapa de parámetro para información de protocolo](#)
- [Configuración general para el filtrado de URL](#)
- [Agregar o editar el servidor de filtro de URL](#)
- [Lista de URL local](#)
- [Agregar o editar expresión regular](#)

### Agregar o editar un mapa de parámetro para información de protocolo

Puede ser necesario identificar servidores para tipos específicos de aplicaciones, como, por ejemplo, aplicaciones **IM**, de manera que pueda restringir el uso a una actividad particular, tal como chat de texto.

#### Nombre de mapa de parámetros

Especifique un nombre que transmita el uso de este mapa de parámetros. Por ejemplo, si está creando una lista de servidores para servidores de chat de texto de Yahoo! Instant Messenger, puede utilizar el nombre ymsggr-pmap.

#### Detalles del servidor

Esta área de la pantalla es una lista de nombres de servidores, direcciones IP de servidores o intervalos de direcciones IP.

## Agregar o editar una entrada del servidor

Puede proporcionar el nombre de host o la dirección IP de un servidor individual, o un intervalo de direcciones IP asignadas a un grupo de servidores.

Puede especificar un nombre de host en el campo **Nombre** si el router puede contactar a un servidor DNS en la red para resolver la dirección IP del servidor. Si desea especificar la dirección IP de un servidor, especifíquela en el campo **Single Dirección IP**. Si hay varios servidores que utilizan un intervalo de direcciones IP, utilice el campo **Intervalo de IP**. Especifique la dirección IP más baja en el campo de la izquierda y la dirección IP más alta en el campo de la derecha. Por ejemplo, para especificar el intervalo 103.24.5.67 a 99, introduzca 103.24.5.67 en el campo de la izquierda, y 103.24.5.99 en el campo de la derecha.

## Agregar o editar expresión regular

Una expresión regular coincide con cadenas de texto, ya sea lateralmente como una cadena exacta, o utilizando *metacaracteres*, de manera que pueda hacer coincidir múltiples variantes de una cadena de texto. Puede utilizar una expresión regular para hacer coincidir el contenido de un determinado tráfico de aplicaciones; por ejemplo, puede hacer coincidir el texto del cuerpo al interior de un paquete HTTP.

Las expresiones regulares que usted crea se pueden utilizar en cualquier lugar que se necesite una expresión regular en las pantallas de firewall de política basado en zona. [Metacaracteres de expresión regular](#) contiene una lista de metacaracteres de expresión regular y la manera de utilizarlos.

### Nombre

Especifique un nombre para identificar la expresión regular. Si está editando la expresión regular, el campo de nombre será de sólo lectura.

## Lista de patrones

Una expresión regular puede contener múltiples patrones. Haga clic en **Agregar** para mostrar un cuadro de diálogo donde puede introducir un nuevo patrón de expresión regular. Cada patrón que crea se agrega automáticamente a la lista. Si necesita copiar un patrón de otra expresión regular, haga clic en **Copiar patrón**, haga clic en el signo más (+) junto al nombre de la expresión regular, luego en el patrón que desea, y por último, en **Aceptar**.

```
tipo de mapa de parámetro regex ref_regex
patrón "\.delfinproject\.com"
patrón "\.looksmart\.com"
tipo de mapa de parámetro regex host_regex
patrón "secure\.keenvalue\.com"
patrón "\.looksmart\.com"
tipo de mapa de parámetro regex usragnt_regex
patrón "Peer Points Manager"
```

Reemplace por la tabla.

## Agregar un patrón

El patrón que especifica en esta ventana se agrega al final del mapa de parámetro de expresión regular que está editando. Si necesita reordenar los patrones en el mapa de parámetro, puede hacerlo en la ventana Editar expresión regular.

### Patrón

Especifique el patrón que desea agregar a la expresión regular.

### Botón guía

Haga clic para mostrar el cuadro de diálogo [Generar expresión regular](#) que le puede ayudar a construir una expresión regular. Si hace clic en **Guía**, cualquier texto que especifique en el campo **Patrón** aparece en el campo [Expresión regular](#) del cuadro de diálogo Generar expresión regular.

## Generar expresión regular

El cuadro de diálogo Generar expresión regular le permite construir una expresión regular de caracteres y metacaracteres. Los campos que insertan metacaracteres incluyen el metacarácter entre paréntesis en el nombre del campo.

### Generar fragmento

Esta área le permite generar fragmentos de texto regular o insertar un metacarácter en el campo Expresión regular.

- Inicia al comienzo de la línea (^): indica que el fragmento debe iniciarse al comienzo de una línea, utilizando el metacarácter de símbolo de intercalación (^). Asegúrese de insertar un fragmento con esta opción al comienzo de la expresión regular.
- Especificar cadena de caracteres: especifique una cadena de texto en forma manual.
  - Cadena de caracteres: especifique una cadena de texto.
  - Omitir caracteres especiales: si especificó algún metacarácter en la cadena de texto que desea que se use literalmente, marque esta casilla para agregar el carácter de escape barra diagonal inversa (\) delante de ellos. Por ejemplo, si especifica “example.com,” esta opción lo convierte en “example\\.com”.
  - Omitir distinción de mayúsculas y minúsculas: si desea que los caracteres mayúsculas y minúsculas coincidan, esta casilla de verificación agrega texto automáticamente para hacer coincidir mayúsculas y minúsculas. Por ejemplo, al especificar “cats”, esta entrada se convierte en “[cC][aA][tT][sS]”.

### Especificar carácter

Le permite especificar un metacarácter para insertarlo en la expresión regular.

- Invalidar el carácter: especifica no hacer coincidir el carácter que identifica.
- Cualquier carácter (.): inserta el metacarácter punto (.) para hacer coincidir cualquier carácter. Por ejemplo, **d.g** coincide con dog, dag, dtg y con cualquier palabra que contenga esos caracteres, como, por ejemplo, doggonnit.

- Conjunto de caracteres: inserta un conjunto de caracteres. El texto puede coincidir con cualquier carácter del juego. Los juegos incluyen:

[0-9A-Za-z]

[0-9]

[A-Z]

[a-z]

[aeiou]

[\n\f\r\t] (lo que coincide con una línea nueva, avance de página, retorno de carro o tabulación)

Por ejemplo, si especifica [0-9A-Za-z], este fragmento coincidirá con cualquier carácter entre la A y la Z (mayúsculas o minúsculas) o con cualquier dígito entre 0 y 9.

- Carácter especial: inserta un carácter que requiere un escape, incluidos \, ?, \*, +, |, ., [, ( ó ^. El carácter de escape es la barra diagonal inversa (\), que se introduce automáticamente al elegir esta opción.
- Carácter de espacio en blanco: los caracteres de espacio en blanco incluyen \n (línea nueva), \f (avance de página), \r (retorno de carro) o \t (tabulación).
- Número octal de tres dígitos: coincide con un carácter ASCII como octal (hasta tres dígitos). Por ejemplo, el carácter \040 representa un espacio. La barra diagonal inversa (\) se introduce automáticamente.
- Número hexadecimal de dos dígitos: coincide con un carácter ASCII que utiliza hexadecimal (exactamente dos dígitos). La barra diagonal inversa (\) se introduce automáticamente.
- Carácter especificado: especifique un carácter único.

## Vista previa de fragmento

*Sólo para presentación.* Muestra el fragmento como se especificará en la expresión regular.

- Adjuntar fragmento: agrega el fragmento al final de la expresión regular.
- Adjuntar fragmento como alternativo: agrega el fragmento al final de la expresión regular, separado por una barra vertical (|), lo que hace coincidir cada expresión que separa. Por ejemplo, **dog|cat** coincide con dog o con cat.
- Insertar fragmento en la posición del cursor: inserta el fragmento en la posición del cursor.

## Expresión regular

Esta área incluye texto de expresión regular que usted puede introducir manualmente y generar con fragmentos. Puede seleccionar texto en el campo Expresión regular y aplicar un cuantificador a la selección.

- Repeticiones de selección: seleccione texto en el campo Expresión regular, haga clic en una de las siguientes opciones y luego en **Aplicar a selección**. Por ejemplo, si la expresión regular es “test me” y usted selecciona “me” y aplica **Una o más veces**, entonces la expresión regular cambia a “test (me)+”.
  - Ninguna o una vez (?): un cuantificador que indica que hay 0 ó 1 evento de la expresión anterior. Por ejemplo, **lo?se** coincide con lse o con lose.
  - Una o más veces (+): un cuantificador que indica que hay al menos 1 evento de la expresión anterior. Por ejemplo, **lo+se** coincide con lose y loose, pero no con lse.
  - Una o más veces (+): un cuantificador que indica que hay al menos 1 evento de la expresión anterior. Por ejemplo, **lo+se** coincide con lose y loose, pero no con lse.
  - Cualquier número de veces (\*): un cuantificador que indica que hay 0, 1 o un número cualquiera de eventos de la expresión anterior. Por ejemplo, **lo\*se** coincide con lse, lose, loose, etc.
  - Como mínimo: repita al menos *x* veces. Por ejemplo, **ab(xy){2,}z** coincide con abxyxyz, abxyxyxyz, etc.
  - Exactamente: repita exactamente *x* veces. Por ejemplo, **ab(xy){3,}z** coincide con abxyxyxyz.
- Aplicar a selección: aplica el cuantificador a la selección.

## Metacaracteres de expresión regular

La tabla siguiente enumera los metacaracteres que tienen significados especiales.

Carácter	Descripción	Notas
.	Punto	Coincide con cualquier carácter. Por ejemplo, <b>d.g</b> coincide con dog, dag, dtg y con cualquier palabra que contenga esos caracteres, como, por ejemplo, doggonnit.
(exp)	Subexpresión	Una subexpresión separa caracteres de caracteres vecinos, de modo que puede utilizar otros metacaracteres en la subexpresión. Por ejemplo, <b>d(o a)g</b> coincide con dog y dag, pero <b>do ag</b> coincide con do y ag. Una subexpresión también se puede utilizar con cuantificadores de repetición para diferenciar los caracteres destinados para repetición. Por ejemplo, <b>ab(xy){3,}z</b> coincide con abxyxyz.
	Alternación	Coincide con cada expresión que separa. Por ejemplo, <b>dog cat</b> coincide con dog o con cat.
?	Signo de interrogación	Cuantificador que indica que hay 0 ó 1 evento de la expresión anterior. Por ejemplo, <b>lo?se</b> coincide con lse o con lose.  <b>Nota</b> Debe especificar <b>Ctrl+V</b> y luego el signo de interrogación, o se invoca la función de ayuda.
*	Asterisco	Cuantificador que indica que hay 0, 1 o un número cualquiera de eventos de la expresión anterior. Por ejemplo, <b>lo*se</b> coincide con lse, lose, loose, etc.
+	Más	Cuantificador que indica que hay al menos 1 evento de la expresión anterior. Por ejemplo, <b>lo+se</b> coincide con lose y loose, pero no con lse.
{x}	Cuantificador de repetición	Repita exactamente <i>x</i> veces. Por ejemplo, <b>ab(xy){3,}z</b> coincide con abxyxyz.
{x,}	Cuantificador de repetición mínima	Repita al menos <i>x</i> veces. Por ejemplo, <b>ab(xy){2,}z</b> coincide con abxyxyz, abxyxyxyz, etc.

Carácter	Descripción	Notas
[abc]	Clase de carácter	Coincide con cualquier carácter que esté entre paréntesis. Por ejemplo, [abc] coincide con a, b o c.
[^abc]	Clase de carácter invalidado	Coincide con un carácter que no está entre paréntesis. Por ejemplo, [^abc] coincide con cualquier carácter que no sea a, b o c. [^A-Z] coincide con cualquier carácter que no esté en mayúsculas.
[a-c]	Clase de intervalo de caracteres	Coincide con cualquier carácter en el intervalo. [a-z] coincide con cualquier minúscula. Puede combinar caracteres e intervalos: [abcq-z] coincide con a, b, c, q, r, s, t, u, v, w, x, y, z, al igual que [a-cq-z]. El guión (-) es literal sólo si es el último o primer carácter dentro del paréntesis: [abc-] o [-abc].
“”	Comillas	Conserva los espacios finales o iniciales de la cadena. Por ejemplo, “ test” conserva el espacio inicial cuando busca una coincidencia.
^	Símbolo de intercalación	Especifica el comienzo de una línea.
\	Carácter de escape	Cuando se usa con un metacarácter, coincide con un carácter literal. Por ejemplo, \[ coincide con el paréntesis de apertura.
cár	Carácter	Cuando el carácter no es un metacarácter, coincide con el carácter literal.
\r	Retorno de carro	Coincide con un retorno de carro 0x0d.
\n	Línea nueva	Coincide con una línea nueva 0x0a.
\t	Tabulación	Coincide con una tabulación 0x09.
\f	Avance de página	Coincide con un avance de página 0x0c.
\xNN	Número hexadecimal con carácter de escape	Coincide con un carácter ASCII que utiliza hexadecimal (exactamente dos dígitos).
\NNN	Número octal con carácter de escape	Coincide con un carácter ASCII como octal (exactamente tres dígitos). Por ejemplo, el carácter 040 representa un espacio.





# CAPÍTULO 35

## Filtrado de URL

---

El filtrado de URL le permite controlar el acceso a sitios de Internet permitiendo o denegando el acceso a sitios Web específicos en función de la información contenida en una lista de URL. Puede conservar una lista de URL local en el router y puede utilizar listas de URL almacenadas en los servidores de listas de filtro de URL Websense o Secure Computing. El filtrado de URL se activa al configurar una política de seguridad de la aplicación que lo habilite.

Incluso si no hay ninguna política de seguridad de la aplicación configurada en el router, podrá conservar una lista de URL local y una lista de servidores de filtro de URL que se podrán utilizar para filtrar URL cuando se cree una política que lo habilite.

Este capítulo contiene las secciones siguientes:

- [Ventana de filtrado de URL](#)
- [Lista de URL local](#)
- [Servidores de filtro de URL](#)

Si desea más información acerca del filtrado de URL, diríjase al siguiente enlace:

[Firewall Websense URL Filtering](#)

Si desea saber cómo se utilizan las políticas de filtrado de URL, haga clic en [Preferencia del filtrado de URL](#).

# Ventana de filtrado de URL

Esta ventana muestra la configuración global para el filtrado de URL en el router. Puede conservar la lista de URL local y la lista de servidores de filtro de URL en las pantallas de Tareas adicionales o en las ventanas de seguridad de la aplicación. La Configuración global para el filtrado de URL sólo se puede mantener desde esta ventana de Tareas adicionales. Utilice el botón **Editar configuración global** si desea cambiar estos valores.

Si desea conocer una descripción de cada ajuste que aparece en esta ventana, haga clic en [Editar configuración global](#).

Consulte la información preliminar en [Filtrado de URL](#) para obtener una descripción de las características del filtrado de URL que ofrece Cisco SDM.

## Editar configuración global

Puede editar las configuraciones globales del filtrado de URL en esta ventana.



### Nota

Se debe activar el registro en el router para notificar alertas del filtro de URL, mensajes de seguimiento de auditoría y mensajes de sistema pertenecientes al servidor de filtro de URL.

### Modo Permitir

Marque esta casilla para permitir que el router entre en modo Permitir cuando no pueda conectarse con ninguno de los servidores de filtrado de URL de la lista de servidores. Cuando el router se encuentra en modo Permitir, se aceptan todas las peticiones HTTP si el router no se puede conectar con ningún servidor de la lista de servidores de filtro de URL. Por defecto, el modo Permitir está desactivado.

### Alerta de filtro de URL

Seleccione esta casilla para permitir que el router registre los mensajes de advertencia de filtrado de URL. Los mensajes de advertencia de filtrado de URL informan de eventos como la caída de un servidor de filtrado de URL o una petición HTTP que contiene una URL demasiado larga para tratarse de una petición de búsqueda. Por defecto, esta opción está desactivada.

## Seguimiento de auditoría

Seleccione esta casilla para permitir que el router mantenga un seguimiento de auditoría en el registro. El router guardará los mensajes de estado de peticiones URL que indican si se ha permitido o denegado la petición HTTP y, además, almacenará otros mensajes de seguimiento de auditoría. Por defecto, esta opción está desactivada.

## Registro del servidor de filtro de URL

Marque esta casilla para permitir que el router guarde mensajes de sistema que pertenezcan al servidor de filtro de URL en el registro. Por defecto, esta opción está desactivada.

## Tamaño caché

Puede establecer el tamaño máximo de la caché que almacena las últimas direcciones IP solicitadas y su respectivo estado de autorización. El valor por defecto de este caché es de 5.000 bytes. El rango oscila entre 0 bytes y 2.147.483.647. El caché se borra cada 12 horas.

## Máxima cantidad de peticiones HTTP en búfer

Puede configurar la cantidad máxima de peticiones HTTP pendientes que el router puede almacenar en el búfer. Por defecto, el router almacena hasta 1.000 peticiones en el búfer. Se pueden especificar de 1 a 2.147.483.647 peticiones.

## Máxima cantidad de respuestas HTTP en búfer

Puede configurar la cantidad máxima de respuestas HTTP desde el servidor de filtrado de URL que el router puede almacenar en el búfer. Una vez alcanzada esta cifra, el router elimina respuestas adicionales. El valor por defecto es 200. Se puede establecer un valor de 0 a 20.000.

## Configuración general para el filtrado de URL

Asigne un nombre al filtro de URL, especifique lo que debe hacer el router cuando detecte una coincidencia y configure el registro y los parámetros de tamaño de caché. También puede especificar una interfaz de origen si no desea que el mapa de parámetros de filtrado de URL se aplique a todas las interfaces del router.

### Nombre del filtro de URL

Especifique un nombre que transferirá información acerca de cómo se configura o usa el filtro de URL. Por ejemplo, si especifica una interfaz de origen de FastEthernet 1, podría especificar el nombre `fa1-parmap`. Si el filtro usa un servidor de filtro de URL Websense en la dirección IP 192.128.54.23, podría especificar `websense23-parmap` como el nombre.

### Modo Permitir

Marque esta casilla para permitir que el router entre en modo Permitir cuando no pueda conectarse con ninguno de los servidores de filtrado de URL de la lista de servidores. Cuando el router se encuentra en modo Permitir, se aceptan todas las peticiones HTTP si el router no se puede conectar con ningún servidor de la lista de servidores de filtro de URL. Por defecto, el modo Permitir está desactivado.

### Alerta de filtro de URL

Seleccione esta casilla para permitir que el router registre los mensajes de advertencia de filtrado de URL. Los mensajes de advertencia de filtrado de URL informan de eventos como la caída de un servidor de filtrado de URL o una petición HTTP que contiene una URL demasiado larga para tratarse de una petición de búsqueda. Por defecto, esta opción está desactivada.

### Seguimiento de auditoría

Seleccione esta casilla para permitir que el router mantenga un seguimiento de auditoría en el registro. El router guardará los mensajes de estado de peticiones URL que indican si se ha permitido o denegado la petición HTTP y, además, almacenará otros mensajes de seguimiento de auditoría. Por defecto, esta opción está desactivada.

## Registro del servidor de filtro de URL

Marque esta casilla para permitir que el router guarde mensajes de sistema que pertenezcan al servidor de filtro de URL en el registro. Por defecto, esta opción está desactivada.

## Tamaño caché

Puede establecer el tamaño máximo de la caché que almacena las últimas direcciones IP solicitadas y su respectivo estado de autorización. El valor por defecto de este caché es de 5.000 bytes. El rango oscila entre 0 bytes y 2.147.483.647. El caché se borra cada 12 horas.

## Número máximo de solicitudes HTTP en búfer

Puede configurar la cantidad máxima de peticiones HTTP pendientes que el router puede almacenar en el búfer. Por defecto, el router almacena hasta 1.000 peticiones en el búfer. Se pueden especificar de 1 a 2.147.483.647 peticiones.

## Número máximo de respuestas HTTP en búfer

Puede configurar la cantidad máxima de respuestas HTTP desde el servidor de filtrado de URL que el router puede almacenar en el búfer. Una vez alcanzada esta cifra, el router elimina respuestas adicionales. El valor por defecto es 200. Se puede establecer un valor de 0 a 20.000.

## Características avanzadas

La casilla Opciones avanzadas le permite elegir la interfaz de origen. Elija la interfaz en la lista Interfaz de origen.

## Lista de URL local

Si la imagen de Cisco IOS en el router admite el filtrado de URL, pero no el firewall de política basado en zonas (ZPF), puede mantener una lista de URL local en el router. Esta lista es utilizada por todas las políticas de seguridad de la aplicación en las que el filtrado de URL esté activado. Las imágenes de Cisco IOS de la versión 12.4(9)T y posteriores admiten todas las funciones de ZPF que admite SDM. En una configuración de ZPF, se puede crear una lista de URL local para cada mapa de parámetro de filtrado de URL.

Se puede utilizar Cisco SDM para crear entradas de lista e importar entradas desde una lista almacenada en su equipo. Cuando una lista de URL local se utiliza en combinación con servidores de filtro de URL, las entradas locales se utilizan primero. Consulte el apartado [Preferencia del filtrado de URL](#) para obtener más información.

### Mantenimiento de la lista de URL local

Se puede utilizar Cisco SDM para conservar una lista de URL local agregando y eliminando entradas una por una e importando una lista de URL desde su equipo; especifique lo que desea que Cisco SDM haga con cada entrada. Utilice los botones **Agregar** y **Eliminar** para administrar entradas específicas en la lista del router y haga clic en el botón **Importar Lista de URL** para importar una lista de URL desde su PC.



#### Nota

---

Si se elimina una entrada de la lista local y el router está configurado para utilizar servidores de filtrado de URL, es posible que las entradas que coincidan con las que está borrando de la lista local existan en esos servidores.

---

Utilice el botón **Eliminar todos** para eliminar todas las entradas del router. Si no hay ninguna lista local configurada en el router, éste deberá confiar en los servidores de filtro de URL configurados. Si desea recuperar la lista de URL que está eliminando en otro momento, utilice el botón **Exportar Lista de URL** para guardar la lista de URL en su equipo antes de eliminar todas las entradas. Cuando guarde una lista de URL en su equipo, la lista recibe la extensión.CSV.

## Importar listas de URL desde su PC

Haga clic en el botón **Importar Lista de URL** para importar una lista de URL desde su equipo al router. La lista de URL que seleccione debe poseer extensión.txt o.CSV. Una vez que seleccione la lista de su equipo, Cisco SDM muestra un cuadro de diálogo que le permite especificar lo que desea hacer con cada entrada de la lista. Consulte el apartado [Importar lista de URL](#) para obtener más información.

## Agregar o editar URL local

Utilice esta ventana para agregar o editar una entrada URL para la lista de URL local del router. Ingrese un nombre de dominio completo o parcial y seleccione **Permitir** o **Denegar** pedidos para esta URL.

Si escribe un nombre de dominio completo como, por ejemplo, www.somedomain.com, todas las peticiones que incluyan ese nombre de dominio (por ejemplo: www.somedomain.com/news o www.somedomain.com/index) serán permitidas o denegadas en función de la configuración que elija en este cuadro de diálogo. Estas peticiones no se enviarán a los servidores de filtrado de URL que el router esté configurado para utilizar.

Si escribe un nombre de dominio parcial como, por ejemplo, .somedomain.com, todas las peticiones que finalicen con esa cadena (por ejemplo: www.somedomain.com/products o wwwin/somedomain.com/eng) serán permitidas o denegadas en función de la configuración que elija en este cuadro de diálogo. Estas peticiones no se enviarán a los servidores de filtrado de URL que el router esté configurado para utilizar.

## Importar lista de URL

Este cuadro de diálogo le permite examinar la lista de URL que está importando desde su equipo al router y especificar lo que desea hacer con cada entrada. Si una entrada URL de este cuadro de diálogo no está presente en el router, puede agregarla a la lista del router haciendo clic en **Anexar**. Si una entrada URL ya se encuentra en el router pero usted desea reemplazarla con la entrada de este cuadro de diálogo, haga clic en **Sustituir**.

Por defecto, todas las casillas de la columna **Importar** están marcadas. Si no desea enviar alguna entrada al router, desmarque la casilla correspondiente. Si desea desmarcar todas las casillas, haga clic en **Deseleccionar todas**. Si hace clic en **Seleccionar todas** marcará todas las casillas.

**Agregar** agrega toda casilla marcada a la lista de URL. Si intenta agregar una entrada que ya se encuentre en la lista de URL, no podrá hacerlo incluso si la acción especificada para el dominio en la entrada difiere de la acción que ya se encuentra en la lista.

Utilice el botón **Sustituir** para especificar una acción diferente para una entrada que ya se encuentre en la lista de URL del router. Si la entrada que marcó no se encuentra en la lista del router, hacer clic en **Sustituir** no surtirá efecto alguno.

## Servidores de filtro de URL

El router puede enviar peticiones HTTP a servidores de filtrado de URL que puedan almacenar listas de URL mucho más extensas que las que puede guardar el router. Si el router está configurado con una lista de servidores de filtro de URL, el router enviará peticiones que no coinciden con las entradas de la lista local al servidor de filtro de URL al que esté conectado y permitirá o denegará la petición en función de la respuesta que reciba del servidor. Cuando el servidor al que está conectado el router falla, el router se comunica con el siguiente servidor de la lista hasta que establece una conexión.

Las listas de los servidores de filtro de URL se pueden utilizar junto con las listas de URL locales. Haga clic en [Preferencia del filtrado de URL](#) si desea saber cómo utiliza estos dos recursos el router.



Haga clic en **Agregar** y elija **Secure Computing** o bien **Websense** para especificar el tipo de servidor que está agregando.

**Nota**

El software Cisco IOS sólo puede utilizar un tipo de servidor de filtrado de URL y no le permitirá agregar un servidor a la lista si se trata de uno de distinto tipo. Por ejemplo, si una lista de servidor de filtro de URL que contiene servidores Websense está configurada en el router, usted recibirá un mensaje de error si intenta agregar un servidor Secure Computing a la lista. Si la lista de servidor de filtro de URL ya contiene un tipo de servidor y usted desea cambiar al otro tipo, deberá eliminar todas las entradas del servidor de la lista antes de agregar entradas del nuevo tipo.

Esta ventana muestra la configuración para cada servidor de filtro de URL de la lista. Consulte [Agregar o editar el servidor de filtro de URL](#) si desea conocer una descripción de cada valor de configuración.

## Agregar o editar el servidor de filtro de URL

Especifique la información para el servidor de filtro de URL Websense o Secure Computing.

### Dirección IP/Nombre de host

Especifique la dirección IP o el nombre de host para el servidor. Si especifica un nombre de host, el router deberá estar conectado a un servidor DNS para poder resolver el nombre de host e interpretarlo como una dirección IP.

### Dirección

Seleccione **Interna** si el servidor de filtro de URL es parte de una red interna. Suele ser una de las redes a las que se conectan las interfaces LAN del router. Seleccione **Externa** si el router se encuentra en la red externa. Suele ser una de las redes a las que se conectan las interfaces WAN del router. El valor por defecto es **Interna**.

## Número de puerto

Almacena automáticamente el número de puerto por defecto para el tipo de servidor de filtro de URL que esté agregando. Si está agregando un servidor Websense, el valor por defecto es 15868. Si se trata de un servidor Secure Computing, el valor será 4005. Cambie este número por el número del puerto que escucha el servidor si dicho número difiere del valor por defecto. Este campo acepta valores del 1 al 65535.

## Contador de retransmisión

Campo opcional. Indique el número de veces que desee que el router intente retransmitir la petición si no recibe respuesta del servidor. El valor por defecto es 2 veces. Este campo acepta valores del 1 al 10.

## Tiempo de inactividad de retransmisión

Campo opcional. Indique el número de segundos que el router debe esperar una respuesta del servidor antes de retransmitir la petición. El valor por defecto es 5 segundos.

# Preferencia del filtrado de URL

El filtrado de URL debe activarse en **Configurar > Firewall y lista de control de acceso > Seguridad de la aplicación > URL Filtrado** y haciendo clic en **Activar filtrado de URL**. Esto sólo puede realizarse cuando se haya configurado una política de seguridad de la aplicación en el router.

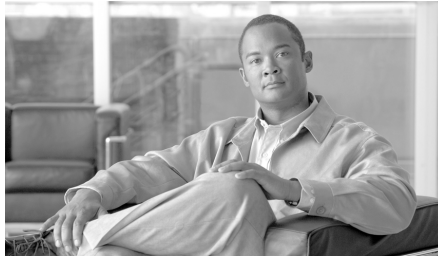
Cuando se activa el filtrado de URL, el router determina cómo manejar una petición HTTP de la siguiente manera:

- Si la URL de la petición coincide con alguna entrada de la lista de URL local del router, éste permite o deniega la petición en función de dicha entrada.
- Si la URL de la petición no coincide con ninguna entrada de la lista de URL local, el router deriva la petición HTTP al servidor de filtrado de URL al que esté conectado. Y permite o deniega la petición en función de la información que devuelve el servidor.

- Si el modo Permitir está desactivado y el router no puede establecer conexión con ningún servidor de filtro de URL, el router denegará la petición. Por defecto, el modo Permitir está desactivado.
- Si el modo Permitir está activado y el router no puede establecer conexión con ningún servidor de filtro de URL, el router permitirá la petición. El modo Permitir se puede activar en el cuadro de diálogo [Editar configuración global](#).

Sólo se puede configurar una lista de URL y una lista de servidores de filtro de URL en el router. Todas las políticas de seguridad de la aplicación utilizan las mismas listas de URL y de servidores de filtro de URL. Estas listas se pueden administrar en las ventanas de seguridad de la aplicación o yendo a **Tareas Adicionales > Filtrado de URL**. Si se eliminan todas las políticas de seguridad de la aplicación, las listas de URL y de servidores de filtro de URL todavía se pueden administrar en las ventanas de Tareas adicionales. Sin embargo, el router no llevará a cabo el filtrado de URL a menos que se active el filtrado de URL en la política de seguridad de la aplicación.





# CAPÍTULO 36

## Gestión de configuración

---

Cisco SDM permite editar el archivo de configuración del router y restablecer los valores por defecto de fábrica del mismo. Debido a que puede perder la conexión entre el PC y el router después de editar directamente el archivo de configuración y restablecer los valores por defecto de fábrica del router, asegúrese de leer la ayuda en línea de todas las pantallas de esta área de Cisco SDM.

## Edición manual del archivo de configuración

Cisco SDM permite editar el archivo de configuración del router mediante un editor de configuración que se puede utilizar para importar un archivo de configuración o para especificar directamente comandos del CLI de Cisco IOS.

Cisco SDM admite los comandos y palabras clave de Cisco IOS más utilizados, pero no admite todos los comandos del CLI. Si es usuario experto del CLI de Cisco IOS y comprende a la perfección el efecto de los comandos de configuración que se especifican en el funcionamiento del router y la red en la que reside, comprobará que el uso del editor de configuración resulta más rápido que los diálogos de Cisco SDM. Si desea agregar una configuración que Cisco SDM no admite, deberá utilizar el editor de configuración o abrir una sesión Telnet con el router y utilizar el CLI de Cisco IOS.

El uso del editor de configuración omite la validación de Cisco SDM. Aunque Cisco SDM devuelve mensajes de error de IOS, no puede comparar los cambios de la configuración con la configuración en ejecución para informar de los conflictos que pueden producirse. Por ejemplo, si utiliza los diálogos de Cisco SDM para especificar una configuración de VPN en un router que ya dispone de configuración de firewall, Cisco SDM examina el firewall y determina las declaraciones de permisos que se deben agregar para activar el tráfico VPN y lo hace automáticamente. Sin embargo, si utiliza el editor de configuración, se deben determinar los conflictos que pueden producirse mediante un examen de la configuración existente para realizar los cambios adicionales que son necesarios para resolver los conflictos y, luego, supervisar el comportamiento del router para ver si gestiona el tráfico de la forma prevista.

Aunque no es obligatorio, se recomienda que permita que Cisco SDM realice una copia de seguridad de la actual configuración en ejecución. Cuando Cisco SDM realiza esta copia de seguridad, siempre utiliza el mismo nombre de archivo, por lo que se sobrescribe cualquier archivo anterior.

## Editor de configuración

El editor de configuración permite ver la configuración en ejecución y realizar cambios en la misma mediante la edición de comandos concretos o la sustitución del archivo de configuración completo por otro importado desde el PC. Puede ver la configuración en ejecución mientras realiza los cambios o puede utilizar la ventana completa para ver la configuración que se envía al router.

### Configuración en ejecución

Por defecto, este cuadro muestra la configuración en ejecución del router. Para ocultar el cuadro, haga clic en **Ocultar** en la esquina superior derecha de la ventana. Para mostrar de nuevo el cuadro, haga clic en **Mostrar**.

### Editar configuración

Realice las ediciones en este cuadro. Por defecto, este cuadro está vacío. Para rellenarlo con la configuración en ejecución del router, haga clic en **Importar > configuración en ejecución**. Para rellenarlo con un archivo de configuración del PC, haga clic en **Importar > configuración del PC**. Puede aumentar el tamaño de este cuadro si oculta el cuadro de la configuración en ejecución.

## Combinar con la configuración en ejecución

Si desea combinar los cambios realizados en el cuadro de edición de configuración con la configuración en ejecución del router, haga clic en **Combinar con configuración en ejecución**. Los cambios se envían al router y surten efecto tan pronto como son recibidos.

## Sustituir la configuración en ejecución

Si desea sustituir la configuración en ejecución por el contenido del cuadro de edición de configuración, haga clic en **Sustituir configuración en ejecución**. No debe utilizar este botón a menos que haya rellenado el cuadro de edición de configuración con una configuración importada y editada desde el router, o con una configuración importada desde el PC.

## Restablecer

Si ha guardado la configuración en ejecución antes de utilizar el editor de configuración, podrá restablecerla en el router mediante este botón. La configuración restablecida se copia en la configuración de inicio del router y éste se carga de nuevo. Si no existe una copia de seguridad de la configuración del router, Cisco SDM muestra un mensaje que indica que no se puede restablecer la configuración.

# Restablecer los valores por defecto de fábrica

Es posible restablecer la configuración del router a los valores por defecto de fábrica y guardar la configuración en ejecución en un archivo que se podrá utilizar más adelante. Si ha cambiado el valor de fábrica 10.10.10.1 de la dirección IP de la LAN del router, perderá la conexión entre el router y el PC dado que dicha dirección IP volverá al valor 10.10.10.1 al restablecer la configuración.



### Nota

- La función Restablecer los valores por defecto de fábrica del router no se admite en los routers de las series 3620, 3640, 3640A y 7000 de Cisco.
- La función Restablecer los valores por defecto de fábrica no se admite si ejecuta una copia de Cisco SDM instalada en el PC.

Restablecer los valores por defecto de fábrica

Antes de comenzar, debe comprender cómo asignar al PC una dirección IP estática en la subred 10.10.10.0 para poder reconectarse al router tras su restablecimiento. La configuración de fábrica no incluye ninguna configuración de servidor DHCP en el router y este último no asignará ninguna dirección IP al PC. Además, la configuración de fábrica limita el acceso HTTP o HTTPS al router; queda restringido a la interfaz LAN y sólo desde la subred interna definida en esta interfaz. Después de acceder al router, puede cambiar la dirección IP por defecto y permitir el acceso remoto.

**Información sobre cómo asignar al PC una dirección IP dinámica o estática después del restablecimiento**

Si desea utilizar Cisco SDM después del restablecimiento, debe asignar al PC una dirección IP estática o dinámica, en función del tipo de router del que dispone. Utilice la tabla siguiente para determinar el tipo de dirección que debe asignarse al PC.

<b>Routers que necesitan direcciones dinámicas</b>	<b>Routers que necesitan direcciones estáticas</b>
SB10x Cisco 83x, 85x y 87x Cisco 1701, 1710 y 171x Cisco 180x y 181x	Cisco 1721, 1751, y 1760 Cisco 1841 Cisco 2600XM, y 2691 Cisco 28xx, 36xx, 37xx, y 38xx

El proceso para asignar al PC una dirección IP estática o dinámica varía ligeramente en función de la versión de Microsoft Windows que se ejecute en el PC.



**Nota**

No vuelva a configurar el PC hasta después de restablecer el router.



### Microsoft Windows NT

En el Panel de control, haga doble clic en el icono **Red** para que aparezca la ventana Red. Haga clic en **Protocolos**, seleccione la primera entrada de Protocolo TCP/IP y haga clic en **Propiedades**. En la ventana Propiedades, seleccione el adaptador de Ethernet que se utiliza para esta conexión. Haga clic en **Obtener una dirección IP automáticamente** para obtener una dirección IP dinámica. Para especificar una dirección IP estática, haga clic en **Especifique una dirección IP**. Especifique la dirección IP 10.10.10.2 o cualquier otra dirección en la subred 10.10.10.0 mayor que 10.10.10.1. Especifique la subred 255.255.255.248. Haga clic en **Aceptar**.

### Microsoft Windows 98 y Microsoft Windows ME

En el Panel de control, haga doble clic en el icono **Red** para que aparezca la ventana Red. Haga doble clic en la entrada Protocolo TCP/IP con el adaptador de red que se utiliza para esta conexión para mostrar las **Propiedades** de TCP/IP. En la ficha de dirección IP, haga clic en **Obtener una dirección IP automáticamente** para obtener una dirección IP dinámica. Para especificar una dirección IP estática, haga clic en **Especifique una dirección IP**. Especifique la dirección IP 10.10.10.2 o cualquier otra dirección en la subred 10.10.10.0 mayor que 10.10.10.1. Especifique la subred 255.255.255.248. Haga clic en **Aceptar**.

### Microsoft Windows 2000

En el Panel de control, seleccione **Conexiones de red y de acceso telefónico/Conexiones de área local**. Seleccione el adaptador Ethernet en el campo Conectar usando. Seleccione Protocolo Internet y haga clic en Propiedades. Haga clic en **Obtener una dirección IP automáticamente** para obtener una dirección IP dinámica. Para especificar una dirección IP estática, haga clic en **Especifique una dirección IP**. Especifique la dirección IP 10.10.10.2 o cualquier otra dirección en la subred 10.10.10.0 mayor que 10.10.10.1. Especifique la subred 255.255.255.248. Haga clic en **Aceptar**.

### Microsoft Windows XP

Haga clic en **Inicio**, seleccione **Configuración, Conexiones de red** y, a continuación, seleccione la conexión LAN que se utilizará. Haga clic en **Propiedades**, seleccione **Protocolo Internet TCP/IP** y haga clic en el botón **Propiedades**. Haga clic en **Obtener una dirección IP automáticamente** para obtener una dirección IP dinámica. Para especificar una dirección IP estática, haga clic en **Especifique una dirección IP**. Especifique la dirección IP 10.10.10.2 o cualquier otra dirección en la subred 10.10.10.0 mayor que 10.10.10.1. Especifique la subred 255.255.255.248. Haga clic en **Aceptar**.

## Para restablecer el router a los valores por defecto de fábrica:

- 
- Paso 1** En el **Paso 1** de la pantalla, deje activada la opción **Guardar configuración en ejecución en el PC**, y especifique un nombre para el archivo de configuración. Cisco SDM proporciona una ruta de acceso y nombre por defecto. No es necesario cambiarlo si no lo desea.
  - Paso 2** Revise la información del cuadro Información acerca de cómo volver a establecer la conexión del **Paso 2** en pantalla para que pueda establecer una conexión al router después del restablecimiento. En el caso necesario, revise la información en **Información sobre cómo asignar al PC una dirección IP dinámica o estática después del restablecimiento**.
  - Paso 3** Haga clic en **Restablecer el router**.
  - Paso 4** Haga clic en **Sí** para confirmar la operación de restablecimiento.
  - Paso 5** Siga el procedimiento que se indica en el cuadro Información acerca de cómo volver a establecer la conexión del **Paso 2** para conectarse de nuevo.
- 

Al restablecer el router con la configuración por defecto de fábrica, se cambia la dirección IP de la interfaz interna del router en 10.10.10.1. La próxima vez que inicie sesión en el router con el explorador, especifique la dirección IP 10.10.10.1 en el campo de ubicación del explorador.

## Esta función no se admite

Esta ventana aparece cuando una función de Cisco SDM no se admite. Esto puede deberse a que el router esté ejecutando una imagen de Cisco IOS que no admite la función o porque Cisco SDM se está ejecutando en un PC y no admite la función.



# CAPÍTULO 37

## Información adicional acerca de...

---

Los temas que se proporcionan en este apartado ofrecen información adicional acerca de los asuntos incluidos en la ayuda en línea de Cisco SDM.

### Direcciones IP y máscaras de subred

En este tema se proporciona información adicional acerca de las direcciones IP y las máscaras de subred, y se muestra cómo utilizarla cuando se especifican direcciones y máscaras en Cisco SDM.

Las direcciones IP de versión 4 tienen una longitud de 32 bits o 4 bytes. Este “espacio” en la dirección se utiliza para designar los elementos siguientes:

- Número de red
- Número de subred opcional
- Un número de host



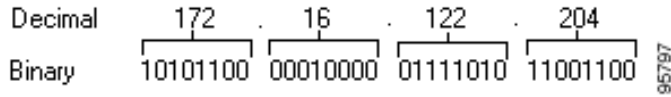
**Nota**

---

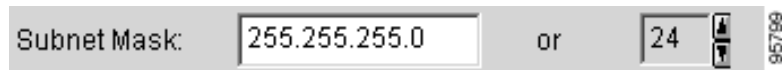
Cisco SDM no admite direcciones IP versión 6.

---

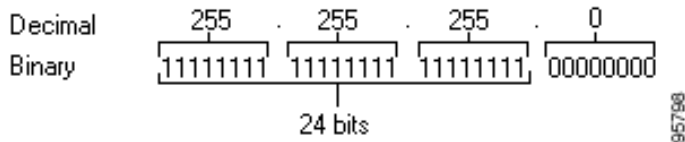
Cisco SDM requiere la introducción de direcciones IP en formato de decimales con puntos. Este formato facilita la lectura y gestión de las direcciones al agrupar los 32 bits en 4 octetos que se muestran en forma de decimales separados por puntos, por ejemplo 172.16.122.204. La dirección en decimales 172.16.122.204 representa la dirección IP binaria que se muestra en la figura siguiente.



La **máscara de subred** se emplea para especificar cuántos de los 32 bits que se utilizan para el número de red y, si se usan subredes, el número de subred. Se trata de una máscara binaria con 1 bit en cada posición que utilizan los números de red y de subred. Al igual que la dirección IP, se trata de un valor de 32 bits expresado en formato de decimales. La siguiente figura muestra una máscara de subred especificada en Cisco SDM. Cisco SDM Esta aplicación muestra la máscara de subred y el número equivalente de bits en la máscara.

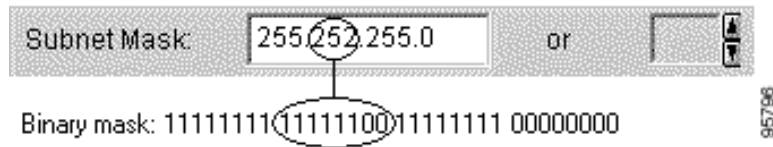


Estos valores especificados en Cisco SDM representan la máscara binaria que se muestra en la figura siguiente:



Esta máscara de subred especifica que los primeros 24 bits de la dirección IP representan el número de red y la máscara de subred, y que los últimos 8 bits corresponden al número de host dentro de dicha red y subred. La máscara puede especificarse en formato de decimales con puntos tal como se muestra en el campo Máscara de subred, o puede seleccionar el número de bits en el campo Bits. Al especificar o seleccionar un valor en un campo, Cisco SDM ajusta el otro automáticamente.

Si especifica una máscara en decimales que resulta en ceros (0) binarios en el área de red o subred de la máscara, Cisco SDM muestra una ventana de advertencia. El campo de máscara de subred siguiente contiene un valor decimal que resultará en ceros binarios en la parte del número de red o subred de la máscara. Observe que el campo de bits situado a la derecha está vacío, lo que indica que se ha especificado un valor no válido en el campo Máscara de subred.



Cuando se muestra una dirección de red en las ventanas de Cisco SDM, es posible que su dirección IP y máscara de subred aparezcan en formato de bits de dirección de red o subred, como se indica en el ejemplo siguiente:

172.28.33.0/24

La dirección de red en este ejemplo es 172.28.33.0. El número 24 indica el número de bits de subred utilizados. Puede considerarla como la abreviatura de la máscara de subred correspondiente 255.255.255.0.

Las direcciones que se utilizan en Internet deben ser exclusivas durante el período de tiempo que estén en uso. En las redes privadas, las direcciones pueden ser exclusivas solamente para la red o subred privada.

Las direcciones también se pueden traducir mediante esquemas como, por ejemplo, [NAT](#) y [PAT](#), y asignarse temporalmente mediante [DHCP](#). Asimismo, puede utilizar Cisco SDM para configurar NAT, PAT y DHCP.

## Campos de host y red

Este tema explica cómo proporcionar información de host o red en las ventanas que permiten especificar una dirección de red o host o un nombre de host.

Especifique la red o el host.

### Tipo

Uno de los siguientes:

- **Una red:** si selecciona esta opción, proporcione una dirección de red en el campo Dirección IP. Tenga en cuenta que la máscara inversa permite especificar un número de red que puede indicar varias subredes.
- **Un nombre de host o dirección IP:** si selecciona esta opción, proporcione una dirección IP o nombre de host en el campo siguiente.
- **Cualquier dirección IP:** la acción especificada se aplica a cualquier host o red.

**Dirección IP/Máscara comodín**

Especifique una dirección de red y, a continuación, la máscara inversa para indicar qué porción de la dirección de red debe coincidir exactamente.

Por ejemplo, si especifica una dirección de red 10.25.29.0 y una máscara inversa 0.0.0.255, se filtrará cualquier subprograma Java con una dirección de origen que contenga 10.25.29. Si la máscara inversa es 0.0.255.255, se filtrará cualquier subprograma Java con una dirección de origen que contenga 10.25.

**Nombre de host/IP**

Este campo aparece si selecciona **Un nombre de host o dirección IP** en Tipo. Si especifica un nombre de host, asegúrese de que la red dispone de un servidor DNS capaz de resolver el nombre de host a una dirección IP.

# Configuraciones de interfaz disponibles

Los tipos de configuraciones disponibles para cada tipo de interfaz se indican en la tabla siguiente.

Si ha seleccionado:	Puede agregar los elementos siguientes:
Una interfaz Ethernet	<ul style="list-style-type: none"> <li>• Conexión PPPoE</li> <li>• Interfaz de túnel</li> <li>• Interfaz de retrobucle</li> </ul>
Cualquiera de los elementos siguientes: <ul style="list-style-type: none"> <li>• Ethernet con una conexión PPPoE</li> <li>• Interfaz de marcación asociada con una configuración ADSL o G.SHDSL</li> <li>• Interfaz de serie con una configuración PPP o HDLC</li> <li>• Subinterfaz de serie con una configuración Frame Relay</li> <li>• Interfaz WAN no compatible</li> </ul>	<ul style="list-style-type: none"> <li>• Interfaz de túnel</li> <li>• Interfaz de retrobucle</li> </ul>

Interfaz ATM sin ninguna encapsulación	<ul style="list-style-type: none"> <li>• Interfaz ADSL</li> <li>• Interfaz G.SHDSL</li> <li>• Túnel o retrobucle para cualquiera de los elementos anteriores</li> </ul>
Interfaz de serie	<ul style="list-style-type: none"> <li>• Conexión Frame Relay</li> <li>• Conexión PPP</li> <li>• Interfaz de túnel</li> <li>• Interfaz de retrobucle</li> </ul>
Subinterfaz ATM	<ul style="list-style-type: none"> <li>• Interfaz de túnel</li> </ul>
Subinterfaz Ethernet	<ul style="list-style-type: none"> <li>• Interfaz de retrobucle</li> </ul>
Interfaz de marcación no asociada con una interfaz ATM	
Retrobucle	
Túnel	

## Conjuntos de direcciones DHCP

Las direcciones IP que el servidor DHCP asigna se obtienen de un conjunto común que se ha configurado mediante la especificación de las direcciones IP inicial y final del intervalo.

El intervalo de direcciones que especifique debe incluirse dentro de los intervalos de direcciones privadas siguientes:

- de 10.1.1.1 a 10.255.255.255
- de 172.16.1.1 a 172.31.255.255

El intervalo de direcciones que especifique también debe incluirse dentro de la misma subred que la de la dirección IP de la interfaz LAN, y puede representar un máximo de 254 direcciones. Los ejemplos siguientes son intervalos válidos:

- de 10.1.1.1 a 10.1.1.254 (suponiendo que la dirección IP de la LAN se encuentra en la subred 10.1.1.0)
- de 172.16.1.1 a 172.16.1.254 (suponiendo que la dirección IP de la LAN se encuentra en la subred 172.16.1.0)

Cisco SDM configura el router para que excluya automáticamente la dirección IP de la interfaz LAN del conjunto.

**Direcciones reservadas**

No debe utilizar las direcciones siguientes en el intervalo de direcciones que especifique:

- La dirección IP de la red o subred
- La dirección de difusión en la red

## Significados de las palabras clave “permit” y “deny”

Las entradas de regla pueden utilizarse en las reglas de acceso, NAT e IPSec, y en reglas de acceso asociadas con mapas de ruta. Las palabras “permit” y “deny” tienen distintos significados en función del tipo de regla que las utiliza.

Tipo de regla	Significado de “permit”	Significado de “deny”
Regla de acceso	Permitir que el tráfico entre o salga por la interfaz si coincide con la regla que se ha aplicado a dicha interfaz.	Abandonar el tráfico que coincida.
Regla NAT	Traducir la dirección IP de tráfico que coincida con la dirección <b>local interna</b> o <b>local exterior</b> especificadas.	No traducir la dirección.
regla IPSec (sólo en modo ampliado)	Cifrar el tráfico entre direcciones que coincidan.	No cifrar el tráfico. Permitir que se envíe sin cifrar.
Regla de acceso que se utiliza en el mapa de ruta	Proteger las direcciones que coincidan contra el mecanismo NAT.	No proteger las direcciones que coincidan contra el mecanismo NAT.



# Servicios y puertos

Este tema proporciona una lista de los servicios que se pueden especificar en las reglas y sus números de puerto correspondientes. También ofrece una breve descripción de cada servicio.

Se divide en las secciones siguientes:

- [Servicios TCP](#)
- [Servicios UDP](#)
- [Tipos de mensajes ICMP](#)
- [Servicios IP](#)
- [Servicios que se pueden especificar en las reglas de inspección](#)

## Servicios TCP

Servicio TCP	Número de puerto	Descripción
bgp	179	Border Gateway Protocol (BGP) intercambia la información de capacidad de alcance con otros sistemas que utilizan este protocolo.
chargen	19	Generador de caracteres.
cmd	514	Comandos remotos. Similar a exec, salvo que cmd dispone de autenticación automática.
daytime	13	Hora de día.
discard	9	Descartar.
domain	53	DNS (Domain Name Service). El sistema que se utiliza en Internet para convertir nombres de nodos de red en direcciones.
echo	7	Solicitud de eco. El mensaje que se envía al emitir el comando ping.
exec	512	Ejecución del proceso remoto.
finger	79	Finger. Aplicación que determina si un usuario dispone de una cuenta en un sitio de Internet específico.

Servicio TCP	Número de puerto	Descripción
ftp	21	File Transfer Protocol (Protocolo de transferencia de archivos). Protocolo de nivel de aplicación que se utiliza para transferir archivos entre nodos de red.
ftp-data	20	Conexiones de datos FTP.
gopher	70	Gopher. Sistema de entrega de documentos distribuidos.
hostname	101	Servidor de nombre de host NIC.
ident	113	Protocolo de identificación.
irc	194	IRC (Internet Relay Chat). Protocolo mundial que permite a los usuarios intercambiar mensajes de texto en tiempo real.
klogin	543	Inicio de sesión Kerberos. Se trata de un estándar en desarrollo para la autenticación de usuarios de red.
kshell	544	Intérprete de comandos Kerberos.
login	513	Inicio de sesión.
lpd	515	LPD (Line Printer Daemon). Protocolo que se utiliza para enviar trabajos de impresión entre sistemas UNIX.
nntp	119	NNTP (Network News Transport Protocol).
pim-auto-rp	496	PIM Auto-RP (Protocol-Independent Multicast Auto-RP). Se trata de una arquitectura de enrutamiento de multidifusión que permite la adición de enrutamiento IP de multidifusión en redes IP existentes.
pop2	109	POP2 (Post Office Protocol v2). Protocolo que utilizan las aplicaciones cliente de correo electrónico para recuperar correo de servidores de correo.
pop3	110	POP3 (Post Office Protocol v3).
smtp	25	SMTP (Protocolo simple de transferencia de correo). Protocolo de Internet que proporciona servicios de correo electrónico.
sunrpc	111	SUN RPC (SUN Remote Procedure Call). Consulte <a href="#">rpc</a> .
syslog	514	Registro del sistema.

## Servicios UDP

Servicio UDP	Número de puerto	Descripción
biff	512	Utilizado por el sistema de correo para avisar a los usuarios que han recibido correo nuevo.
bootpc	69	Cliente BOOTP (Bootstrap Protocol).
bootps	67	Servidor BOOTP (Bootstrap Protocol).
discard	9	Descartar.
dnsix	195	Auditoría del protocolo de seguridad DNSIX.
domain	53	DNS (Domain Name Service).
echo	7	Consulte <a href="#">echo</a> .
isakmp	500	ISAKMP (Internet Security Association and Key Management Protocol).
mobile-ip	434	Registro de IP móvil.
nameserver	42	Servicio de nombres IEN116 (obsoleto).
netbios-dgm	138	Servicio de datagramas de NetBios. Sistema de entrada y salida básicas de red. Una API que las aplicaciones utilizan para solicitar servicios de procesos de red de menor nivel.
netbios-ns	137	Servicio de nombres de NetBios.
netbios-ss	139	Servicio de sesiones de NetBios.
ntp	123	Network Time Protocol (Protocolo de hora de red). Este protocolo garantiza el mantenimiento exacto local de la hora con referencia a relojes de radio y atómicos situados en Internet.
pim-auto-rp	496	PIM (Protocol Independent Multicast), desbordamiento de ruta de acceso inversa, modo denso.
rip	520	Routing Information Protocol (Protocolo de información de enrutamiento). Protocolo que se utiliza para intercambiar información de ruta entre routers.
snmp	161	Simple Network Management Protocol (Protocolo simple de gestión de redes). Protocolo que se utiliza para supervisar y controlar los dispositivos de red.

Servicio UDP	Número de puerto	Descripción
snmptrap	162	Interrupciones SNMP. Notificación de gestión del sistema de un evento que se ha producido en un sistema gestionado de manera remota.
sunrpc	111	SUN RPC (SUN Remote Procedure Call). Las RPC (Remote Procedure Call) son llamadas de procedimiento creadas o especificadas por los clientes y ejecutadas en los servidores, cuyos resultados se devuelven al cliente a través de la red.
syslog	514	Servicio de registros del sistema.
tacacs	49	TACACS (Terminal Access Controller Access Control System). Protocolo de autenticación que proporciona autenticación de acceso remoto y servicios relacionados como, por ejemplo, el inicio de sesión.
talk	517	Talk. Protocolo cuya intención original era la comunicación entre terminales de teletipo, pero que ahora se ha convertido en un puerto de reunión a partir del cual se puede establecer una conexión TCP.
tftp	69	Trivial File Transfer Protocol (Protocolo trivial de transferencia de archivos). Versión simplificada de FTP que permite la transferencia de archivos entre nodos de red.
time	37	Hora.
who	513	Puerto hacia las bases de datos que muestra quién ha iniciado sesión en las máquinas de una red local y el promedio de carga de la máquina.
xdmcp	177	X-DMCP (X-Display Manager Client Protocol). Protocolo que se utiliza para la comunicación entre clientes y administradores X-Display.
non500-isakmp	4500	ISAKMP (Internet Security Association and Key Management Protocol). Esta palabra clave se utiliza cuando se requiere la flotación de puertos de NAT transversal.

## Tipos de mensajes ICMP

Mensajes ICMP	Número de puerto	Descripción
alternate-address	6	Dirección de host alternativa.
conversion-error	31	Se envía para indicar un error de conversión de datagramas.
echo	8	Tipo de mensaje que se envía al emitir el comando ping.
echo-reply	0	Respuesta a un mensaje de solicitud de eco (ping).
information-reply	16	Obsoleto. Respuesta a un mensaje enviado por el host para descubrir el número de la red en la que se encuentra. Sustituido por DHCP.
information-request	15	Obsoleto. Mensaje enviado por el host para descubrir el número de la red en la que se encuentra. Sustituido por DHCP.
mask-reply	18	Respuesta a un mensaje enviado por el host para descubrir la máscara de red de la red en la que se encuentra.
mask-request	17	Obsoleto. Mensaje enviado por el host para descubrir la máscara de red de la red en la que se encuentra.
mobile-redirect	32	Redireccionamiento de host móvil. Se envía para notificar a un host móvil de un mejor nodo de primer salto en la ruta de acceso a un destino.
parameter-problem	12	Mensaje que se genera en respuesta a un paquete con un problema en el encabezado.
redirect	5	Se envía para notificar a un host de un mejor nodo de primer salto en la ruta de acceso a un destino.
router-advertisement	9	Se envía periódicamente o en respuesta a una solicitud de router.
router-solicitation	10	Mensajes que se envían para solicitar a los routers que generen rápidamente mensajes de anuncios de router.
source-quench	4	Se envía cuando no hay espacio de búfer suficiente como para poner en cola los paquetes para la transmisión al próximo salto (next hop) o por el router de destino cuando los paquetes llegan demasiado rápido para su procesamiento.

Servicios y puertos

Mensajes ICMP	Número de puerto	Descripción
time-exceeded	11	Se envía para indicar que el campo de tiempo de vida de los paquetes recibidos ha alcanzado cero.
timestamp-reply	14	Respuesta a una solicitud de marcador de hora que se utiliza para la sincronización entre dos dispositivos.
timestamp-request	13	Solicitud de marcador de hora que se utiliza para la sincronización entre dos dispositivos.
traceroute	30	Mensaje que se envía en respuesta a un host que ha emitido una solicitud de traceroute.
unreachable	3	Destino inalcanzable. El paquete no se puede transmitir por motivos distintos de la congestión.

Servicios IP

Servicios IP	Número de puerto	Descripción
aahp	51	
eigrp	88	Enhanced Interior Gateway Routing Protocol (Protocolo mejorado de enrutamiento de gateway interior). Versión avanzada de IGRP desarrollado por Cisco.
esp	50	Procesador de servicios ampliados.
icmp	1	Internet Control Message Protocol (Protocolo de mensajes de control por Internet). Protocolo de nivel de red que informa sobre los errores y proporciona otros datos pertinentes al procesamiento de paquetes IP.
igmp	2	Internet Group Management Protocol (Protocolo de administración de grupos de Internet). Utilizado por los hosts IP para informar su pertenencia a grupos de multidifusión a los routers de multidifusión adyacentes.
ip	0	Protocolo de Internet. Protocolo de nivel de red que ofrece servicio de interred sin conexiones.
ipinip	4	Encapsulación IP en IP.
nos	94	NOS (Network Operating System). Protocolo de sistemas de archivos distribuidos.

Servicios IP	Número de puerto	Descripción
ospf	89	Open Shortest Path First (Abrir la ruta más corta en primer lugar). Algoritmo de enrutamiento jerárquico de estado de enlace.
pcp	108	PCP (Payload Compression Protocol).
pim	103	PIM (Protocol-Independent Multicast). Se trata de una arquitectura de enrutamiento de multidifusión que permite la adición de enrutamiento IP de multidifusión en redes IP existentes.
tcp	6	Transmission Control Protocol (Protocolo de control de transmisión). Protocolo de nivel de transporte orientado hacia la conexión que proporciona una transmisión dúplex de datos fiable.
udp	17	User Datagram Protocol (Protocolo de datagrama de usuario). Protocolo de nivel de transporte sin conexiones en la pila de protocolo TCP/IP.

### Servicios que se pueden especificar en las reglas de inspección

Protocolo	Descripción
cuseeme	Protocolo de videoconferencia.
fragment	Especifica que la regla debe realizar una inspección por fragmentos.
ftp	Consulte <a href="#">ftp</a> .
h323	Consulte <a href="#">H.323</a> .
http	Consulte <a href="#">HTTP</a> .
icmp	Consulte <a href="#">icmp</a> .
netshow	NetShow. de flujo de vídeo.
remd	RCMD (Remote Comman d). Protocolo que se utiliza cuando un sistema local ejecuta comandos en un sistema remoto.
realaudio	RealAudio. Protocolo de flujo de audio.

Protocolo	Descripción
rpc	RPC (Remote Procedure Call). Las RPC son llamadas de procedimiento creadas o especificadas por los clientes y ejecutadas en los servidores, cuyos resultados se devuelven al cliente a través de la red.
rtsp	RTSP (Real-Time Streaming Protocol). Protocolo de nivel de aplicación que se utiliza para controlar la transmisión de datos con propiedades de tiempo real.
sip	Session Initiation Protocol (Protocolo de inicio de sesión). Protocolo de telefonía que se utiliza para integrar servicios de telefonía y datos.
skinny	Protocolo de telefonía que permite que los clientes de telefonía cumplan la norma H.323.
smtp	Consulte <a href="#">smtp</a> .
sqlnet	Protocolo para las bases de datos con capacidad para red.
streamworks	Protocolo StreamWorks de flujo de vídeo.
tcp	Consulte <a href="#">tcp</a> .
tftp	Consulte <a href="#">tftp</a> .
udp	Consulte <a href="#">udp</a> .
vdolive	Protocolo VDOLive de flujo de vídeo.

## Información adicional acerca de NAT

Esta sección proporciona información de escenario que le puede ayudar a completar las ventanas de la regla de traducción NAT e información adicional que explica por qué las reglas NAT que se crean mediante CLI no se pueden modificar en Cisco SDM.

## Escenarios de traducción de direcciones estáticas

Los escenarios siguientes le muestran cómo puede utilizar la ventana de la regla de traducción de direcciones estáticas.



## Escenario 1

Necesita asignar una dirección IP para un único host a una dirección pública. La dirección del host es 10.12.12.3 y la dirección pública es 172.17.4.8.

La tabla siguiente muestra cómo se deberían usar los campos en la ventana Agregar regla de traducción de direcciones.

Estática/dinámica	Campos Traducir desde la interfaz		Campos Traducir a la interfaz	
	Dirección IP	Máscara de red	Dirección IP	Puerto de redireccionamiento
Estática	10.12.12.3	Dejar en blanco	172.17.4.8	Dejar sin marcar.

### Resultado

La dirección de origen 10.12.12.3 se traduce a la dirección 172.17.4.8 en los paquetes que salen del router. Si ésta es la única regla NAT para esta red, 10.12.12.3 es la única dirección de la red que se traduce.

## Escenario 2

Debe asignar cada dirección IP de una red a una dirección IP pública exclusiva y no desea crear una regla independiente para cada asignación. El número de red de origen es 10.12.12.0 y la red de destino es 172.17.4.0. Sin embargo, en este escenario no es necesario conocer los números de red de origen y de destino. Es suficiente con especificar las direcciones host y una máscara de red.

La tabla siguiente muestra cómo se deberían usar los campos en la ventana Agregar regla de traducción de direcciones.

Estática/dinámica	Campos Traducir desde la interfaz		Campos Traducir a la interfaz	
	Dirección IP	Máscara de red	Dirección IP	Puerto de redireccionamiento
Estática	10.12.12.35 (host)	255.255.255.0	172.17.4.8 (host)	Dejar sin marcar.

**Resultado**

NAT deriva la dirección de red de “Traducir desde” a partir de la dirección IP de host y la máscara de subred, y la dirección de red del campo “Traducir a” a partir de la máscara de red especificada en los campos “Traducir desde” y la dirección IP de “Traducir a”. La dirección IP de origen en todo paquete que sale de la red original se traduce a una dirección de la red 172.17.4.0.

**Escenario 3**

Desea utilizar la misma dirección IP global para varios hosts en una red fiable. El tráfico entrante tendrá un número de puerto diferente en función del host de destino.

La tabla siguiente muestra cómo se deberían usar los campos en la ventana Agregar regla de traducción de direcciones.

	Campos Traducir desde...		Campos Traducir a...	
	Dirección IP	Máscara de red	Dirección IP	Puerto de redireccionamiento
Estática/dinámica				
Estática	10.12.12.3	Dejar en blanco	172.17.4.8	UDP Puerto original 137 Puerto traducido 139

**Resultado**

La dirección de origen 10.12.12.3 se traduce a la dirección 172.17.4.8 en los paquetes que salen del router. El número de puerto del campo Puerto de redireccionamiento cambia de 137 a 139. El tráfico de vuelta que lleva la dirección de destino 172.17.4.8 se enruta al puerto número 137 del host con la dirección IP 10.12.12.3.

Necesita crear una entrada independiente para cada asignación de host/puerto que desee crear. Puede utilizar la misma dirección IP del campo “Traducir a” en cada entrada pero debe especificar una dirección IP “Traducir desde” en cada entrada y un conjunto distinto de números de puerto.

## Escenario 4

Desea que las direcciones de origen de “Traducir desde” utilicen la dirección IP asignada a la interfaz Fast Ethernet 0/1 172.17.4.8. También desea utilizar la misma dirección IP global para varios hosts en una red fiable. El tráfico entrante tendrá un número de puerto diferente en función del host de destino. En la tabla siguiente se muestra cómo se utilizarán los campos de la ventana Agregar regla de traducción de direcciones.

Estática/dinámica	Campos Traducir desde...		Campos Traducir a...	
	Dirección IP	Máscara de red	Dirección IP	Puerto de redireccionamiento
Estática	10.12.12.3	Dejar en blanco	FastEthernet 0/1	UDP Puerto original 137 Puerto traducido 139

### Resultado

La dirección de origen 10.12.12.3 se traduce a la dirección 172.17.4.8 en paquetes que salen del router. El número de puerto del campo Puerto de redireccionamiento cambia de 137 a 139. El tráfico de vuelta que lleva la dirección de destino 172.17.4.8 se enruta al puerto número 137 del host con la dirección IP 10.12.12.3.

## Escenarios de traducción de direcciones dinámicas

Los escenarios siguientes le muestran cómo puede utilizar las reglas de traducción de direcciones dinámicas. Estos escenarios se aplican independientemente de si selecciona las opciones De interna a externa o De externa a interna.

### Escenario 1

Desea que las direcciones de origen de “Traducir desde” utilicen la dirección IP asignada a la interfaz Fast Ethernet 0/1 172.17.4.8. La traducción de direcciones de puerto (PAT) se utilizará para distinguir el tráfico asociado con hosts distintos. La regla de la lista de control de acceso que se utiliza para definir las direcciones de “Traducir desde” se configura tal como se indica a continuación:

```
access-list 7 deny host 10.10.10.1
access-list 7 permit 10.10.10.0 0.0.0.255
```

Cuando se utiliza en una regla NAT, esta regla de acceso permitirá que cualquier host de la red 10.10.10.0, excepto el que tenga la dirección 10.10.10.1, reciba la traducción de direcciones.

La tabla siguiente muestra cómo se deberían usar los campos en la ventana Agregar regla de traducción de direcciones.

Estática/dinámica	Campos Traducir desde...	Campos Traducir a...		
	Regla de la lista de control de acceso	Tipo	Interfaz	Conjunto de direcciones
Dinámica	7	Interfaz	FastEthernet0/1	Desactivada

**Resultado**

La dirección IP de origen del tráfico de todos los hosts de la red 10.10.10.0 se traducirá a 172.17.4.8. Se utilizará PAT para distinguir el tráfico asociado con hosts distintos.

**Escenario 2**

Desea que las direcciones de host especificadas en el comando access-list 7 del escenario anterior utilicen las direcciones de un conjunto definido por el usuario. Si se utilizan todas las direcciones del conjunto, desea que el router utilice PAT para satisfacer solicitudes adicionales de direcciones del conjunto.

En la tabla siguiente se muestra cómo se utilizarán los campos de la ventana Conjunto de direcciones para este escenario.

Nombre del conjunto	Traducción de direcciones de puerto	Campos de Dirección IP		Máscara de red
Conjunto 1	Marcado	172.16.131.2	172.16.131.10	255.255.255.0

En la tabla siguiente se muestra cómo se utilizarán los campos de la ventana Agregar regla de traducción de direcciones para este escenario.

Estática/dinámica	Campos Traducir desde...	Campos Traducir a...		
	Regla de la lista de control de acceso	Tipo	Interfaz	Conjunto de direcciones
Dinámica	7	Conjunto de direcciones	Desactivada	Conjunto 1

**Resultado**

Las direcciones IP de host de la red 10.10.10.0 se traducen a la dirección IP en el intervalo 172.16.131.2 a 172.16.131.10. Cuando se presente un mayor número de solicitudes de traducción de direcciones que el número de direcciones disponibles en Conjunto 1, se utilizará la misma dirección para satisfacer las solicitudes subsiguientes y se recurrirá a PAT para distinguir entre los hosts que utilicen dicha dirección.

## Motivos por los cuales Cisco SDM no puede modificar una regla NAT

Una regla NAT previamente configurada será de sólo lectura y no se podrá configurar cuando una regla NAT estática se haya configurado con cualquiera de los elementos siguientes:

- Los comandos de IOS de Cisco **inside source static** y **destination**
- El comando **inside source static network** con una de las palabras clave “extendable” “no-alias” o “no-payload”
- El comando **outside source static network** con una de las palabras clave “extendable” “no-alias” o “no-payload”
- El comando **inside source static tcp** con una de las palabras clave “no-alias” o “no-payload”
- El comando **inside source static udp** con una de las palabras clave “no-alias” o “no-payload”
- El comando **outside source static tcp** con una de las palabras clave “no-alias” o “no-payload”

- El comando **outside source static udp** con una de las palabras clave “no-alias” o “no-payload”
- El comando **inside source static** con una de las palabras clave “no-alias”, “no-payload”, “extendable”, “redundancy”, “route-map” o “vrf”
- El comando **outside source static** con una de las palabras clave “no-alias”, “no-payload”, “extendable” o “add-route”
- El comando **inside source static** con la palabra clave “esp”
- El comando **inside source static** con el comando **interface**

Una regla dinámica NAT se configura con la interfaz de retrobucle

## Información adicional acerca de VPN

En estos temas se incluye información adicional acerca de VPN, DMVPN, IPSec e IKE.

## Recursos de Cisco.com

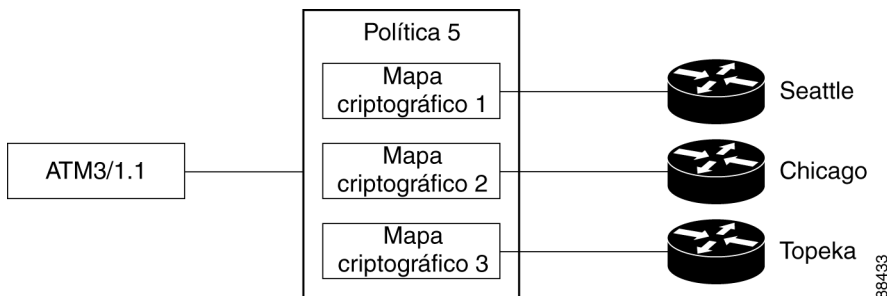
Los enlaces siguientes proporcionan recursos TAC e información adicional acerca de los temas relacionados con VPN.

- [How Virtual Private Networks Work \[Funcionamiento de VPN \(Virtual Private Network\)\]](#)
- [Dynamic Multipoint IPSec VPNs \(VPN IPSec multipunto dinámicas\)](#)
- [TAC-authored articles on IPSec \(Artículos sobre IPSec redactados por el servicio TAC\)](#)
- [TAC-authored articles on Cisco SDM \(Artículos sobre SDM redactados por el servicio TAC\)](#)
- [Security and VPN Devices \(Seguridad y dispositivos VPN\)](#)
- [IPSecurity Troubleshooting—Understanding and Using Debug Commands \(Solución de problemas de IPSec: comprensión y uso de comandos de depuración\)](#)
- [Field Notices \(Notas sobre productos\)](#)

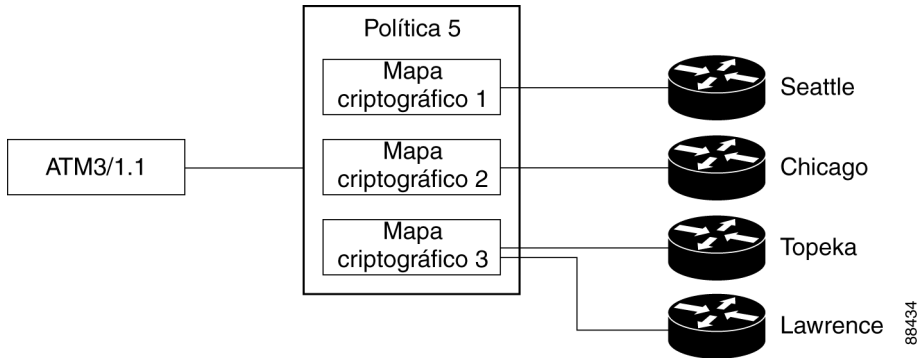
## Información adicional acerca de conexiones VPN y políticas IPsec

Una conexión VPN es una asociación entre una interfaz de router y una política IPsec. La base de una política IPsec es el mapa criptográfico, en el cual se especifican los elementos siguientes: un conjunto de transformación y otros parámetros que regirán el cifrado, la identidad de uno o varios homólogos y una regla IPsec que especifica el tráfico que se cifrará. Una política IPsec puede disponer de varios mapas criptográficos.

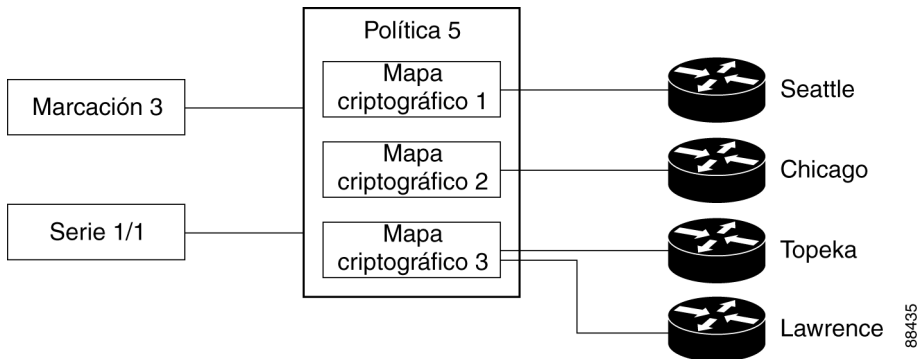
En el diagrama siguiente se muestra una interfaz (ATM 3/1.1) asociada con una política IPsec, la cual dispone de tres mapas criptográficos, cada uno de los cuales especifica un sistema de homólogos distinto. De este modo, la interfaz ATM 3/1.1 está asociada con tres conexiones VPN.



Un mapa criptográfico puede especificar más de un homólogo para una conexión. Esto se puede establecer con el fin de proporcionar redundancia. En el diagrama siguiente se muestra la misma interfaz y política, pero el mapa criptográfico CM-3 especifica dos homólogos: Topeka y Lawrence.



Una interfaz de router se puede asociar con una sola política IPsec. No obstante, una política IPsec se puede asociar con varias interfaces de router y un mapa criptográfico puede especificar más de un homólogo para una conexión. En el diagrama siguiente se muestran dos interfaces de router asociadas con la política y un mapa criptográfico que especifica dos homólogos.



Esta configuración dispone de seis conexiones VPN, ya que tanto la interfaz de marcación 3 y la interfaz de serie 1/1 poseen conexiones con Seattle, Chicago, Topeka y Lawrence. Cisco SDM mostrará los enlaces a Topeka y Lawrence como una conexión para ambas interfaces.



## Información adicional acerca de IKE

IKE se encarga de las tareas siguientes:

- [Autenticación](#)
- [Negociación de sesión](#)
- [Intercambio de claves](#)
- [Negociación y configuración de túneles IPsec](#)

### Autenticación

Sin duda, la autenticación es la tarea más importante que realiza IKE, y también la más complicada. Al realizar una negociación, es sumamente importante saber con quién se está efectuando la operación. IKE puede utilizar uno de varios métodos para autenticar las partes negociantes entre sí.

- **Clave previamente compartida.** IKE utiliza una técnica de hash para garantizar que únicamente un usuario que posee la misma clave puede haber enviado los paquetes IKE.
- **Firmas digitales DSS o RSA.** IKE utiliza criptografía de firma digital mediante clave pública para comprobar que cada usuario es quién dice ser.
- **Cifrado RSA.** IKE utiliza uno de dos métodos para cifrar una porción suficiente de la negociación con el fin de garantizar que solamente un usuario con la clave privada correcta podrá continuar con dicha operación.



#### Nota

---

Cisco SDM admite el método de autenticación de clave previamente compartida.

---

### Negociación de sesión

Durante la negociación de sesión, IKE permite que los usuarios negocien cómo realizarán la autenticación y cómo protegerán las negociaciones futuras (es decir, la negociación de túneles IPsec). Se negocian los elementos siguientes:

- **Método de autenticación.** Se trata de uno de los métodos de autenticación que se indican arriba.

- **Algoritmo de intercambio de claves.** Se trata de una técnica matemática para el intercambio seguro de claves criptográficas a través de un soporte público (es decir, Diffie-Hellman). Las claves se utilizan en los algoritmos de cifrado y firma de paquetes.
  - **Algoritmo de cifrado:** DES, 3DES o AES
  - **Algoritmo de firmas de paquete:** MD5 o SHA-1

## Intercambio de claves

IKE utiliza el método de intercambio de claves negociadas (consulte “Negociación de sesiones” arriba) para crear el número de bits suficiente de material de claves criptográficas para garantizar la seguridad de las transacciones futuras. Este método garantiza la protección de cada sesión IKE con un nuevo conjunto seguro de claves.

La autenticación, la negociación de sesiones y el intercambio de claves constituyen la primera fase de una negociación IKE.

## Negociación y configuración de túneles IPSec

Cuando se haya finalizado la negociación de un método seguro para el intercambio de información (fase 1), IKE se utiliza para negociar un túnel IPSec. Esta operación se realiza en la segunda fase de IKE. Durante este intercambio, IKE crea nuevo material de claves para que lo utilice el túnel IPSec (empleando las claves de la primera fase de IKE o realizando un nuevo intercambio de claves). También se negocian los algoritmos de cifrado y autenticación para este túnel.

## Información adicional acerca de las políticas IKE

Al iniciarse una negociación IKE, éste último busca una política IKE que sea igual en ambos homólogos. El homólogo que inicia la negociación enviará todas sus políticas al homólogo remoto y este último buscará una política correspondiente. Para ello, el homólogo remoto comparará su propia política de mayor prioridad con las políticas recibidas del otro homólogo. A continuación, comprobará cada una de sus políticas en el orden de prioridad (la de mayor prioridad en primer lugar) hasta que encuentre una que coincida.

Una coincidencia se establece cuando las dos políticas de ambos homólogos contienen los mismos valores de cifrado, hash, autenticación y parámetro Diffie-Hellman y cuando la política del homólogo remoto especifica una duración de actividad inferior o igual a la de la política que se está comparando. Si las duraciones no son idénticas, se utilizará la duración más corta de la política del homólogo remoto.

## Combinaciones de transformación permitidas

Para definir un conjunto de transformaciones, debe especificar entre una y tres transformaciones. Cada transformación especifica un protocolo de seguridad IPsec (**AH** o **ESP**), además del algoritmo que se desee utilizar. Cuando durante las negociaciones para las asociaciones de seguridad IPsec se utiliza el conjunto de transformaciones en particular, todo el conjunto de transformaciones (la combinación de protocolos, algoritmos y otros ajustes) debe coincidir con un conjunto de transformación en el homólogo remoto.

En la tabla siguiente se proporciona una lista de las selecciones aceptables de combinación de transformaciones para los protocolos AH y ESP.

<b>Transformación AH</b> <i>(Seleccionar un máximo de una)</i>	<b>Transformación de cifrado ESP</b> <i>(Seleccionar un máximo de una)</i>	<b>Transformación de autenticación</b> <i>(Seleccionar un máximo de una)</i>	<b>Transformación de compresión IP</b> <i>(Seleccionar un máximo de una)</i>	<b>Ejemplos</b> <i>(Se permite un total de tres transformaciones)</i>
ah-md5-hmac ah-sha-hmac	esp-des esp-3des esp-null es-aes-128 esp-aes-192 esp-aes-256 esp-seal	esp-md5-hmac esp-sha-hmac	comp-lzs	<ol style="list-style-type: none"> <li><b>1.</b> ah-md5-hmac</li> <li><b>2.</b> esp-3des y esp-md5-hmac</li> <li><b>3.</b> ah-sha-hmac, esp-des y esp-sha-hmac</li> </ol>

La tabla siguiente describe cada una de las transformaciones.

<b>Transformación</b>	<b>Descripción</b>
<b>ah-md5-hmac</b>	AH con el algoritmo de autenticación MD5 (variante HMAC).
<b>ah-sha-hmac</b>	AH con el algoritmo de autenticación SHA (variante HMAC).
esp-des	ESP con el algoritmo de cifrado DES de 56 bits.
esp-3des	ESP con el algoritmo de cifrado DES de 168 bits (3DES o Triple DES).
esp-null	Algoritmo de cifrado nulo.
esp-seal	ESP con el algoritmo de cifrado SEAL (Software Encryption Algorithm) de clave de cifrado de 160 bits.
esp-md5-hmac	ESP con el algoritmo de autenticación MD5 (variante HMAC).
es-aes-128	ESP con AES (Advanced Encryption Standard). Cifrado con una clave de 128 bits.
esp-aes-192	ESP con AES. Cifrado con una clave de 192 bits.
esp-aes-256	ESP con AES. Cifrado con una clave de 256 bits.
<b>esp-sha-hmac</b>	ESP con el algoritmo de autenticación SHA (variante HMAC).
comp-lzs	Compresión IP con el algoritmo LZS.

## Ejemplos

Los elementos siguientes son ejemplos de combinaciones de transformaciones permitidas:

- ah-md5-hmac
- esp-des
- esp-3des y esp-md5-hmac
- ah-sha-hmac, esp-des y esp-sha-hmac
- comp-lzs

# Motivos por los cuales una configuración de interfaz o subinterfaz de serie puede ser de sólo lectura

Una interfaz o subinterfaz de serie previamente configurada será de sólo lectura y no se podrá configurar en los casos siguientes:

- La interfaz se ha configurado con los comandos de Cisco IOS **encapsulation ppp** y **ppp multilink ...**.
- La interfaz se ha configurado con los comandos **encapsulation hdle** e **ip address negotiated**.
- La interfaz forma parte de un WIC SERIAL\_CSUDSU\_56K.
- La interfaz forma parte de un WIC síncrono/asíncrono configurado con el comando **physical-layer async**.
- La interfaz se ha configurado con el comando **encapsulation frame-relay** con una dirección IP en la interfaz principal.
- La encapsulación de la interfaz no es “hdlc”, “ppp” ni “frame-relay”.
- El comando **encapsulation frame-relay ...** contiene la opción **mfr ...**
- La interfaz se ha configurado con el comando **encapsulation ppp**, pero la configuración PPP contiene comandos incompatibles.
- La interfaz se ha configurado con los comandos **encapsulation frame-relay** y **frame-relay map ...**
- La interfaz principal se ha configurado con los comandos **encapsulation frame-relay** y **frame-relay interface-dlci ...**
- La interfaz principal se ha configurado con el comando **encapsulation frame-relay** y la subinterfaz se ha configurado con el comando **frame-relay priority-dlci-group ...**
- La subinterfaz se ha configurado con el comando **interface-dlci ...** que incluye cualquiera de las palabras clave “ppp”, “protocol”, o “switched”.
- La subinterfaz es de tipo “multipunto” en lugar de “punto a punto”.
- La subinterfaz se ha configurado con una encapsulación que no es “frame-relay”.

# Motivos por los cuales una configuración de interfaz o subinterfaz ATM puede ser de sólo lectura

Una interfaz o subinterfaz ATM previamente configurada será de sólo lectura y no se podrá configurar en los casos siguientes:

- Contiene un **PVC** con el comando **dialer pool-member**.
- Contiene un PVC en el que el protocolo especificado en el comando **protocol** no es un protocolo **ip**.
- Contiene un PVC con varios comandos **protocol ip**.
- La encapsulación del PVC no es “aal5mux” ni “aal5snap”.
- Si el protocolo de encapsulación en aal5mux no es “ip”.
- Si la dirección IP no se ha configurado en el PVC en el comando **protocol ip**.
- Si la opción de “marcación a petición” se ha configurado en el comando **pppoe-client**.
- Si se ha configurado más de un PVC en la interfaz.
- Si la encapsulación de la marcación asociada está en blanco o no es “ppp”.
- Si no se ha configurado ninguna dirección IP en la marcación asociada.
- Si se requiere **VPDN** (lo que se determina dinámicamente desde la imagen de IOS de Cisco) pero no está configurado para esta conexión.
- Si el modo operativo es “CO” en una interfaz SHDSL (solamente interfaces ATM principales).
- Si no se ha configurado ninguna dirección IP en la interfaz y esta última no se ha configurado para PPPoE (solamente subinterfaces ATM).
- La interfaz dispone de una dirección IP pero ningún PVC asociado.
- La interfaz dispone de un PVC pero ninguna dirección IP, y no se ha configurado para PPPoE.
- Se ha configurado el comando **bridge-group** en la interfaz.
- Si la interfaz principal dispone de uno o más PVC, además de una o más subinterfaces.
- Si la interfaz principal no se puede configurar (solamente subinterfaces ATM).
- Se trata de una interfaz multipunto (solamente subinterfaces ATM).

## Motivos por los cuales una configuración de interfaz Ethernet puede ser de sólo lectura

Una interfaz LAN o WAN previamente configurada será de sólo lectura y no se podrá configurar en los casos siguientes:

- Si la interfaz LAN se ha configurado como un servidor DHCP y con una dirección IP auxiliar.

## Motivos por los cuales una configuración de interfaz ISDN (RDSI) BRI puede ser de sólo lectura

Una interfaz ISDN (RDSI) BRI previamente configurada será de sólo lectura y no se podrá configurar en los casos siguientes:

- Se ha asignado una dirección IP a la interfaz ISDN (RDSI) BRI.
- Se ha configurado una encapsulación distinta de ppp en la interfaz ISDN (RDSI) BRI.
- Se ha configurado el comando **dialer-group** o **dialer string** en la interfaz ISDN (RDSI) BRI.
- Se ha configurado el comando **dialer pool-member <x>** en la interfaz ISDN (RDSI) BRI, pero no está presente la interfaz de marcación <x> correspondiente.
- Se han configurado varios miembros del conjunto de marcación en la interfaz ISDN (RDSI) BRI.
- Se ha configurado el comando **dialer map** en la interfaz ISDN (RDSI) BRI.
- Se ha configurado una encapsulación distinta de ppp en la interfaz de marcación.
- El comando **dialer-group** o el **dialer-pool** no se ha configurado en la interfaz de marcación.
- Se ha configurado el comando **dialer-group <x>** en la interfaz de marcación, pero no se ha configurado el comando **dialer -list <x> protocol** correspondiente.

- Se ha configurado el comando **dialer idle-timeout** <num> con una palabra clave opcional (either/inbound) en la interfaz de marcación.
- Se ha configurado el comando **dialer string** con la palabra clave opcional **class** en la interfaz de marcación.
- Al utilizar la conexión ISDN (RDSI) BRI como conexión de reserva, una vez que la configuración de reserva se realiza a través de Cisco SDM, si se produce cualquiera de las condiciones siguientes, dicha conexión se mostrará como de sólo lectura:
  - Se quita la ruta por defecto a través de la interfaz principal
  - No se ha configurado la ruta por defecto de la interfaz de reserva
  - Se quita la política local de IP
  - No se han configurado los comandos **track /rtr** o **both**
  - Se quita el mapa de ruta
  - Se quita o modifica la lista de acceso (por ejemplo, se modifica la dirección IP de seguimiento)
  - Las interfaces compatibles con Cisco SDM se configuran con configuraciones incompatibles
  - Las interfaces principales no son compatibles con Cisco SDM

## Motivos por los cuales una configuración de interfaz de módem analógico puede ser de sólo lectura

Una interfaz de módem analógico previamente configurada será de sólo lectura y no se podrá configurar en los casos siguientes:

- Se ha asignado una dirección IP a la interfaz asíncrona.
- Se ha configurado una encapsulación distinta de ppp en la interfaz asíncrona.
- Se ha configurado el comando **dialer-group** o **dialer string** en la interfaz asíncrona.
- Se ha configurado el modo asíncrono **interactive** en la interfaz asíncrona.
- Se ha configurado el comando **dialer pool-member** <x> en la interfaz asíncrona, pero no está presente la interfaz de marcación <x> correspondiente.



- Se han configurado varios miembros del conjunto de marcación en la interfaz asíncrona.
- Se ha configurado una encapsulación distinta de ppp en la interfaz de marcación.
- El comando **dialer-group** o el **dialer-pool** no se ha configurado en la interfaz de marcación.
- Se ha configurado el comando **dialer-group <x>** en la interfaz de marcación, pero no se ha configurado el comando **dialer -list <x> protocol** correspondiente.
- Se ha configurado el comando **dialer idle-timeout <num>** con una palabra clave opcional (*either/inbound*) en la interfaz de marcación.
- En el modo de colección de configuración de línea, no se ha configurado el comando **modem inout**.
- En el modo de colección de configuración de línea, no se ha configurado el comando **autoselect ppp**.
- Al utilizar la conexión de módem analógico como conexión de reserva, una vez que la configuración de reserva se realiza a través de Cisco SDM, si se produce cualquiera de las condiciones siguientes, la conexión de reserva se mostrará como de sólo lectura:
  - Se quita la ruta por defecto a través de la interfaz principal
  - No se ha configurado la ruta por defecto de la interfaz de reserva
  - Se quita la política local de IP
  - No se han configurado los comandos **track /rtr** o **both**
  - Se quita el mapa de ruta
  - Se quita o modifica la lista de acceso (por ejemplo, se modifica la dirección IP de seguimiento)
  - Las interfaces compatibles con Cisco SDM se configuran con configuraciones incompatibles
  - Las interfaces principales no son compatibles con Cisco SDM

# Escenario de utilización de políticas de firewall

Para obtener información acerca de la gestión de políticas de firewall, incluidos escenarios detallados de implementación, consulte el documento en el siguiente enlace:

[http://www.cisco.com/application/pdf/en/us/guest/products/ps5318/c1225/ccmigration\\_09186a0080230754.pdf](http://www.cisco.com/application/pdf/en/us/guest/products/ps5318/c1225/ccmigration_09186a0080230754.pdf)

## Recomendaciones para la configuración de DMVPN

En este tema de ayuda se incluyen recomendaciones sobre cómo proceder con la configuración de los routers en una DMVPN.

### Configuración del hub en primer lugar

Es importante configurar el hub en primer lugar porque los spokes deben configurarse con la información acerca de éste. Si desea configurar un hub, puede utilizar la función de configuración de spoke disponible en la ventana Resumen. Deberá generar un archivo de texto con un procedimiento y enviarlo a los administradores de spokes para que puedan configurar los spokes con la información de hub correcta. Si desea configurar un spoke, debe obtener los datos correctos acerca del hub antes de empezar.

### Asignación de direcciones spoke

Todos los routers de la DMVPN deben encontrarse en la misma subred. Por lo tanto, el administrador de hubs debe asignar direcciones en la subred a los routers spoke para evitar que se produzcan conflictos de direcciones y para asegurarse de que todos los usuarios utilizan la misma máscara de subred.

### Recomendaciones para la configuración de protocolos de enrutamiento en DMVPN

A continuación, se incluyen pautas que se deben tener en cuenta a la hora de configurar protocolos de enrutamiento para las DMVPN. Puede omitir estas pautas, pero tenga en cuenta que Cisco SDM no se ha probado en escenarios fuera de las mismas y es posible que no pueda modificar las configuraciones dentro de Cisco SDM después de especificarlas.

Estas recomendaciones se presentan por orden de prioridad:

- Si existe un proceso de enrutamiento que anuncia en el interior de las redes, utilice este proceso para anunciar redes a la DMVPN.
- Si existe un proceso de enrutamiento que anuncia redes de túnel para VPN, por ejemplo túneles GRE sobre IPSec, utilice este proceso para anunciar las redes DMVPN.
- Si existe un proceso de enrutamiento que anuncia redes para las interfaces WAN, asegúrese de utilizar un número AS o ID de proceso que las interfaces WAN no usen para anunciar redes.
- Al configurar información de enrutamiento de DMVPN, Cisco SDM comprueba si el número del sistema autónomo (EIGRP) o el ID de área (OSPF) especificados ya se utilizan para anunciar redes para la interfaz física del router. Si el valor ya está en uso Cisco SDM le informa y recomienda que emplee un valor nuevo o que seleccione un protocolo de enrutamiento distinto para anunciar redes en la DMVPN.

### Uso de interfaces con conexiones de acceso telefónico

Si selecciona una interfaz que utilice una conexión de marcación podría ocurrir que la conexión esté activa en todo momento. Puede consultar las interfaces admitidas en Interfaces y conexiones para averiguar si para la interfaz física seleccionada se ha configurado una conexión de acceso telefónico a redes como, por ejemplo, una conexión ISDN (RDSI) o conexión asíncrona.

### Realizar un ping al hub antes de comenzar con la configuración del spoke

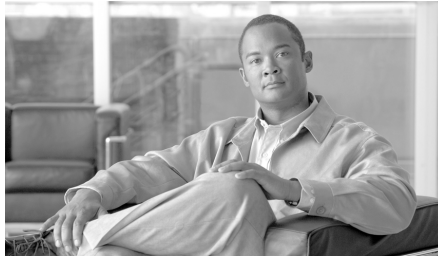
Antes de configurar un router de spoke, debe enviar el comando ping para probar la conectividad con el hub. Si el ping no se realiza correctamente, debe volver a establecer la configuración.

## Informes técnicos sobre Cisco SDM

Existen varios informes técnicos que describen cómo se puede utilizar Cisco SDM. Estos informes técnicos están disponibles en el siguiente enlace.

<http://www.cisco.com/univercd/cc/td/doc/product/software/sdm/appnote/index.htm>





# CAPÍTULO 38

## Pasos iniciales

---

Administrador del dispositivo de seguridad de Cisco (Cisco SDM) es una sencilla herramienta de software basada en el explorador de Internet diseñada para configurar [LAN](#), [WAN](#) y las funciones de seguridad de un router. La herramienta Cisco SDM está dirigida a distribuidores y administradores de red de pequeñas y medianas empresas que dominen los conceptos básicos de la LAN, así como el diseño de red básico.

Si desea realizar una configuración rápida y eficaz de las redes Ethernet, conectividad WAN, firewalls y VPN (Virtual Private Network), Cisco SDM le guiará por el proceso de configuración con la ayuda de asistentes, que son pantallas en secuencia que desglosan los pasos de configuración y proporcionan texto explicativo. Posteriormente, podrá editar la configuración que ha creado, para obtener un mayor control sobre el router y la red. Cisco SDM no requiere que el usuario tenga experiencia con dispositivos Cisco ni con la interfaz de la línea de comandos (CLI) de Cisco.

Al iniciar la herramienta Cisco SDM, ésta muestra la página de inicio, una ventana con información general de configuración y de sistema que proporciona datos cruciales acerca del software y hardware del router. Estos datos se pueden utilizar para determinar los parámetros que desea configurar. Una vez finalizada la configuración, Cisco SDM puede ayudarlo a verificarla y resolver los problemas y de esta forma usted podrá asegurarse de que la configuración funcione.

Cisco SDM dispone además de un modo Supervisión, que le permite observar el rendimiento del router y recopilar las estadísticas asociadas con las configuraciones realizadas en el router.

## ¿Qué novedades trae esta versión?

La presente versión admite las funciones nuevas detalladas a continuación:

- Servidor de la autoridad certificadora: puede configurar el router como un servidor de Autoridad certificadora (CA) y permitir que otorgue certificados a hosts en la red. El uso de un servidor de CA en la red facilita el desarrollo de la tecnología VPN, permitiendo que los hosts locales se suscriban a los certificados desde el servidor de CA que configura, y no desde un servidor de CA público.
- Autenticación 802.1x: el router se puede configurar para realizar autenticación IEEE 802.1x, lo que permite que un cliente autentique utilizando la identidad de la máquina en lugar de la dirección IP.
- Interfaces dinámicas de túnel virtual: DVTI le permite configurar una conexión Easy VPN utilizando una interfaz virtual. Los túneles virtuales dinámicos proporcionan una interfaz de acceso virtual separada a petición para cada conexión de Easy VPN. La configuración de las interfaces de acceso virtual se clona desde una configuración de plantilla virtual, que incluye la configuración de IPSec y cualquier función del software Cisco IOS configurada en la interfaz de plantilla virtual, como, por ejemplo, QoS, NetFlow o ACL.
- Firewall de política basado en zonas: el firewall de política basado en zonas utiliza un modelo de configuración basado en zonas que es más flexible que los firewalls basados en la interfaz. Las interfaces se asignan a zonas y las zonas se ubican en pares de zonas para definir las interfaces de origen y destino del tráfico. Las políticas de inspección se pueden aplicar a pares de zonas para gobernar el tráfico que fluye desde las interfaces de origen a las interfaces de destino en un par de zonas.
- Lenguaje de política de clasificación común de Cisco: C3PL le permite crear políticas basadas en clases. Las clases identifican tipos de tráfico, como, por ejemplo, P2P y IM. Las políticas asocian clases de tráfico y acciones. Especifican la acción que el router debe realizar en el tráfico de una clase específica, como, por ejemplo, inspeccionarlo, permitirle el paso o rechazarlo. Estas políticas se pueden aplicar a pares de zonas.

- **IPS Mejoras:** se admiten mejoras de Cisco IOS IPS disponibles con la versión 12.4(11)T de Cisco IOS. Se admite un nuevo formato de archivo de definición de firmas (SDF), como también otras funciones, como, por ejemplo, Procesador de acción de evento de firma. El SEAP permite mayor control sobre el filtrado, lo que le permite crear Filtros de acción de evento de firma (**SEAF**) y asignar Anulaciones de acción de evento de firma (**SEAO**).
- **Mejoras de calidad de servicio:** **QoS** se ha mejorado para permitirle especificar marcados de **DSCP** o **NBAR** para tráfico, y para crear políticas de QoS que utilizan C3PL.

Para mayor información acerca de esta nueva versión, visite:

<http://www.cisco.com/go/sdm>

Haga clic en el enlace Información general y, a continuación, en Notas de la versión.

## Versiones de Cisco IOS admitidas

Para determinar las versiones de Cisco IOS que Cisco SDM admite, vaya a la siguiente dirección URL:

<http://www.cisco.com/go/sdm>

Haga clic en el enlace Documentación técnica y, a continuación, en Notas de la versión.







# CAPÍTULO 39

## Visualizar la información del router

---

El modo Supervisión de Administrador del dispositivo de seguridad de Cisco (Cisco SDM) le permite ver una instantánea actual de la información sobre el router, las interfaces del router, el firewall y todas las conexiones VPN activas. Asimismo, permite ver los mensajes del registro de eventos del router.



### Nota

---

La ventana Supervisar no se actualiza de forma dinámica con la información más reciente. Para ver la información que ha cambiado desde que abrió la ventana, debe hacer clic en **Actualizar**.

---

El modo Supervisión examina el registro del router y muestra los resultados de los comandos **show** de Cisco IOS. Para las funciones del modo Supervisión que se basan en entradas de registro, como estadísticas de firewall, es preciso activar el registro. El registro se activa por defecto en Cisco SDM, pero se puede cambiar este ajuste desde **Tareas adicionales > Propiedades del router > Registro**. Además, es posible que sea necesario configurar [reglas](#) individuales para que generen eventos de registro. Para obtener más información, consulte el tema de ayuda [¿Como se visualiza la actividad en el firewall?](#)

■ Aspectos generales

Si desea:	Haga lo siguiente:
Visualizar información sobre las interfaces del router.	En la barra de herramientas, haga clic en <b>Supervisar</b> y, a continuación, en el marco izquierdo, haga clic en <b>Estado de la interfaz</b> . En el campo Seleccionar la interfaz seleccione la interfaz sobre la que desea obtener información y, a continuación, en el grupo Available Items (Elementos disponibles), seleccione la información que desea visualizar. Seguidamente, haga clic en <b>Ver detalles</b> .
Visualizar gráficos de la CPU o del uso de la memoria.	En la barra de herramientas, haga clic en <b>Supervisar</b> . La página de Aspectos generales incluye gráficos del uso de la CPU y uso de la memoria.
Visualizar información sobre el firewall.	En la barra de herramientas, haga clic en <b>Supervisar</b> y, a continuación, en el marco izquierdo, haga clic en <b>Estado del firewall</b> .
Visualizar información sobre las conexiones VPN.	En la barra de herramientas, haga clic en <b>Supervisar</b> y, a continuación, en el marco izquierdo, haga clic en <b>Estado de la red VPN</b> . Luego seleccione la ficha de los Túneles IPSec, Túneles DMVPN, Servidores Easy VPN o IKE SAs.
Visualizar los mensajes del registro de eventos del router.	En la barra de herramientas, haga clic en <b>Supervisar</b> y, a continuación, en el marco izquierdo, haga clic en <b>Registro</b> .

## Aspectos generales

La pantalla Aspectos generales del modo Supervisión muestra los aspectos generales de la actividad y las estadísticas del router y sirve de resumen de la información que contienen las otras pantallas del modo Supervisión. Incluye la información que se describe en este tema de ayuda.



**Nota**

Si en la pantalla Aspectos generales no encuentra información sobre las funciones que se describen en este tema de ayuda, la imagen de Cisco IOS no es compatible con la función. Por ejemplo, si el router está ejecutando una imagen de Cisco IOS que no admite funciones de seguridad, las secciones Estado del firewall y Estado de la red VPN no aparecerán en la pantalla.

## Botón Iniciar aplicación inalámbrica

Si el router tiene interfaces de radio, puede hacer clic en este botón para supervisarlas y configurarlas. La ventana Aspectos generales de supervisión proporciona información sobre el estado de la interfaz relacionada con estas interfaces, pero no se enumeran las interfaces de radio en la ventana Estado de la interfaz de supervisión.

Este botón no aparecerá si el router no tiene interfaces de radio.

## Botón Actualizar

Recupera la información actual del router y actualiza las estadísticas que aparecen en pantalla.

## Estado del recurso

Muestra información básica sobre el hardware del router y contiene los campos siguientes:

### Uso de la CPU

Muestra el porcentaje de uso de la CPU.

### Uso de la memoria

Muestra el porcentaje de uso de la RAM.

### Uso de la flash

Muestra la flash disponible respecto a la cantidad de flash instalada en el router.

## Estado de la interfaz

Muestra información básica sobre las interfaces instaladas en el router y su estado.



### Nota

---

En estas estadísticas solamente se incluyen los tipos de interfaz admitidos por Cisco SDM. Las interfaces no admitidas no se cuentan.

---

### Interfaces totales en servicio

El número total de interfaces activadas (en servicio) en el router.

**Interfaces totales fuera de servicio**

El número total de interfaces desactivadas (fuera de servicio) en el router.

**Interfaz**

El nombre de la interfaz.

**IP**

La dirección IP de la interfaz.

**Estado**

El estado de la interfaz, en servicio o fuera de servicio.

**Uso del ancho de banda**

El porcentaje del ancho de banda de la interfaz que se utiliza.

**Descripción**

Descripción disponible para la interfaz. Cisco SDM puede añadir descripciones como \$FW\_OUTSIDE\$ o \$ETH\_LAN\$.

**Grupo Estado del firewall**

Muestra información básica sobre los recursos del router y contiene los campos siguientes:

**Nº de intentos denegados**

Muestra el número de mensajes del registro generados por los intentos de conexión (por protocolos como [Telnet](#), [HTTP](#), [ping](#) y otros) rechazados por el [firewall](#). Tenga en cuenta que para que se genere una entrada de registro por un intento de conexión rechazado, la [regla](#) de acceso que rechaza el intento de conexión se debe configurar para crear entradas de registro.

**Registro de firewall**

Si está activado, muestra el número de entradas de registro del firewall.

**Calidad de servicio (QoS)**

El número de interfaces con una política de calidad de servicio asociada.

## Grupo Estado de la red VPN

Muestra información básica sobre los recursos del router y contiene los campos siguientes:

### Nº de SAs de IKE abiertas

Muestra el número de conexiones de Asociaciones de seguridad (SA) IKE configuradas en ese momento y en ejecución.

### Nº de túneles IPSec abiertos

Muestra el número de conexiones de Red privada virtual (VPN) IPSec configuradas en ese momento y en ejecución.

### Nº de clientes DMVPN

Si el router está configurado como hub DMVPN, el número de clientes DMVPN.

### Nº de clientes VPN activos

Si el router está configurado como servidor Easy VPN, este campo muestra el número de clientes de Easy VPN remoto.

## Grupo de Estado NAC

Muestra una imagen básica del estado del Control de Admisión a la Red (NAC) en el router.

### Campo de número de interfaces con IPS activada

Corresponde al número de interfaces de router en las cuales el NAC está activado.

### Campo de número de hosts validados

Corresponde al número de hosts con agentes de gestión de estado que han sido validados por el proceso de control de admisiones.

## Grupo Registro

Muestra información básica sobre los recursos del router y contiene los campos siguientes:

### Entradas totales de registro

El número total de entradas guardadas en ese momento en el registro del router.

### Gravedad extrema

El número de entradas de registro guardadas con un nivel de gravedad 2 o inferior. Estos mensajes requieren una atención inmediata. Tenga en cuenta que esta lista estará vacía si no tiene ningún mensaje de gravedad extrema.

### Alerta

El número de entradas de registro guardadas con un nivel de gravedad 3 ó 4. Estos mensajes pueden indicar que existe un problema en la red pero es probable que no requieran una atención inmediata.

### Informativo

El número de entradas de registro guardadas con un nivel de gravedad 6 o superior. Estos mensajes informativos indican la existencia de eventos de red normales.

## Estado de la interfaz

En la pantalla Estado de la interfaz se muestra el estado vigente de las distintas interfaces del router y el número de paquetes, bytes o errores de datos que se han transmitido por la interfaz seleccionada. Las estadísticas que aparecen en esta pantalla son acumulativas desde la última vez que se reinició el router, desde que se restablecieron los contadores o desde que se restableció la interfaz seleccionada.

### Botón de supervisión de interfaz y detención de la supervisión

Haga clic en este botón para iniciar o detener la supervisión de la interfaz seleccionada. La etiqueta del botón cambia dependiendo de si Cisco SDM se encuentra supervisando la interfaz o no.

## Botón Probar conexión

Haga clic en este botón para probar la conexión seleccionada. Aparecerá un cuadro de diálogo que permite especificar un host remoto al que se podrá hacer ping a través de esta conexión. A continuación, el cuadro de diálogo muestra un informe indicando si la prueba se ha realizado correctamente o no. Si la prueba no se realiza correctamente, se proporcionará información sobre los posibles motivos, además de los pasos que se deberán llevar a cabo para corregir el problema.

## Lista de interfaces

Seleccione la interfaz de esta lista cuyas estadísticas desee visualizar. Esta lista incluye nombre, dirección IP, máscara de subred, ranura y puerto en el que se ubica, así como cualquier descripción de usuario o Cisco SDM especificada.

## Grupo Seleccione los tipos de diagramas que desea supervisar

Estas casillas de verificación son los elementos de datos para los que Cisco SDM puede mostrar estadísticas en la interfaz seleccionada. Los elementos de datos son los siguientes:

- Entrada de paquetes: número de paquetes recibidos en la interfaz.
- Salida de paquetes: número de paquetes enviados por la interfaz.
- Uso del ancho de la banda: El porcentaje del ancho de banda utilizado por al interfaz, indicado como valor del porcentaje. A continuación se indica cómo se calcula el porcentaje del ancho de banda.

$$\text{Porcentaje de ancho de banda} = (\text{Kbps}/\text{bw}) * 100,$$

donde

$$\text{bits por segundos} = ((\text{cambio en la entrada} + \text{cambio en la salida}) * 8) / \text{intervalo de sondeo}$$

$$\text{Kbps} = \text{bits por segundo} / 1024$$

$$\text{bw} = \text{capacidad del ancho de banda de la interfaz}$$

Ya que la diferencia entre la entrada y la salida de bytes sólo puede calcularse después del segundo intervalo de vista, el gráfico de porcentaje del ancho de banda muestra la cifra correcta de uso comenzando con el segundo intervalo de vista. Consulte la sección Ver intervalo de este tema para intervalos de sondeo e intervalos de vista.

- Entrada de bytes: número de bytes recibidos en la interfaz.
- Salida de bytes: número de bytes enviados por la interfaz.
- Entr. de errores: número de errores producidos durante la recepción de datos en la interfaz.
- Salida de errores: número de errores producidos durante el envío de datos desde la interfaz.
- Flujo de paquetes: número de paquetes en el flujo para la interfaz seleccionada. Este elemento de datos aparece sólo si se configuró en **Configurar > Interfaces y conexiones > Editar > Servicio de aplicación** para la interfaz seleccionada.
- Flujo de bytes: número de bytes en el flujo para la interfaz seleccionada. Este elemento de datos aparece sólo si se configuró en **Configurar > Interfaces y conexiones > Editar > Servicio de aplicación** para la interfaz seleccionada.
- Flujo total: número total de flujos, desde orígenes y destinos, para la interfaz seleccionada. Este elemento de datos aparece sólo si se configuró en **Configurar > Interfaces y conexiones > Editar > Servicio de aplicación** para la interfaz seleccionada.

**Nota**

---

Si la imagen de Cisco IOS del router no admite Netflow, los contadores de flujos no estarán disponibles.

---

Para visualizar las estadísticas de estos elementos:

- 
- Paso 1** Seleccione los elementos que desee visualizar marcando las casillas de verificación correspondientes.
- Paso 2** Para ver las estadísticas de todos los elementos de datos seleccionados, haga clic en **Supervisar interfaz**.
-



## Área Estado de la interfaz

### Ver intervalo

Este campo desplegable selecciona la cantidad de datos mostrados para cada elemento y la frecuencia con que éstos se actualizan. Contiene las opciones siguientes.

**Nota**

---

Las frecuencias de consulta que aparecen son aproximaciones y pueden variar ligeramente de las horas de la lista.

---

- Datos en tiempo real cada 10 segundos. Esta opción seguirá consultando el router durante un máximo de dos horas, lo que resulta en 120 puntos de datos, aproximadamente.
- 10 minutos de datos escrutados cada 10 segundos.
- 60 minutos de datos escrutados cada minuto.
- 12 horas de datos escrutados cada 10 minutos.

**Nota**

---

Con las últimas tres opciones se recopilan un máximo de 60 puntos de datos. Una vez recopilados 60 puntos de datos, Cisco SDM continuará consultando los datos y reemplazando los puntos de datos más antiguos por los más recientes.

---

### Mostrar tabla/Ocultar tabla

Haga clic en este botón para mostrar u ocultar los diagramas de rendimiento.

### Botón Restablecer

Haga clic en este botón para restablecer los contadores de estadísticas de la interfaz a cero.

## Área de diagrama

En esta área se muestran diagramas y valores numéricos simples de los datos especificados.



### Nota

Con las últimas tres opciones se recopilan un máximo de 30 puntos de datos. Una vez recopilados 30 puntos de datos, Cisco SDM continuará consultando los datos y reemplazando los puntos de datos más antiguos por los más recientes.

# Estado de firewall

En esta ventana se muestra la siguiente estadística sobre el [firewall](#) configurado en el router:

- Número de interfaces configuradas para su inspección: el número de interfaces en el router cuya configuración indica que el firewall inspeccionará su tráfico.
- Número de recuento de paquetes TCP: número total de paquetes TCP transmitidos a través de las interfaces configuradas para su inspección.
- Número de recuento de paquetes UDP: número total de paquetes UDP transmitidos a través de las interfaces configuradas para su inspección.
- Número total de conexiones activas: el recuento de las sesiones actuales.

La ventana Estado del firewall también muestra las sesiones de firewall activas en una tabla con las siguientes columnas:

- Dirección IP de origen: la dirección IP del host de origen del paquete.
- Dirección IP de destino: la dirección IP del host de destino del paquete.
- Protocolo: el protocolo de red que se está examinando.
- Recuento de coincidencias: número de paquetes que coinciden con las condiciones de firewall.

## Botón de actualización

Haga clic en este botón para actualizar las sesiones de firewall en la tabla y mostrar los datos más recientes del router.

# Estado del firewall de política basado en zonas

Si el router ejecuta una imagen de Cisco IOS que admite la función de firewall de política basado en zonas, puede visualizar el estado de la actividad de firewall de cada par de zonas configurado en el router.

## Área de lista de la política de firewall

El área de lista de la política de firewall muestra el nombre de la política, zona de origen y de destino de cada par de zonas. La siguiente tabla contiene datos de ejemplo de dos pares de zonas.

Nombre del par de zonas	Nombre de La Política	Zona de origen	Zona de destino
wan-dmz-in	pmap-wan	zone-wan	zone-dmz
wan-dmz-out	pmap-dmz	zone-dmz	zone-wan

En esta tabla de ejemplo hay un par de zonas configurado para el tráfico entrante a **DMZ** y el tráfico saliente de DMZ.

Seleccione el par de zonas para el que desee mostrar estadísticas de firewall.

## Ver intervalo

Seleccione una de las siguientes opciones para especificar cómo se deben recopilar los datos:

- Datos en tiempo real cada 10 seg.: los datos se revisan cada 10 segundos. Cada marca de visto en el eje horizontal del gráfico Paquetes rechazados y paquetes permitidos representa 10 segundos.
- 60 minutos de datos escrutados cada 1 minuto: los datos se revisan cada 1 minuto. Cada marca de visto en el eje horizontal del gráfico Paquetes rechazados y paquetes permitidos representa 1 minuto.
- 12 horas de datos escrutados cada 12 minutos: los datos se revisan cada 12 minutos. Cada marca de visto en el eje horizontal del gráfico Paquetes rechazados y paquetes permitidos representa 12 minutos.

**Supervisar política**

Haga clic en **Supervisar política** para recopilar datos del firewall de la política seleccionada.

**Detener supervisión**

Haga clic en **Detener supervisión** para detener la recopilación de datos del firewall.

**Área de estadísticas**

Esta área muestra las estadísticas de firewall del par de zonas seleccionado. Controle la visualización en esta área haciendo clic en los nodos del árbol que se encuentra a la izquierda. Las siguientes secciones describen lo que aparece al hacer clic en cada uno de los nodos.

**Sesiones activas**

Al hacer clic en **Sesiones activas** aparece el tipo de tráfico, la dirección IP de origen y destino del tráfico que se inspecciona en el par de zonas elegido.

**Paquetes rechazados**

Para el par de zonas elegido, al hacer clic en **Paquetes rechazados** aparece un gráfico que muestra el número acumulativo de paquetes rechazados en comparación con el intervalo de tiempo elegido en la lista Ver intervalo. Los datos se recopilan en el tráfico configurado que se rechazó y registró en el mapa de política de capa 4.

**Paquetes permitidos**

Para el par de zonas elegido, al hacer clic en **Paquetes permitidos** aparece un gráfico que muestra el número acumulativo de paquetes permitidos en comparación con el intervalo de tiempo elegido en la lista Ver intervalo. Los datos se recopilan en el tráfico configurado con la acción de aprobación del mapa de política de capa 4.

# Estado de la red VPN

En esta ventana se muestra un árbol de las conexiones VPN posibles en el router. Puede seleccionar una de las siguientes categorías de VPN en el árbol de conexiones VPN:

- [Túneles IPSec](#)
- [Túneles DMVPN](#)
- [Servidor Easy VPN](#)
- [IKE SA](#)
- [Componentes de SSL VPN](#)

Para ver las estadísticas sobre una categoría de VPN activa, selecciónela en el árbol.

## Túneles IPSec

En este grupo se muestran las estadísticas de cada una de las redes VPN IPSec configuradas en el router. Cada fila de la tabla representa una VPN IPSec. Las columnas de la tabla y la información que ofrecen son las siguientes:

- Columna Interfaz  
La interfaz WAN del router en la que el túnel IPSec está activo.
- Columna IP local  
La dirección IP de la interfaz IPSec local.
- Columna IP remoto  
La dirección IP de la interfaz IPSec remota.
- Columna Par  
La dirección IP del [par](#) remoto.
- Estado del túnel  
El estado actual del túnel IPSec. Los valores posibles son:
  - En servicio: el [túnel](#) está activo.
  - Fuera de servicio: el túnel está inactivo debido a un error o fallo del hardware.

- Columna Paquetes de encapsulación  
Número de paquetes encapsulados en la conexión VPN IPSec.
- Columna Paquetes de desencapsulación  
Número de paquetes desencapsulados en la conexión VPN IPSec.
- Columna Enviar paquetes de errores  
El número de errores producidos durante el envío de paquetes.
- Columna Errores en paquetes recibidos  
El número de errores producidos durante la recepción de paquetes.
- Columna Paquetes cifrados  
Número de paquetes cifrados en la conexión.
- Columna Paquetes descifrados  
Número de paquetes descifrados sobre la conexión.

### Botón Supervisar túnel

Haga clic en este botón para supervisar el túnel IPSec seleccionado en la tabla del túnel IPSec. Consulte [Supervisión de un túnel IPSec](#).

### Botón Probar túnel

Haga clic para probar un túnel VPN determinado. Los resultados de la prueba se mostrarán en otra ventana.

### Botón de actualización

Haga clic en este botón para actualizar la tabla del túnel IPSec y mostrar los datos más recientes del router.

## Supervisión de un túnel IPSec

Para supervisar un túnel IPSec, siga los pasos que se describen a continuación:

- 
- Paso 1** Seleccione el túnel que desea supervisar en la tabla de túnel IPSec.
  - Paso 2** Seleccione los tipos de información que desee supervisar marcando las casillas de verificación en **Seleccionar elemento a supervisar**.
  - Paso 3** Seleccione el intervalo de tiempo para las gráficas en tiempo real utilizando la lista desplegable **Ver intervalo**.
- 

## Túneles DMVPN

Este grupo muestra las estadísticas siguientes sobre los túneles de VPN multipunto dinámicas (DMVPN). Cada fila refleja un túnel VPN.

- Columna Subred remota  
La dirección de red de la subred con la que se conecta el túnel.
- Columna IP de túnel remota  
La dirección IP del túnel remoto. Es la dirección IP privada que el dispositivo remoto asigna al túnel.
- Columna IP de interfaz pública de router remoto  
Dirección IP de la interfaz (externa) pública del router remoto.
- Columna Estado  
El estado del túnel DMVPN.
- Columna Vencimiento  
Fecha y hora en que vence el registro del túnel y el túnel DMVPN quedará inactivo.

### Botón Supervisar túnel

Haga clic en este botón para supervisar el túnel DMVPN seleccionado en la tabla del túnel DMVPN. Consulte [Supervisión de un túnel DMVPN](#).

## Botón de actualización

Haga clic en este botón para actualizar la tabla del túnel DMVPN y mostrar los datos más recientes del router.

## Botón Restablecer

Haga clic en este botón para restablecer los contadores de estadísticas de la lista de túneles. El número de paquetes encapsulados y desencapsulados, el número de errores enviados y recibidos y el número de paquetes cifrados y sin cifrar están fijados en cero.

## Supervisión de un túnel DMVPN

Para supervisar un túnel DMVPN, siga los pasos que se describen a continuación:

- 
- Paso 1** Seleccione el túnel que desea supervisar en la tabla de túnel DMVPN.
  - Paso 2** Seleccione los tipos de información que desee supervisar marcando las casillas de verificación en **Seleccionar elemento a supervisar**.
  - Paso 3** Seleccione el intervalo de tiempo para las gráficas en tiempo real utilizando la lista desplegable **Ver intervalo**.
- 

## Servidor Easy VPN

Este grupo muestra la información siguiente sobre cada uno de los grupos de Servidor Easy VPN:

- Número total de clientes de servidor (en la esquina superior derecha)
- Nombre del grupo
- Número de clientes DMVPN



**Botón Detalles de grupo**

Al hacer clic en **Detalles de grupo** aparece la información siguiente sobre el grupo seleccionado.

- Nombre del grupo
- Clave
- Nombre del conjunto
- Servidores DNS
- Servidores WINS
- Nombre de dominio
- ACL
- Servidores de reserva
- Firewall Are-U-There
- Incluir LAN local
- Bloqueo de grupo
- Guardar contraseña
- Número máximo de conexiones permitidas en este grupo
- Número máximo de inicios de sesión por usuario

**Conexiones de cliente en este grupo**

En esta área aparece la información siguiente sobre el grupo seleccionado.

- Dirección IP pública
- Dirección IP asignada
- Paquetes cifrados
- Paquetes descifrados
- Paquetes salientes rechazados
- Paquetes entrantes rechazados
- Estado

## Botón de actualización

Haga clic en este botón para mostrar los datos más recientes del router.

## Botón de desconexión

- Elija una fila de la tabla y haga clic en Desconectar para interrumpir la conexión con el cliente.

## IKE SA

En este grupo se muestran las estadísticas siguientes de cada una de las asociaciones de seguridad IKE activas configuradas en el router:

- Columna IP de origen  
La dirección IP del par que origina la IKE SA.
- Columna IP de destino  
La dirección IP del par IKE remoto.
- Columna Estado  
Describe el estado actual de las negociaciones IKE. Los estados posibles son los siguientes:
  - MM\_NO\_STATE: se ha creado la SA del Protocolo de la asociación de seguridad en Internet y gestión de claves (ISAKMP) pero aún no ha sucedido nada más.
  - MM\_SA\_SETUP: los pares han coincidido en los parámetros de la SA de ISAKMP.
  - MM\_KEY\_EXCH: los pares han intercambiado claves públicas Diffie-Hellman y han generado un secreto compartido. La SA de ISAKMP aún no se ha autenticado.
  - MM\_KEY\_AUTH: la SA de ISAKMP se ha autenticado. Si el router ha iniciado este intercambio, este estado realiza transiciones inmediatamente a QM\_IDLE y se inicia un intercambio de modo Rápido.
  - AG\_NO\_STATE: se ha creado la SA de ISAKMP pero aún no ha sucedido nada más.

- AG\_INIT\_EXCH: los pares han realizado el primer intercambio en modo Agresivo pero la SA no se ha autenticado.
  - AG\_AUTH: la SA de ISAKMP se ha autenticado. Si el router ha iniciado este intercambio, este estado realiza transiciones inmediatamente a QM\_IDLE y se inicia un intercambio de modo Rápido.
  - QM\_IDLE: la SA de ISAKMP está inactiva. Permanece autenticada con su par y se puede utilizar para los intercambios subsiguientes en modo Rápido.
- Botón Actualizar: haga clic en este botón para actualizar la tabla IKE SA y mostrar los datos más recientes del router.
  - Botón Borrar: seleccione una fila de la tabla y haga clic en este botón para borrar la conexión IKE SA.

## Componentes de SSL VPN

Si hace clic en el botón Estado de la red VPN en la ventana de supervisión, el router comenzará a supervisar la actividad de SSL VPN. En esta ventana se muestran los datos recopilados para todos los contextos de SSL VPN configurados en el router.

Por defecto, estos datos se actualizan cada 10 segundos. Si 10 segundos es un intervalo muy breve para que usted vea los datos antes de la siguiente actualización, puede seleccionar un intervalo de actualización automática de **Datos en tiempo real cada minuto**.

Seleccione un contexto en el árbol de SSL VPN para ver datos para ese contexto y datos para los usuarios configurados para el contexto.

### Recursos del sistema

El porcentaje de recursos de la CPU y la memoria que el tráfico de SSL VPN usa en todos los contextos que se muestran en esta área.

## Número de usuarios conectados

Esta gráfica muestra el número de usuarios activos en el tiempo. El número máximo de usuarios activos desde que comenzó la supervisión se muestra en la parte superior del área de la gráfica. La hora en que comenzó la supervisión se muestra en la esquina inferior izquierda de la gráfica, y la hora actual se muestra en el centro debajo de la gráfica.

## Área de fichas

Esta área de la ventana muestra las estadísticas recopiladas en una serie de fichas para facilitar la visualización.

Para obtener una descripción de los datos que muestra la ficha, haga clic en los enlaces siguientes.

[Sesiones de usuario](#)

[Truncado de URL](#)

[Mapeo de puertos](#)

[CIFS](#)

[Túnel completo](#)



### Nota

---

Si no ha configurado una función como el mapeo de puertos o el túnel completo en el router, la ficha correspondiente a esa función no mostrará datos.

---

Algunas estadísticas se recopilan de nuevo cada vez que el router actualiza los datos de supervisión. Otras estadísticas, como las estadísticas del número máximo de usuarios activos, se recopilan en el momento de la actualización, pero se comparan con los mismos datos recopilados en el momento en que comenzó la supervisión. La supervisión de toda la actividad de VPN, incluida SSL VPN, comienza cuando hace clic en el botón **Estado de la red VPN**.

## Contexto de SSL VPN

En esta ventana se muestran los mismos tipos de información que en la ventana Componentes de SSL VPN, pero sólo se muestran los datos recopilados para el contexto seleccionado. Para obtener una descripción de la información que se muestra, haga clic en [Componentes de SSL VPN](#).

## Sesiones de usuario

Esta ficha muestra la información siguiente sobre las sesiones de usuario de SSL VPN.

- Sesiones de usuario activas: número de sesiones de usuario de SSL VPN, de todos los tipos de tráfico, activas desde la última actualización de los datos de supervisión.
- Número máximo de sesiones de usuario: número máximo de sesiones de usuario de SSL VPN activas desde que comenzó la supervisión.
- Conexiones TCP de usuario activas: número de sesiones de usuario de SSL VPN basadas en TCP activas desde la última actualización de los datos de supervisión.
- Fallos de asignación de sesión: número de fallos de asignación de sesión ocurridos desde que comenzó la supervisión.
- Límite de tiempo de sesión VPN: número de límites de tiempo de sesión VPN alcanzados desde que comenzó la supervisión.
- Sesiones VPN despejadas por el usuario: número de sesiones de VPN que fueron despejadas por usuarios desde que comenzó la supervisión.
- Peticiones pendientes de AAA: número de peticiones de AAA pendientes desde la última actualización de los datos de supervisión.
- Hora pico: la sesión de usuario más larga registrada desde que comenzó la supervisión.
- Sesiones de usuario finalizadas: número de sesiones de usuario finalizadas desde que comenzó la supervisión.
- Fallos de autenticación: número de sesiones con fallos de autenticación desde que comenzó la supervisión.
- Límite de tiempo de inactividad de VPN: número de límites de tiempo de inactividad de VPN alcanzados desde que comenzó la supervisión.
- Límite de usuarios de contexto excedido: número de veces, desde que comenzó la supervisión, que un usuario intentó iniciar una sesión una vez alcanzado el límite de sesión de contexto.
- Límite de usuarios total excedido: número de veces, desde que comenzó la supervisión, que un usuario intentó iniciar una sesión una vez alcanzado el límite de sesiones total.

## Truncado de URL

Esta ficha muestra datos sobre las actividades de truncado de URL. Para obtener más información, consulte la referencia de comandos disponible en el siguiente enlace:

[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_command\\_reference\\_chapter09186a0080419245.html#wp1226849](http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849)

## Mapeo de puertos

Esta ficha muestra datos recopilados sobre las actividades de mapeo de puertos. Para obtener más información, consulte la referencia de comandos en el siguiente enlace:

[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_command\\_reference\\_chapter09186a0080419245.html#wp1226849](http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849)

## CIFS

Esta ficha muestra datos recopilados sobre las solicitudes CIFS, las respuestas y las conexiones. Para obtener más información, consulte la referencia de comandos disponible en el siguiente enlace:

[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_command\\_reference\\_chapter09186a0080419245.html#wp1226849](http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849)

## Túnel completo

Esta ficha muestra información sobre las conexiones de túnel completo entre los clientes y los servidores de SSL VPN en la intranet corporativa.

- Conexiones de túnel activas: número de conexiones de túnel completo activas desde la última actualización de los datos. Los datos pueden actualizarse cada 10 segundos o cada minuto.
- Hora pico de conexiones activas: la conexión de túnel completo de mayor duración desde que comenzó la supervisión.
- Número máximo de conexiones de túnel activas: el número más alto de conexiones de túnel completo activas desde que comenzó la supervisión.

- Intentos fallidos de conexión de túnel: número de intentos de conexión de túnel completo fallidos desde que comenzó la supervisión.
- Intentos de conexión de túnel que han tenido éxito: número de conexiones de túnel completo establecidos correctamente desde que comenzó la supervisión.

Servidor:

- Paquetes IP enviados al servidor: número de paquetes IP desde los clientes de túnel completo que el router reenvió a los servidores en la intranet corporativa.
- Tráfico IP enviado al servidor en bytes: la cantidad de tráfico IP, en bytes, reenviado desde los clientes de túnel completo a los servidores en la intranet corporativa.
- Paquetes IP recibidos del servidor: número de paquetes IP que el router ha recibido de los servidores con conexiones de túnel completo con los clientes.
- Tráfico IP recibido del servidor en bytes: la cantidad de tráfico IP, en bytes, recibido de los servidores en la intranet corporativa con conexiones de túnel completo con los clientes.

## Lista de usuarios

En esta ventana se muestra información sobre los usuarios para el contexto seleccionado en el árbol Componentes de SSL VPN. Dado que existen varias políticas de grupo configuradas para el contexto, donde cada una utiliza su propia lista de direcciones URL y listas de servidores, esta pantalla proporciona información útil sobre cómo los usuarios individuales utilizan sus conexiones SSL VPN.

Puede controlar el uso individual de SSL VPN en esta ventana si selecciona un usuario y hace clic en el botón **Desconectar**.

### Área de lista de usuarios

Esta área enumera todos los usuarios activos en todos los grupos configurados para este contexto. Esta área muestra la siguiente información:

- Nombre de inicio de sesión de usuario: el nombre de usuario autenticado con el servidor AAA.
- Dirección IP del cliente: dirección IP de SSL VPN asignada al usuario para esta sesión. Esta dirección IP se obtiene del conjunto de direcciones configurado para este contexto.

- Contexto: el contexto de SSL VPN según el cual se ha configurado la política de grupo para este usuario.
- Número de conexiones: número de conexiones activas para el usuario. Por ejemplo, el usuario puede tener una conexión con un servidor de correo y también puede examinar archivos en otro servidor de la red.
- Creado: la hora en que se creó la sesión.
- Último uso: la hora en que el usuario envió por última vez tráfico a través de una conexión activa.
- Cisco Secure Desktop: verdadero o falso. Indica si se ha descargado Cisco Secure Desktop en el PC del usuario.
- Nombre del grupo: nombre de la política de grupo según la cual se configura el usuario. La política de grupo especifica la lista de dirección URL, los servicios disponibles para los usuarios, los servidores WINS disponibles para resolver nombres de servidores y los servidores que los usuarios pueden ver al examinar archivos en la intranet corporativa.
- Nombre de lista de direcciones URL: nombre de la lista de direcciones URL que aparece en la página del portal del usuario. La lista de direcciones URL se configura para el grupo al que pertenece el usuario. Consulte el apartado [Política de grupo: Ficha Sin clientes](#) para obtener más información.
- Límite de tiempo de inactividad: número de segundos que una sesión puede permanecer inactiva antes de que el router la finalice. Este valor se configura para el grupo al que pertenece el usuario. Consulte el apartado [Política de grupo: Ficha General](#) para obtener más información.
- Límite de tiempo de sesión: número máximo de segundos que una sesión puede permanecer activa antes de finalizarse. Este valor se configura para el grupo al que pertenece el usuario. Consulte el apartado [Política de grupo: Ficha General](#) para obtener más información.
- Nombre de lista de mapeo de puertos: este valor se configura para el grupo al que pertenece el usuario. Consulte el apartado [Política de grupo: Ficha Cliente ligero](#) para obtener más información.
- Nombre de lista de Servicio de Nombre WINS: este valor se configura para el grupo al que pertenece el usuario. Consulte el apartado [Política de grupo: Ficha Sin clientes](#) para obtener más información.



# Estado del tráfico

En esta ventana se muestra un árbol de los tipos de tráfico que pueden supervisarse en una interfaz. Debe activar un tipo de tráfico cualquiera en al menos una interfaz antes de poder supervisarlos.

Puede seleccionar uno de los siguientes tipos de tráfico en el árbol Estado del tráfico:

- [Usuarios más activos de Netflow](#)
- [Calidad de servicio \(QoS\)](#)
- [Tráfico de aplicaciones/protocolos](#)

Este tipo usa el Reconocimiento de aplicaciones basadas en la red (NBAR) para supervisar el tráfico.

## Usuarios más activos de Netflow

Si se han activado las estadísticas de Netflow para al menos una interfaz en **Configurar > Interfaces y conexiones > Editar interfaz/conexión**, puede ver las estadísticas de Netflow. Seleccione **N flujos de tráfico más activos > Protocolos más activos** o **N flujos de tráfico más activos > Usuarios más activos** (orígenes de mucho tráfico) en el árbol de Estado del tráfico.



### Nota

---

Si la imagen de Cisco IOS del router no admite Netflow, las opciones de Netflow no estarán disponibles en el árbol del Estado del tráfico.

---

## Protocolos más activos

En esta ventana se muestra una tabla con las columnas siguientes:

- Protocolo: el protocolo que se está examinando.
- Número total de flujos: número total de flujos asociados a ese protocolo.
- Flujos/seg: flujos activos por segundo para el protocolo.
- Paquetes/flujo: paquetes transmitidos por flujo.
- Bytes/paquete: bytes por paquete transmitido.
- Paquetes/seg: paquetes transmitidos por segundo.

## Botón Actualizar

Actualiza la ventana con información actual sobre los flujos.

## Usuarios más activos

En esta ventana se muestra una tabla con las columnas siguientes:

- **Dirección IP de origen:** dirección IP de origen para el usuario más activo. Seleccione una dirección IP de origen para obtener más información en **Estado del flujo para la dirección de origen**.
- **Paquetes:** número total de paquetes recibidos de la dirección IP de origen.
- **Bytes:** número total de bytes recibidos de la dirección IP de origen.
- **Flujos:** número de flujos asociados a la dirección IP de origen.



### Nota

---

Si la opción Usuarios más activos de Netflow no está activada en **Configurar > Tareas adicionales > Propiedades del router > NetFlow**, se mostrarán las estadísticas para los diez usuarios más activos.

---

## Estado del flujo para la dirección de origen

Esta tabla muestra la información siguiente sobre los flujos asociados a la dirección IP de origen seleccionada.

- **Dirección IP de destino:** dirección IP de destino del usuario más activo.
- **Protocolos:** protocolos utilizados en los paquetes intercambiados con la dirección IP de destino.
- **Número de paquetes:** número de paquetes intercambiados con la dirección IP de destino.

## Botón Actualizar

Actualiza la ventana con información actual sobre los flujos.

## Calidad de servicio (QoS)

La ventana Estado de [QoS](#) le permite supervisar el rendimiento del tráfico en las interfaces configuradas con QoS (consulte [Asociación de una política de QoS a una interfaz](#)). Esta ventana también le permite supervisar el uso del ancho de banda y los bytes enviados para las interfaces sin configuración de QoS. La supervisión del tráfico entrante en las interfaces de QoS muestra las estadísticas únicamente en el nivel de protocolo. Las estadísticas de nivel de protocolo para las interfaces sin configuración QoS se recopilan para el tráfico en ambas direcciones.

Esta ventana permite supervisar las estadísticas siguientes:

- El uso del ancho de banda para los tipos de tráfico definidos por Cisco SDM
  - El uso del ancho de banda por clase bajo cada tipo de tráfico
  - El uso del ancho de banda para los protocolos bajo cada tipo de clase

El uso del ancho de banda se muestra en Kbps.

- Total de bytes entrantes y salientes para cada tipo de tráfico
  - Los bytes entrantes y salientes para cada clase definida bajo el tipo de tráfico
  - Los bytes entrantes y salientes para cada protocolo y clase

Si el valor es superior a 1.000.000, es posible que el gráfico muestre los bytes como un múltiple de  $10^6$ . Si el valor es superior a 1.000.000.000, es posible que el gráfico muestre los bytes como un múltiple de  $10^9$ .

- Las estadísticas de paquetes rechazados para cada tipo de tráfico

### Interfaz—IP/Máscara—Ranura/Puerto—Descripción

Esta área muestra las interfaces con políticas de QoS asociadas, sus direcciones IP y máscaras de subred, la información de ranura o puerto (si procede) y las descripciones disponibles.

Seleccione en esta lista la interfaz que desee supervisar.

## Ver intervalo

Seleccione el intervalo por el que se deben recopilar las estadísticas:

- Ahora: las estadísticas se recopilan al hacer clic en **Iniciar supervisión**.
- Cada 1 minuto: las estadísticas se recopilan al hacer clic en **Iniciar supervisión** y se actualizan en intervalos de 1 minuto.
- Cada 5 minutos: las estadísticas se recopilan al hacer clic en **Iniciar supervisión** y se actualizan en intervalos de 5 minutos.
- Cada 1 hora: las estadísticas se recopilan al hacer clic en **Iniciar supervisión** y se actualizan en intervalos de 1 hora.

## Iniciar supervisión

Haga clic en esta opción para iniciar la supervisión de las estadísticas de QoS.

## Seleccionar los parámetros de QoS para la supervisión

Seleccione la dirección del tráfico y el tipo de estadísticas que desea supervisar.

### Dirección

Haga clic en **Entrada** o **Salida**.

### Estadísticas

Seleccione uno de los elementos siguientes:

- Ancho de banda
- Bytes
- Paquetes rechazados

## Todo el tráfico—Tiempo real—Importante para la empresa—Trivial

Cisco SDM muestra estadísticas para todas las clases de tráfico en forma de gráfico de barras, en función del tipo de estadística seleccionada. Si para un tipo de tráfico en particular no existen estadísticas adecuadas, Cisco SDM mostrará un mensaje en lugar de un gráfico de barras.

## Asociación de una política de QoS a una interfaz

- 
- Paso 1** Vaya a **Interfaces y conexiones > Editar interfaz/conexión**.
  - Paso 2** En la Lista de interfaces, seleccione la interfaz a la que desea asociar una política de QoS.
  - Paso 3** Haga clic en el botón **Editar**.
  - Paso 4** Haga clic en la ficha **Servicio de aplicación**.
  - Paso 5** Seleccione una política de QoS en la lista desplegable **Entrante** para asociarla al tráfico entrante de la interfaz.
  - Paso 6** Seleccione una política de QoS en la lista desplegable **Saliente** para asociarla al tráfico saliente de la interfaz.
- 

## Tráfico de aplicaciones/protocolos

Esta ventana le permite supervisar el tráfico de aplicaciones y protocolos utilizando el reconocimiento de aplicaciones basadas en la red (NBAR), una función de descubrimiento de protocolos y aplicaciones. El NBAR se utiliza para clasificar paquetes para un manejo más eficaz del tráfico de red a través de una interfaz específica.

**Nota**

Si la imagen de Cisco IOS del router no admite NBAR, esta ventana de estado no estará disponible.

---

### Activar NBAR

Para mostrar el estado del NBAR para una interfaz específica, primero debe activarse NBAR en esa interfaz. Para hacerlo, siga los pasos descritos a continuación:

- 
- Paso 1** Vaya a **Interfaces y conexiones > Editar interfaz/conexión**.
  - Paso 2** Seleccione la interfaz para la que desee activar NBAR en la Lista de interfaces.
  - Paso 3** Haga clic en el botón **Editar**.
  - Paso 4** Haga clic en la ficha **Servicio de aplicación**.
  - Paso 5** Marque la casilla de verificación **NBAR**.
-

## Estado de la red NBAR

La tabla de estado de NBAR muestra las siguientes estadísticas para la interfaz que seleccionó en la lista desplegable **Seleccionar una interfaz**:

- Recuento de paquetes de entrada: número de paquetes del protocolo que se muestran como entrantes en la interfaz seleccionada.
- Recuento de paquetes de salida: número de paquetes del protocolo que se muestran como salientes de la interfaz seleccionada.
- Velocidad de bits (bps): la velocidad, en bits por segundo, de tráfico a través de la interfaz.

## Estado de la red NAC

Si se configura el NAC en el router, Cisco SDM puede mostrar información resumida de las sesiones NAC en el router, las interfaces en las cuales se ha configurado el NAC y estadísticas NAC para la interfaz seleccionada.

La fila superior de la ventana muestra el número de sesiones NAC activas, el número de sesiones NAC iniciadas, y un botón que le permite borrar todas las sesiones NAC activas así como las que se inicializan.

Esta ventana muestra las interfaces del router con políticas NAC asociadas.

```
FastEthernet0/0    10.10.15.1/255.255.255.0    0
```

Haga clic en una entrada de interfaz para mostrar la información devuelta por los agentes de gestión de estados instalados en los hosts de la subred de dicha interfaz. El siguiente es un ejemplo de información de interfaz:

```
10.10.10.5        Política de EAP remoto Infectado        12
```

10.10.10.1 es la dirección IP del host. El tipo de política de autenticación en vigor es la política de EAP remoto. La gestión de estados actual del host se encuentra infectada y han transcurrido 12 minutos desde que el host completó el proceso de control de las admisiones.



### Nota

Esta zona de la ventana no contendrá datos si los hosts de la subred seleccionada no devuelven información de gestión de estados.

Los tipos de autenticación son los siguientes:

- **Política de excepciones locales:** corresponde a una política configurada en el router que se usa para validar el host.
- **Política de EAP remoto:** el host devuelve una gestión de estados y se usa una política de excepción asignada por un servidor ACS.
- **Política de acceso genérico remoto:** el host no tiene un agente de gestión de estados instalado, y el servidor ACS asigna una política de host sin agente.

Los agentes de gestión de estados en los hosts pueden devolver los tokens de gestión de estados siguientes:

- **Sano:** el host se encuentra libre de virus y posee los archivos de definición de virus más recientes.
- **Examen:** el agente de gestión de estados se encuentra analizando si se han instalado los archivos de definición de virus más recientes.
- **Cuarentena:** el host no tiene instalados los archivos de definición de virus más recientes. Se redirecciona al usuario hacia el sitio de mitigación específico que contiene instrucciones para descargar los archivos de definición de virus más recientes.
- **Infectado:** el host se encuentra infectado con un virus conocido. Se redirecciona al usuario hacia un sitio de mitigación para obtener actualizaciones de archivos de definición de virus.
- **Desconocido:** se desconoce la gestión de estados del host.

## Registro

Cisco SDM ofrece los siguientes registros:

- Syslog: el registro del router.
- Registro de firewall: si se ha configurado un firewall en el router, este registro muestra las entradas generadas por ese firewall.
- Registro de seguridad de la aplicación: si se ha configurado un firewall de la aplicación en el router, este registro muestra las entradas generadas por ese firewall.
- Registro de mensajes SDEE: si se ha configurado SDEE en el router, este registro muestra los mensajes SDEE.

Para abrir un registro, haga clic en la ficha del nombre del registro.

# Syslog

El router contiene un registro de eventos clasificados según el nivel de gravedad, como un servicio UNIX syslog.

**Nota**

---

Lo que se muestra es el registro del router, aunque los mensajes de registro se dirijan a un servidor syslog.

---

## Búfer de registro

Indica si el búfer de registro y el registro de syslog están activados. Cuando ambos están activados aparece el texto “Activado”. El búfer de registro reserva una cantidad especificada de memoria para retener los mensajes de registro. La configuración de este campo no se guarda si se reinicia el router. Según la configuración por defecto de estos campos el búfer del registro está activado con 4.096 bytes de memoria.

## Hosts de registro

Muestra la dirección IP de los hosts de syslog a los que se dirigen los mensajes de registro. Este campo es de sólo lectura. Para configurar las direcciones IP de hosts syslog, utilice **Tareas adicionales > Propiedades del router > ventana Registro**.

## Nivel de registro (búfer)

Muestra el nivel de registro configurado para el búfer en el router.

## El número de mensajes en el registro

Muestra el número total de mensajes guardados en el registro del router.

## Seleccione el nivel de registro que desee visualizar

En este campo, seleccione el nivel de gravedad de los mensajes que desea visualizar en el registro. Si se cambia la configuración de este campo se actualizará la lista de los mensajes del registro.



## Registro

Se muestran todos los mensajes con el nivel de gravedad especificado en el campo Seleccione el nivel de registro que desee visualizar. Los eventos de registro contienen la información siguiente.

- Columna Gravedad

Muestra la gravedad del evento registrado. La gravedad se indica con un número del 0 al 7, de modo que los números inferiores indican eventos de mayor gravedad. La descripción de cada nivel de gravedad es la siguiente:

- 0: emergencias  
Sistema inutilizable
- 1: alertas  
Se requiere una acción inmediata
- 2: importante  
Condiciones importantes
- 3: errores  
Condiciones de error
- 4: advertencias  
Condiciones de advertencia
- 5: notificaciones  
Una condición normal pero significativa
- 6: informativo  
Sólo mensajes informativos
- 7: depuraciones  
Mensajes de depuración

- Columna Hora

Muestra la hora en que se han producido los eventos del registro.

- Columna Descripción

Muestra una descripción del evento del registro.

### Botón Actualizar

Actualiza la ventana con información actual sobre los detalles del registro y con las entradas de registro más recientes.

### Botón Borrar registro

Borra todos los mensajes del búfer de registro en el router.

### Botón Buscar

Abre una ventana de búsqueda. En esta ventana, especifique el texto en el campo Buscar y haga clic en el botón **Buscar** para mostrar todas las entradas que incluyan el texto de búsqueda. Las búsquedas *no* distinguen entre mayúsculas y minúsculas.

## Registro de firewall

Las entradas de registro que aparecen en la parte superior de esta ventana se determinan con los mensajes de registro generados por el firewall. Para conseguir que el firewall genere entradas de registro, debe configurar las [reglas](#) de acceso individuales de modo que se generen mensajes de registro cuando se invocan. Para obtener instrucciones sobre la configuración de las reglas de acceso para que se realicen mensajes de registro, consulte el tema de ayuda [¿Como se visualiza la actividad en el firewall?](#)

Con el fin de obtener entradas de registro de firewall, se debe configurar el acceso al router. Vaya a **Tareas adicionales > Propiedades del router > Registro**. Haga clic en **Editar** y configure el registro. Para obtener mensajes de registro del firewall, debe configurar un nivel de registro de depuración (7).

### Registro de firewall

El registro de firewall se muestra si el router está configurado para mantener un registro de los intentos de conexión denegados por el firewall.

### Número de intentos denegados por el firewall

Muestra el número de intentos de conexión denegados por el firewall.

## Tabla de intentos denegados por el firewall

Muestra una lista de los intentos de conexión denegados por el firewall. Esta tabla incluye las columnas siguientes:

- Columna Hora

Muestra la hora en que se han producido los intentos de conexión denegados.

- Columna Descripción

Contiene la siguiente información sobre los intentos denegados: nombre de registro, nombre de regla de acceso o número, servicio, dirección de origen, dirección de destino y número de paquetes. Un ejemplo a continuación:

```
%SEC-6-IPACCESSLOGDP: enumera 100 icmp 171.71.225.148-denegadas>10.77.158.140 (0/0),  
3 paquetes
```

## Botón Actualizar

Sondea el router y actualiza la información que se muestra en la pantalla con información actual.

## Botón Buscar

Abre una ventana de búsqueda. Seleccione un tipo de búsqueda en el menú **Buscar** y especifique el texto adecuado en el campo Buscar y, a continuación, haga clic en el botón **Buscar** para mostrar las entradas del registro que coincidan.

Los tipos de búsqueda son:

- Dirección IP de origen: la dirección IP del host de origen del ataque.  
Se puede especificar una dirección IP parcial.
- Dirección IP de destino: dirección IP del destino del ataque.  
Se puede especificar una dirección IP parcial.
- Protocolo: el protocolo de red que se utilizó en el ataque.
- Texto: cualquier texto encontrado en la entrada del registro.

Las búsquedas *no* distinguen entre mayúsculas y minúsculas.

## Ver ataques más frecuentes

Seleccione una de las siguientes formas para mostrar información sobre los ataques más frecuentes en el menú desplegable Ver:

- Puertos de ataque más importantes: ataques más importantes por puerto de destino.
- Atacantes más importantes: por dirección IP del atacante.

La tabla de ataques más importantes debajo del menú desplegable Ver muestra las entradas de ataques más importantes. Si selecciona Puertos de ataque más importantes en el menú desplegable Ver, la tabla de ataques más importantes mostrará entradas con las siguientes columnas:

- Número de puerto: puerto de destino.
- Número de ataques: número de ataques contra el puerto de destino.
- Número de paquetes denegados: número de paquetes a los que se denegó el acceso al puerto de destino.
- Ver detalles: un enlace que abre una ventana con el registro completo de los ataques contra el puerto seleccionado.

Si selecciona Atacantes más importantes en el menú desplegable Ver, la tabla de ataques más importantes mostrará entradas con las siguientes columnas:

- Dirección IP del atacante: dirección IP desde la cual provienen los ataques.
- Número de ataques: número de ataques que provienen de la dirección IP.
- Número de paquetes denegados: número de paquetes que provienen de la dirección IP a los que se denegó el acceso al puerto de destino.
- Ver detalles: un enlace que abre una ventana con el registro completo de los ataques provenientes de la dirección IP seleccionada.

## Supervisión del firewall con una cuenta de usuario de “Vista que no es de administrador”

La supervisión de firewall requiere la activación del Registro a un búfer en el router. Si la opción Registro a un búfer no está activada, inicie la sesión en Cisco SDM mediante una cuenta de vista de Administrador o mediante una cuenta de usuario de nivel de privilegio 15 no basada en vistas y configure el registro.

Para configurar el registro en Cisco SDM, vaya a **Tareas adicionales > Propiedades del router > Registro**.

## Registro de Seguridad de la aplicación

Si el registro se encuentra habilitado y se ha especificado que las alarmas serán activadas cuando el router encuentre tráfico desde aplicaciones o protocolos especificados, se reunirán dichas alarmas en un registro que se puede consultar desde esta ventana.

Con el fin de obtener entradas de registro de la seguridad de la aplicación, se debe configurar el acceso al router. Vaya a **Tareas adicionales > Propiedades del router > Registro**. Haga clic en **Editar** y configure el registro. Para obtener mensajes de registro de firewall, se debe configurar un nivel de registro **informativo (6)** o mayor. Si ya se ha configurado el registro de acceso para **depuración(7)**, el registro contendrá mensajes de registro de seguridad de la aplicación.

El siguiente es un ejemplo de texto de registro:

```
*Sep 8 12:23:49.914: %FW-6-DROP_PKT: Dropping im-yahoo pkt
128.107.252.142:1481 => 216.155.193.139:5050
*Sep 8 12:24:22.762: %FW-6-DROP_PKT: Dropping im-aol pkt
128.107.252.142:1505 => 205.188.153.121:5190
*Sep 8 12:26:02.090: %FW-6-DROP_PKT: Dropping im-msn pkt
128.107.252.142:1541 => 65.54.239.80:1863
*Sep 8 11:42:10.959: %APPFW-4-HTTP_PORT_MISUSE_IM: Sig:10006 HTTP
Instant Messenger detected - Reset - Yahoo Messenger from
10.10.10.2:1334 to 216.155.194.191:80
*Sep 8 12:27:54.610: %APPFW-4-HTTP_STRICT_PROTOCOL: sig:15 HTTP
protocol violation detected - Reset - HTTP not detected from
10.10.10.3:1583 to 66.218.75.184:80
*Sep 8 12:26:14.866: %FW-6-SESS_AUDIT_TRAIL_START: Start im-yahoo
session: initiator (10.10.10.3:1548) -- responder (66.163.172.82:5050)
*Sep 8 12:26:15.370: %FW-6-SESS_AUDIT_TRAIL: Stop im-yahoo session:
initiator (10.10.10.3:1548) envió 0 bytes -- responder
(66.163.172.82:5050) sent 0 bytes
*Sep 8 12:24:44.490: %FW-6-SESS_AUDIT_TRAIL: Stop im-msn session:
initiator (10.10.10.3:1299) sent 1543 bytes -- responder
(207.46.2.74:1863) sent 2577 bytes
*Sep 8 11:42:01.323: %APPFW-6-IM_MSN_SESSION: im-msn-un-recognized
service session initiator 14.1.0.1:2000 sends 1364 bytes to responder
207.46.108.19:1863
*Sep 8 11:42:01.323: %APPFW-6-IM_AOL_SESSION: im-aol text-chat
service session initiator 14.1.0.1:2009 sends 100 bytes to responder
216.155.193.184:5050
```

### Botón Actualizar

Actualiza la pantalla con información actual sobre los detalles del registro y con las entradas de registro más recientes.

### Botón Buscar

Abre una ventana de búsqueda. En esta ventana, especifique el texto en el campo **Buscar** y haga clic en el botón **Buscar** para mostrar todas las entradas que incluyan el texto de búsqueda. Las búsquedas *no* distinguen entre mayúsculas y minúsculas.

## Registro de mensajes SDEE

Esta ventana muestra una lista de los mensajes [SDEE](#) recibidos por el router. Los mensajes SDEE se generan cuando existen cambios en la configuración de IPS.

### Mensajes SDEE

Seleccione el tipo de mensaje SDEE para mostrar:

- Todos: se muestran los mensajes de advertencia, estado y error SDEE.
- Error: sólo se muestran los mensajes de error de SDEE.
- Estado: sólo se muestran los mensajes de estado de SDEE.
- Alertas: sólo se muestran los mensajes de advertencia de SDEE.

### Botón Actualizar

Haga clic en él para ver los nuevos mensajes SDEE.

### Botón Buscar

Abre una ventana de búsqueda. Seleccione un tipo de búsqueda en el menú **Buscar** y especifique el texto adecuado en el campo **Buscar** y, a continuación, haga clic en el botón **Buscar** para mostrar las entradas del registro que coincidan.

Los tipos de búsqueda son:

- Dirección IP de origen
- Dirección IP de destino
- Texto

Las búsquedas *no* distinguen entre mayúsculas y minúsculas.

## Hora

La hora en que se recibió el mensaje.

## Tipo

Los tipos son: Error, Estado y Alertas. Haga clic en [Texto de los mensajes SDEE](#) para ver los mensajes SDEE posibles.

## Descripción

Descripción disponible.

# Estado de la red IPS

Esta ventana aparece si el router usa una imagen de Cisco IOS que admite IPS versión 4.x o anterior. En esta ventana se muestra una tabla de las estadísticas de firmas de IPS, agrupadas por tipo de firma. Se muestran las siguientes estadísticas:

- **ID de firma:** identificador numérico de la firma.
- **Descripción:** descripción de la firma.
- **Índice de riesgo:** valor entre 0 y 100 que representa la cuantificación numérica del riesgo asociado con un evento particular en la red.
- **Acción:** acción que se debe tomar cuando un paquete coincide con una firma.
- **Dirección IP de origen:** la dirección IP del host de origen del paquete.
- **Dirección IP de destino:** dirección IP del host de destino del paquete.
- **Coincidencias:** número de paquetes coincidentes.
- **Número de interrupciones:** número de paquetes coincidentes rechazados.

Para ordenar las firmas, haga clic en el encabezado de la columna cuyo nombre de estadística de firma desea establecer como criterio de ordenación.

**Nota**

Si ordena las firmas, es posible que éstas ya no se agrupen por tipo. Para restaurar la agrupación de firmas por tipo, haga clic en el botón **Actualizar**.

**Número total de firmas activas**

Muestra el número total de firmas disponibles activas en el router.

**Número total de firmas inactivas**

Muestra el número total de firmas disponibles inactivas en el router.

**Botón Actualizar**

Haga clic en este botón para buscar e incluir las estadísticas de firmas más recientes.

**Botón Borrar**

Haga clic en este botón para restablecer todos los contadores de estadísticas de firmas en 0.

**Registro de SDEE**

Haga clic para ver los mensajes SDEE. Puede ver estos mensajes haciendo clic en **Supervisar > Registro > Registro de mensajes SDEE**.



# Estadísticas de firmas de IPS

Esta ventana aparece si el router usa una configuración IOS IPS 5.x. Las estadísticas aparecen para cada firma activada en la configuración IOS IPS. La parte superior de la ventana muestra los totales de firmas para proporcionar una instantánea de la configuración de firmas. Se proporcionan los siguientes números totales:

- Número total de firmas
- Número total de firmas activadas
- Número total de firmas retiradas
- Número total de firmas compiladas

## Botones Actualizar y Borrar

Haga clic en **Actualizar** para buscar e incluir las estadísticas de firmas más recientes. Haga clic en **Borrar** para restablecer todos los contadores de estadísticas de firmas en 0.

## Registro de SDEE

Haga clic para ver los mensajes SDEE. Puede ver estos mensajes haciendo clic en **Supervisar > Registro > Registro de mensajes SDEE**.

## Área de lista de firmas

El ID de firma, descripción, número de coincidencias y número de interrupciones se muestra para todas las firmas. Si llega un paquete que coincide con una firma, las direcciones IP de origen y de destino también se indican.

## Estadísticas de alertas de IPS

La ventana Estadísticas de alertas de IPS muestra las estadísticas de alerta en formato codificado por colores para una fácil configuración. La parte superior de la pantalla muestra una leyenda que explica el uso de colores en la pantalla.

Color	Explicación
<b>ROJO</b>	El evento que generó la alerta tiene un índice de riesgo (RR) alto que se encuentra en el intervalo de 70 a 100.
<b>MAGENTA</b>	El evento que generó la alerta tiene un índice de riesgo (RR) medio que se encuentra en el intervalo de 40 a 69.
<b>AZUL</b>	El evento que generó la alerta tiene un índice de riesgo (RR) bajo que se encuentra en el intervalo de 0 a 39.

Al hacer clic en el encabezado de la columna, se puede clasificar la visualización según los valores de ese parámetro. Por ejemplo, si hace clic en el encabezado **ID de firma**, puede clasificar la visualización en orden numérico ascendente o descendente de ID de firma. Cada columna se describe en la siguiente lista:

- **ID de firma:** identificador numérico de la firma.
- **Descripción:** descripción de la firma.
- **Índice de riesgo:** valor entre 0 y 100 que representa la cuantificación numérica del riesgo asociado con un evento particular en la red.
- **Acción de evento:** acción que debe tomar IOS IPS si se produce un evento que coincide con la firma.
- **Dirección IP de origen:** la dirección IP desde donde se originó el paquete.
- **Dirección IP de destino:** la dirección IP hacia la que se dirigió el paquete. Si el paquete es malintencionado, la dirección IP de destino puede considerarse como destino.
- **Coincidencias:** número de paquetes coincidentes.
- **Número de interrupciones:** número de paquetes coincidentes rechazados.
- **Motor:** el [motor de firmas](#) asociado a la firma.

# Estado de la autenticación 802.1x

## Autenticación 802.1x en áreas de interfaces

Interfaz

Autenticación 802.1x

Reautenticación

## Área de clientes 802.1x

Dirección MAC del cliente

Estado de la autenticación

Interfaz





# CAPÍTULO 40

## Comandos del menú Archivo

---

Las opciones siguientes aparecen en el menú Archivo de Administrador del dispositivo de seguridad de Cisco (Cisco SDM).

### Guardar configuración en ejecución en el PC

Guarda el archivo de configuración en ejecución del router en un archivo de texto del PC.

### Enviar configuración al router

Esta ventana permite entregar al router cualquier cambio de configuración que se haya realizado utilizando Cisco SDM. Tenga en cuenta que cualquier cambio en la configuración mediante Cisco SDM no influirá en el router hasta que haya enviado la configuración.

#### Guardar la configuración en ejecución en la configuración de inicio del router

Marque esta casilla de verificación para que Cisco SDM guarde la configuración mostrada en la ventana, tanto en el router que ejecuta el archivo de configuración, como en el archivo de inicio. El archivo de configuración en ejecución es sólo temporal y se borrará cuando se vuelva a arrancar el router. Si guarda la configuración en la configuración de inicio del router, los cambios efectuados en la misma permanecerán después de arrancar de nuevo el sistema.

Si se utiliza Cisco SDM para configurar un router Cisco 7000, la casilla de verificación **Guardar la configuración en ejecución en la configuración de inicio del router** se desactivará si existen comandos **boot network** o **boot host** con comandos **service config** en la configuración en ejecución.

### Cancelar

Haga clic en este botón para eliminar el cambio de configuración y cerrar el cuadro de diálogo Entrega Cisco SDM a router.

### Guardar a archivo

Haga clic en este botón para guardar los cambios efectuados en la configuración que aparece en la ventana en un archivo de texto.

## Escribir en la configuración de inicio

Esta opción permite escribir el archivo de configuración en ejecución del router en la configuración de inicio de éste.

Si se utiliza Cisco SDM para configurar un router Cisco 7000, este elemento del menú se desactivará si hay comandos **boot network** o **boot host** con comandos **service config** en la configuración en ejecución.

## Restablecer los valores por defecto de fábrica

Consulte [Restablecer los valores por defecto de fábrica](#).

# Gestión de archivos

Esta ventana permite ver y gestionar el sistema de archivos de su memoria flash de router Cisco y de los dispositivos flash USB conectados a ese router. Esta ventana sólo permite ver y gestionar sistemas de archivo DOSFS.

El lado izquierdo de la ventana muestra un árbol expansible que representa el sistema de directorio de la memoria flash de su router Cisco y de los dispositivos flash USB conectados a ese router.

El lado derecho de la ventana muestra una lista con los nombres de los archivos y directorios encontrados en el directorio elegido en el lado izquierdo de la ventana. También muestra el tamaño de cada archivo en bytes, así como la fecha y hora de la última modificación de cada archivo y directorio.

Es posible elegir un archivo o directorio de la lista al lado derecho de la ventana y luego elegir uno de los comandos sobre la lista.

Es posible cambiar el nombre o eliminar los directorios (carpetas). Es posible copiar, pegar o eliminar uno o varios archivos, y es posible cambiar el nombre de un solo archivo. Sin embargo, se aplican las siguientes restricciones:

- Los archivos no se pueden pegar en el mismo directorio de donde se copiaron.
- Si se invoca Cisco SDM desde la memoria flash del router, los archivos de Cisco SDM no se pueden eliminar.

Se pueden eliminar archivos de Cisco SDM que son copias o si Cisco SDM se invoca desde un PC.

- Si se invoca Cisco SDM desde la memoria flash del router, no se puede cambiar el nombre de los archivos de Cisco SDM.

Se puede cambiar el nombre de los archivos de Cisco SDM que son copias o si Cisco SDM se invoca desde un PC.

- Si se invoca Cisco SDM desde la memoria flash del router, no se puede sustituir (reemplazar por un archivo con el mismo nombre) un archivo de Cisco SDM.

Se pueden reemplazar los archivos de Cisco SDM que son copias o si Cisco SDM se invoca desde un PC.

- No se puede cambiar el nombre de los archivos del software de Cisco IOS.
- No se pueden copiar los directorios (carpetas).

Si el router se arranca desde un servidor tftp, las restricciones de archivo anteriores no se aplican.

## Botón Actualizar

Haga clic en el botón **Actualizar** para buscar una nueva imagen de los directorios y archivos en la memoria flash del router Cisco y en los dispositivos conectados a ese router.

## Botón Formatear

Haga clic en el botón **Formatear** para reformatear la memoria flash del router Cisco o para reformatear un dispositivo flash USB conectado a ese router. El botón **Formatear** sólo se activa si se elige un icono que represente la memoria flash del router Cisco o un dispositivo flash USB en el lado izquierdo de la ventana.



### Precaución

---

Si elige reformatear la memoria flash del router Cisco o un dispositivo flash USB conectado a ese router hará que se *borren* todos los archivos en el sistema de archivos.

---

## Botón Nueva Carpeta

Haga clic en el botón **Nueva Carpeta** para crear un nuevo directorio en el directorio elegido en el lado izquierdo de la ventana. Los nombres de las carpetas no pueden contener espacios ni signos de interrogación (“?”).

## Botón Cargar archivos desde el PC

Haga clic en el botón **Cargar archivos desde el PC** para abrir una ventana de selección de archivos en el PC local. Elija un archivo para guardarlo en el directorio elegido de la memoria flash de su router Cisco o en un dispositivo flash USB conectado a ese router. Los archivos de Cisco SDM y los archivos con nombres que contienen espacios no pueden ser cargados usando la opción Cargar archivos desde el PC.

Los archivos de Cisco SDM como Cisco SDM.tar no pueden ser cargados usando la opción Cargar archivos desde el PC. Los archivos de Cisco SDM deben cargarse mediante **Herramientas > Actualizar SDM**.

Si se usa Cargar Archivo desde el PC para cargar un archivo de imagen de arranque, no se puede guardar en el directorio actual de archivo de imagen de arranque.



## Botón Copiar

Elija un archivo del lado derecho de la ventana y haga clic en el botón **Copiar** para copiar el archivo.

## Botón Pegar

Después de hacer clic en el botón **Copiar** para copiar un archivo, haga clic en el botón **Pegar** para pegar la copia del archivo en un directorio diferente. Elija un directorio de destino en el lado izquierdo de la ventana. No se puede pegar una copia del archivo en el mismo directorio que el archivo original.

## Botón Cambiar nombre

Elija un archivo o directorio del lado derecho de la ventana y haga clic en el botón **Cambiar nombre** para cambiar su nombre. Los nombres no pueden contener espacios ni signos de interrogación (“?”).

## Botón Eliminar

Elija un archivo o directorio del lado derecho de la ventana y haga clic en el botón **Eliminar** para eliminar el archivo. Un archivo con el icono de no escritura junto a su nombre no podrá ser eliminado.

## Nombre

Haga clic en **Nombre** para ordenar los archivos y directorios alfabéticamente por nombre. Haga clic en **Nombre** nuevamente para invertir el orden.

## Tamaño

Haga clic en **Tamaño** para ordenar los archivos y directorios por tamaño. Los directorios siempre tienen un tamaño de cero bytes, aunque no estén vacíos. Haga clic en **Tamaño** nuevamente para invertir el orden.

## Hora de modificación

Haga clic en **Hora de modificación** para ordenar los archivos y directorios por fecha y hora de modificación. Haga clic en **Hora de modificación** nuevamente para invertir el orden.

## Cambiar nombre

Esta ventana permite cambiar el nombre de un archivo de la memoria flash de su router Cisco o de los dispositivos flash USB conectados a ese router.

Especifique el nuevo nombre de archivo en el campo Nuevo Nombre. La ruta a la ubicación del archivo aparece sobre el campo Nuevo Nombre.

## Nueva carpeta

Esta ventana permite asignar un nombre y crear una nueva carpeta en el directorio de sistema de la memoria flash de su router Cisco y en los dispositivos flash USB conectados a ese router.

Especifique el nombre de la nueva carpeta en el campo Nombre de la Carpeta. La ruta a la ubicación de la nueva carpeta aparece sobre el campo Nueva Carpeta.

## Guardar SDF a PC

Si se encuentra trabajando en IPS, se puede guardar el archivo de definición de firma (SDF) con que está trabajando en el PC. Navegue hasta el directorio donde desea guardar el archivo y haga clic en **Guardar**.

## Salir

Permite salir de Administrador del dispositivo de seguridad de Cisco.

# No se ha podido realizar la compresión de flash

Esta ventana aparece cuando el router no consigue llevar a cabo la operación de compresión de flash porque nunca se ha realizado la operación **erase flash**: en el router. En este tema de la ayuda se explica cómo deben descargarse los archivos necesarios para la operación **erase flash**: cómo ejecutar **erase flash**: y cómo deben volverse a cargar los archivos al router y volver a establecer la conexión con Cisco SDM a continuación.

Al ejecutar el comando **erase flash** se borrará Cisco SDM y la imagen de Cisco IOS de la **memoria flash** del router y perderá la conexión con éste. Se recomienda imprimir el contenido de este tema de la ayuda para que pueda utilizar las instrucciones y obtener una imagen de Cisco IOS y SDM.tar de Cisco.com e instalarlas en el router.

- 
- Paso 1** Asegúrese de que el router no pierda rendimiento. Si ocurre así después de una operación de **borrado de flash**:, no se guardará ninguna imagen de Cisco IOS en la memoria.



**Nota** Si el rendimiento del router disminuye después de la operación de borrado de flash, puede utilizar el procedimiento que aparece en el enlace siguiente para recuperarlo:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_mod/cis3700/sw\\_conf/37\\_swcf/appendc.htm#xtocid11](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3700/sw_conf/37_swcf/appendc.htm#xtocid11)

- 
- Paso 2** Para guardar la configuración en ejecución del router en un archivo del PC, haga clic en **Archivo > Guardar configuración en ejecución en el PC** y especifique un nombre de archivo.

- Paso 3** Prepare un servidor **TFTP** en el que desee guardar los archivos y cópielos al router. Debe tener acceso de escritura al servidor TFTP. Su PC se puede utilizar para ello si dispone de un programa de servidor TFTP.

- Paso 4** Utilice el comando **ftfpcopy** para copiar la imagen de Cisco IOS y los archivos SDM.tar y SDM.shtml de la memoria Flash al servidor TFTP:

**copy flash: tftp://dirección-servidor-tftp/nombre-archivo**

Ejemplo:

```
copy flash: tftp://10.10.10.3/SDM.tar
```




---

**Nota** Si prefiere descargar una imagen de Cisco IOS, así como los archivos SDM.tar y SDM.shtml, siga estas instrucciones para descargar una imagen de Cisco IOS, los archivos SDM.tar y SDM.shtml admitidos por Cisco SDM a través de una conexión a Internet. A continuación, coloque estos archivos en un servidor TFTP.

---

- a. Haga clic en el enlace siguiente para obtener una imagen de Cisco IOS del Software Center de Cisco:  
<http://www.cisco.com/kobayashi/sw-center/>
- b. Obtenga una imagen que admita las funciones que desee en la versión 12.2(11)T o posterior. Guarde el archivo en el servidor TFTP al que se puede acceder desde el router.
- c. Utilice el enlace siguiente para obtener los archivos SDM.tar y SDM.shtml. A continuación, guárdelos en el servidor TFTP.

**<http://www.cisco.com/go/sdm>**

---

**Paso 5** Desde el PC, conéctese al router por medio de Telnet y habilite el modo Activar.

**Paso 6** Especifique el comando **erase flash:** y confírmelo. La imagen de IOS, el archivo de configuración y los archivos SDM.tar y SDM.shtml del router se extraen de la RAM no volátil (NVRAM).

**Paso 7** Utilice el comando **tftpcopy** para copiar primero la imagen de IOS y después el archivo SDM.tar del servidor TFTP al router:

**copy tftp://dirección-servidor-tftp/nombre de archivo flash:**

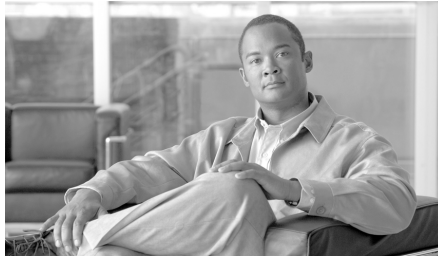
Ejemplo:

```
copy tftp://10.10.10.3/nombre_imagen_ios flash:
! Reemplace nombre_imagen_ios por nombre real de la imagen de IOS
copy tftp://10.10.10.3/SDM.tar flash:
```

**Paso 8** Inicie el explorador Web y vuelva a establecer conexión con Cisco SDM a través de la misma dirección IP que usó al iniciar la sesión en Cisco SDM.

Ahora que se ha realizado una operación **erase flash:** en el router, podrá ejecutar el comando **squeeze flash** siempre que sea necesario.

---



# CAPÍTULO 41

## Comandos del menú Editar

---

Las opciones siguientes aparecen en el menú Editar de Administrador del dispositivo de seguridad de Cisco (Cisco SDM).

### Preferencias

Esta pantalla permite configurar las opciones de Administrador del dispositivo de seguridad de Cisco siguientes:

#### **Obtener una vista previa de los comandos antes de enviarlos al router**

Elija esta opción si desea que Cisco SDM muestre una lista de los comandos de configuración de Cisco IOS generados antes de enviar los comandos al router.

#### **Guardar el archivo de firma en la Flash**

Elija esta opción si desea que el archivo de definición de firma (SDF) con que está trabajando se guarde en la memoria flash del router cuando haga clic en **Aplicar cambios**.

#### **Confirmar antes de salir de Cisco SDM**

Éste es el comportamiento de Cisco SDM por defecto. Seleccione esta opción si desea que Cisco SDM muestre un cuadro de diálogo en el que se solicita una confirmación para salir de Cisco SDM.

## Continuar la supervisión del estado de la interfaz al cambiar de modo o tarea

Este es el comportamiento de Cisco SDM por defecto. Cisco SDM empieza a supervisar el estado de la interfaz al hacer clic en **Supervisar** y seleccionar el **estado Interfaz**. Para que Cisco SDM siga supervisando la interfaz aunque usted salga del modo Supervisar y realice otras tareas en Cisco SDM, seleccione esta casilla de verificación y especifique el número máximo de interfaces que desea que Cisco SDM supervise. El número máximo por defecto de interfaces que pueden supervisarse es 4.



# CAPÍTULO 42

## Comandos del menú Ver

---

Las opciones siguientes aparecen en el menú Ver de Administrador del dispositivo de seguridad de Cisco (Cisco SDM).

### Inicio

Muestra la página de inicio de Cisco SDM, que proporciona información sobre el hardware del router, el software y las configuraciones de LAN, WAN, firewall y VPN.

### Configurar

Muestra la barra de tareas de Cisco SDM, que permite realizar configuraciones guiadas y manuales de interfaces y conexiones, firewalls y ACL, enrutamiento de VPN y otras tareas.

### Supervisar

Muestra la ventana Supervisar de Cisco SDM, que le permite ver estadísticas sobre el router y la red.

# Configuración en ejecución

Muestra la configuración en ejecución del router.

## Mostrar comandos

Aparece el cuadro de diálogo Mostrar comandos, que le permite enviar comandos **show** de Cisco IOS al router, ver el resultado y guardarlo en su PC. El resultado se guarda con el nombre de archivo por defecto `show_<comando>[dirección_ip_router]`.

El cuadro de diálogo Mostrar comandos permite ver el resultado de los comandos **show** siguientes.

- **show flash**: muestra el contenido de la memoria Flash del router.
- **show startup-config**: muestra el archivo de configuración de inicio del router.
- **show access-lists**: muestra todos los comandos de las Listas de control de acceso (ACL) que están configurados en el router.
- **show diag**: muestra información acerca del hardware instalado en el router.
- **show interfaces**: muestra información acerca de la configuración de cada interfaz y acerca de los paquetes transferidos por las mismas.
- **show protocols**: muestra información acerca de los protocolos de red configurados en cada interfaz.
- **show version**: muestra información acerca de la versión del software de Cisco IOS que se ejecuta en el router.
- **show tech-support**: muestra el resultado de todos los demás comandos **show**.
- **show environment** : muestra información acerca de la fuente de alimentación del router. Es posible que este comando no aparezca en la lista desplegable **Mostrar comandos** si no es compatible con el router.



# Reglas de Cisco SDM por defecto

En la pantalla Reglas de Cisco SDM por defecto aparece una lista de todas las reglas por defecto configuradas por Cisco SDM. Esta pantalla se organiza de la siguiente forma: en la parte izquierda aparece un árbol con las opciones de reglas de acceso, firewall, política IKE - VPN y grupos de transformación VPN. Para ver las reglas por defecto de estas opciones, haga clic en la opción que desee del árbol. En la derecha aparecerán las reglas por defecto de esa opción. Para obtener más información acerca de las reglas, consulte las descripciones de la opción siguientes:

## Reglas de acceso

Muestra todas las reglas de la Lista de control de acceso por defecto ([ACL](#)) y una breve descripción de cada una.

## Firewall

Muestra las políticas de seguridad de la aplicación por defecto de Cisco SDM. Elija la política de seguridad que desea ver de la lista que se encuentra en la esquina superior derecha de la ventana.

- **SDM\_HIGH**: esta política impide el uso de Mensajería instantánea y aplicaciones Punto a punto en la red. Supervisa el tráfico HTTP y de correo electrónico y rechaza el tráfico que no cumple con el protocolo utilizado. Devuelve otro tráfico TCP y UDP para las sesiones iniciadas dentro del firewall.
- **SDM\_MEDIUM**: esta política supervisa el uso de Mensajería instantánea y aplicaciones Punto a punto en la red, así como el tráfico HTTP y de correo electrónico. Devuelve otro tráfico TCP y UDP para las sesiones iniciadas dentro del firewall.
- **SDM\_LOW**: esta política no supervisa tráfico de aplicaciones. Devuelve otro tráfico TCP y UDP para las sesiones iniciadas dentro del firewall.

## Política IKE - VPN

Muestra las políticas por defecto del Intercambio de claves por Internet ([IKE](#)).

## Conjuntos de transformación - VPN

Muestra los conjuntos de transformación de la seguridad IP ([IPSec](#)) por defecto.

# Actualizar

Carga de nuevo la información de configuración del router. Si existen comandos no enviados, Cisco SDM muestra una ventana de mensaje que le informa que si actualiza perderá todos los comandos que no se hayan enviado. Si desea enviar los comandos, haga clic en **No** en esta ventana y, a continuación, en **Enviar** en la barra de herramientas de Cisco SDM.



# CAPÍTULO 43

## Comandos del menú Herramientas

---

Las opciones siguientes aparecen en el menú Herramientas de Administrador del dispositivo de seguridad de Cisco (Cisco SDM).

### Ping

Aparece el cuadro de diálogo Ping, que permite enviar un mensaje [ping](#) a otro dispositivo de la red. Consulte [Generar el reflejo...](#) para obtener información sobre cómo usar la ventana Ping.

### Telnet

Muestra el cuadro de diálogo Telnet de Windows, que le permite establecer conexión con el router y acceder a la interfaz de línea de comandos (CLI) de Cisco IOS por medio del protocolo [Telnet](#).

### Auditoría de seguridad

Muestra la pantalla Auditoría de seguridad de Cisco SDM. Consulte el apartado [Auditoría de seguridad](#) para obtener más información.

# Configuración de PIN del token USB

El cuadro de diálogo Configuración de PIN del token USB permite configurar PINs para los tokens USB conectados a su router.

## Seleccione un tipo de PIN

Elija **PIN de usuario** para configurar un PIN de usuario, o **PIN de administrador** para configurar un PIN de administrador.

Se usa un PIN de usuario para acceder al router. Si se conecta un token USB a un router y el nombre del token y el PIN de usuario corresponden a una de las entradas en **Configurar > VPN > Componentes VPN > Infraestructura de clave pública > Tokens USB**, quedará automáticamente registrado en ese router.

Se usa un PIN de administrador para gestionar la configuración del token USB utilizando el software del fabricante. Cisco SDM permite cambiar el PIN de administrador para un token USB si se introduce el PIN de administrador actual.

## Nombre del token

Especifique el nombre del token USB.

El nombre del token viene definido de fábrica. Por ejemplo, los tokens fabricados por Aladdin Knowledge Systems tienen como nombre eToken.

También puede utilizar el nombre “usbtoken $x$ ”, donde  $x$  es el número de puerto USB donde se conecta el token USB. Por ejemplo, un token conectado al puerto USB 0 se llamará usbtoken0.

## PIN actual

Especifique el PIN de usuario o administrador existente. Si no conoce el PIN existente, se debe usar el software del token USB del fabricante para encontrarlo.

## Nuevo PIN

Especifique un nuevo PIN para el token USB. El PIN existente será reemplazado por el nuevo PIN. El nuevo PIN debe tener un mínimo de 4 caracteres.

## Confirmar PIN

Reintroduzca el nuevo PIN para confirmarlo.

## Guardar el nuevo PIN en el router

Marque la casilla de verificación **Guardar el nuevo PIN en el router** si desea guardar el nuevo PIN como una entrada en **Configurar > VPN > Componentes VPN > Infraestructura de clave pública > Tokens USB**. Si ya existe una entrada con el mismo nombre en **Configurar > VPN > Componentes VPN > Infraestructura de clave pública > Tokens USB**, será reemplazada por la nueva entrada.

La casilla de verificación **Guardar el nuevo PIN en el router** sólo estará disponible para los PINS de usuario.

# Aplicación inalámbrica

Si el router tiene interfaces de radio, puede iniciar la aplicación inalámbrica para supervisar y configurar las interfaces. Cisco SDM puede ayudarle a configurar y visualizar la dirección IP o los detalles de bridge acerca de una interfaz de radio, pero debe usar la aplicación inalámbrica para definir otros parámetros de configuración.

# Actualizar Cisco SDM

Puede hacer que Cisco SDM obtenga e instale automáticamente una actualización.

## Actualizar Cisco SDM desde Cisco.com

Puede actualizar Cisco SDM directamente desde Cisco.com. Cisco SDM busca en Cisco.com todas las versiones disponibles y le informa si encuentra alguna versión más reciente que la utilizada en su router. Entonces, puede actualizar Cisco SDM mediante el asistente para la actualización.

Para actualizar Cisco SDM desde Cisco.com:

- 
- Paso 1** Seleccione **Actualizar Cisco SDM** desde Cisco.com en el menú Herramientas. Al seleccionar esta opción se inicia el asistente para la actualización.
  - Paso 2** Utilice el asistente para la actualización para obtener los archivos de Cisco SDM y copiarlos en el router.
- 

### Actualizar Cisco SDM desde un PC local

Puede actualizar Cisco SDM por medio de un archivo SDM.zip que se descarga de Cisco.com. Cisco SDM proporciona un asistente para la actualización que copiará los archivos necesarios en su router.

Para actualizar Cisco SDM desde el PC que está utilizando para ejecutar Cisco SDM siga los pasos descritos a continuación:

- 
- Paso 1** Descargue el archivo `sdm-vnn.zip` de la dirección URL siguiente:  
<http://www.cisco.com/cgi-bin/tablebuild.pl/sdm>
  - Si existe más de un archivo Cisco SDM.zip, obtenga la copia con el número de versión mayor.
  - Paso 2** Utilice el asistente para la actualización para copiar los archivos de Cisco SDM de su PC al router.
- 

### Actualizar Cisco SDM desde un CD

Si tiene el CD de Cisco SDM, puede utilizarlo para actualizar Cisco SDM en el router. Para hacerlo, siga los pasos descritos a continuación:

- 
- Paso 1** Coloque el CD de Cisco SDM en la unidad de CD del PC.
  - Paso 2** Seleccione **Actualizar Cisco SDM desde un CD** y haga clic en **Actualizar Cisco SDM** en la ventana de Instrucciones generales después de leer el texto.
  - Paso 3** Cisco SDM le permitirá encontrar el archivo `SDM-Updates.xml` en el CD. Cuando encuentre el archivo, haga clic en **Abrir**.
  - Paso 4** Siga las instrucciones del asistente de instalación.
-

# Inicio de sesión en CCO

Deberá proporcionar datos de inicio de sesión y contraseña CCO para acceder a esta página Web. Indique un nombre de usuario y contraseña y, luego, haga clic en Aceptar.

Si no posee nombre de usuario ni contraseña de CCO, puede obtenerlos si abre una instancia de su explorador Web y se dirige al siguiente enlace del sitio Web de Cisco:

<http://www.cisco.com>

Cuando se abra la página Web, haga clic en Register y suministre la información necesaria para obtener un nombre de usuario y contraseña. Luego, vuelva a realizar esta operación.







## CAPÍTULO **44**

# Comandos del menú Ayuda

---

Las opciones siguientes aparecen en el menú Ayuda de Administrador del dispositivo de seguridad de Cisco (Cisco SDM).

## Temas de Ayuda

Muestra la ayuda en línea de Cisco SDM. En la parte izquierda de la ayuda aparece el índice de la ayuda en línea de Cisco SDM.

## Cisco SDM en CCO

Abre un explorador y muestra la página Cisco SDM del sitio Web Cisco.com.

## Matriz de hardware/software

Abre un explorador y muestra una matriz de los modelos de router de Cisco y las versiones de imágenes del Cisco IOS para guiarlo en la selección de software compatible con las imágenes de Cisco IOS. El acceso a la matriz requiere un nombre de usuario y una contraseña de Cisco Connection Online.

## Acerca de este router...

Muestra información acerca del hardware y del software del router en el que se ejecuta Cisco SDM.

## Acerca de Cisco SDM

Muestra información de la versión de Cisco SDM.



## G L O S A R I O

---

### Símbolos y números

- 3DES** Triple DES. Algoritmo de cifrado que utiliza tres claves de cifrado DES de 56 bits (168 bits efectivos) en rápida sucesión. Existe una versión 3DES alternativa que sólo utiliza dos claves DES de 56 bits, aunque usa una de ellas dos veces, por lo que se obtiene efectivamente una clave de 112 bits de longitud. De uso legal sólo en los Estados Unidos. Consulte [DES](#).
- 802.1x** 802.1x es un estándar IEEE para brindar control de acceso de nivel de medios, ofreciendo la capacidad de permitir o denegar la conectividad de red, controlar el acceso VLAN y aplicar una política de tráfico basada en la identidad del usuario o de la máquina.

---

### A

- AAA** Authentication, Authorization and Accounting (Autenticación, autorización y cuentas). Pronunciado “triple A”.
- AAL5-MUX** ATM Adaptation Layer 5 Multiplexing.
- AAL5-SNAP** ATM Adaptation Layer 5 Subnetwork Access Protocol.
- ACE** Entrada de control de acceso. Entrada en una ACL que especifica un host o red de origen y si se permite o deniega el tráfico desde dicho host. Una ACE también puede especificar un host o red de destino y el tipo de tráfico.

<b>ACL</b>	Lista de control de acceso. Información de un dispositivo que especifica las entidades a las que se da permiso de acceso al propio dispositivo o a las redes que están detrás de él. Las listas de control de acceso están formadas por una o más entradas de control de acceso (ACE).
<b>ACS</b>	Servidor de Control de Acceso Seguro de Cisco. Software de Cisco que puede implementar un servidor RADIUS o un servidor TACACS+. El ACS se usa para almacenar las bases de datos de políticas que utiliza <a href="#">Easy VPN</a> , <a href="#">NAC</a> y otras funciones para controlar el acceso a la red.
<b>acuerdo de claves</b>	Proceso por el que dos o varias partes se ponen de acuerdo para usar la misma clave simétrica secreta.
<b>ADSL</b>	Asymmetric Digital Subscriber Line (Línea de suscriptor digital asimétrica).
<b>AH</b>	Authentication Header (Encabezado de autenticación). Protocolo IPsec antiguo que, en la mayoría de las redes, es menos importante que ESP. AH proporciona servicios de autenticación, aunque no de cifrado. Su función es asegurar la compatibilidad con pares IPsec que no admiten ESP, que suministra tanto autenticación como cifrado.
<b>AHP</b>	Authentication Header Protocol (Protocolo de encabezado de autenticación). Permite autenticar el host de origen y proporciona integridad de datos. AHP no ofrece confidencialidad.
<b>AH-MD5-HMAC</b>	Encabezado de autenticación con el algoritmo hash MD5 (variante HMAC).
<b>AH-SHA-HMAC</b>	Encabezado de autenticación con el algoritmo hash SHA (variante HMAC).
<b>algoritmo</b>	Secuencia lógica de pasos que permite resolver problemas. Los algoritmos de seguridad son de cifrado de datos o de autenticación.  DES y 3DES son algoritmos de cifrado de datos.  Entre los algoritmos de cifrado y descifrado figuran block cipher, CBC, null cipher y stream cipher.  Los algoritmos de autenticación incluyen hash como MD5 y SHA.
<b>algoritmo de hash</b>	Los algoritmos de hash se usan para crear un valor hash, también conocido como message digest, y permiten asegurar que el contenido de los mensajes no se modifica durante la transmisión. Los dos tipos de algoritmos de hash más utilizados son el algoritmo de hash seguro (SHA) y MD5.

<b>AMI</b>	Alternate Mark Inversion (Inversión alternada de marcas).
<b>Anulación de acción de evento</b>	Las anulaciones de acción de evento se usan en IOS IPS 5.x. Permiten cambiar las acciones asociadas con un evento basado en el <a href="#">RR</a> de dicho evento.
<b>anulación de acción de evento</b>	
<b>archivo delta</b>	Archivo que Cisco IOS IPS crea para guardar los cambios efectuados en las firmas.
<b>ARP</b>	Address Resolution Protocol (Protocolo de resolución de direcciones). Protocolo TCP/IP de bajo nivel que asigna la dirección de hardware de un nodo (llamada <i>dirección MAC</i> ) a la dirección IP.
<b>arquitectura cliente/servidor</b>	Término utilizado para describir los sistemas de red de computación (procesamiento) distribuida en los que las responsabilidades de la transacción se dividen en dos partes: cliente (interfaz de usuario) y servidor (sistema secundario). También se denomina arquitectura distribuida. Consulte también <a href="#">RPC</a> .
<b>arquitectura de túneles</b>	Proceso de canalización del flujo de un protocolo a través de otro protocolo.
<b>ASA</b>	Adaptive Security Algorithm (Algoritmo de seguridad adaptable). Permite conexiones de una sola dirección (de dentro hacia fuera) sin que haya una configuración explícita para cada aplicación y sistema interno.
<b>ATM</b>	Asynchronous Transfer Mode (Modo de transferencia asíncrona). Estándar internacional de relé de celdas en el que varios tipos de servicios (como voz, vídeo y datos) se transfieren en celdas de longitud fija (53 bytes). Las celdas de longitud fija permiten que el proceso de celdas se produzca en el hardware y, por consiguiente, que haya una disminución de los retrasos del tránsito.
<b>autenticación</b>	Establecer la verdad de una identidad.
<b>autenticación</b>	En seguridad, verificación de la identidad de una persona o proceso. La autenticación establece la integridad de un flujo de datos, con lo que se asegura que durante la transmisión no se produjo ninguna alteración, además de confirmar el origen del flujo de datos.
<b>autenticación del origen de los datos</b>	Función de un servicio de no repudiación.

---

**B**

- bits de red** En una máscara de subred, número de bits establecidos en 1 binario. Una máscara de subred 255.255.255.0 tiene 24 bits de red, ya que hay 24 bits de la máscara establecidos en 1. Una máscara de subred 255.255.248 tiene 17 bits de red.
- bits de subred** Máscara de dirección de 32 bits utilizada en IP para indicar los bits de una dirección IP que se emplean en la dirección de red y la dirección de subred
- máscara de subred** opcional. Las máscaras de subred se indican en decimales. La máscara 255.255.255.0 especifica los 24 primeros bits de la dirección que, en ocasiones, se denominan sencillamente “máscara”. Consulte también “máscara de dirección” y “dirección IP”.
- bloque** Secuencia de bits de longitud fija.
- BOOTP** Protocolo Bootstrap que utiliza un nodo de red para determinar la dirección IP de las interfaces Ethernet para influir en el arranque de la red.

---

**C**

- C3PL** Lenguaje de política de clasificación común de Cisco. C3PL es un reemplazo estructurado para comandos de configuración específicos de la función y permite que la funcionalidad configurable se exprese en términos de un evento, una condición o una acción.
- CA** Autoridad certificadora. Entidad fiable de terceros que emite o revoca certificados digitales. En ocasiones se denomina *notario* o *autoridad de certificación*. En un dominio de CA determinado, cada dispositivo necesita únicamente su propio certificado y la clave pública de la CA para autenticar los otros dispositivos de dicho dominio.
- CA raíz** Autoridad certificadora (CA) suprema que firma los certificados de las CA subordinadas. La CA raíz tiene un certificado firmado por ella misma que contiene su propia clave pública.

<b>caché</b>	Repositorio temporal de información acumulada de ejecuciones de tareas anteriores que puede volverse a utilizar, por lo que disminuye el tiempo necesario para ejecutar las tareas.
<b>canal libre</b>	Se entiende por canal libre aquel por el que puede fluir el tráfico que no está cifrado. Este tipo de canales no impone restricciones de seguridad sobre los datos transmitidos.
<b>CBAC</b>	Context-based Access Control (Control de acceso basado en contexto). Protocolo que proporciona a los usuarios internos un control de acceso seguro en todas las aplicaciones y todo el tráfico situados en el interior de los perímetros de la red. CBAC escruta tanto la dirección de origen como la de destino y realiza un seguimiento del estado de la conexión de cada aplicación.
<b>CDP</b>	Cisco Discovery Protocol (Protocolo de descubrimiento de Cisco). Se trata de un protocolo de descubrimiento de dispositivos independiente de protocolos y de soportes, que se ejecuta en todos los equipos fabricados por Cisco, incluidos routers, servidores de acceso, bridges y switches. Mediante CDP, un dispositivo puede anunciar su existencia a otros dispositivos y recibir información acerca de otros dispositivos situados en la misma LAN o en el lado remoto de una WAN.
<b>CDP</b>	Punto de distribución de la lista de revocaciones de certificados. Ubicación desde la que se puede recuperar la lista de revocaciones de certificados. Un CDP normalmente es un URL HTTP o LDAP.
<b>CEP</b>	Certificate Enrollment Protocol (Protocolo de suscripción de certificados). Protocolo de gestión de certificados. CEP es una implementación temprana de CRS (Certificate Request Syntax), estándar propuesto a IETF (Internet Engineering Task Force). Dicho protocolo especifica cómo se comunica un dispositivo con una CA, incluido cómo recuperar la clave pública de la CA, suscribir un dispositivo a la CA y recuperar una lista de revocaciones de certificados (CRL). CEP utiliza los PKCS (Public Key Cryptography Standards) 7 y 10 como tecnologías de componentes clave. El grupo de trabajo de infraestructuras de claves públicas (PKIX) del IETF está trabajando para estandarizar un protocolo para estas funciones, ya sea CRS o un equivalente. Cuando haya un estándar IETF definitivo, Cisco agregará compatibilidad para éste. CEP ha sido desarrollado conjuntamente por Cisco Systems y VeriSign, Inc.
<b>certificado</b>	Consulte <a href="#">certificado digital</a> .

<b>certificado de firma</b>	Utilizado para asociar la firma digital a los mensajes o documentos y para asegurar que los mensajes o archivos se transfieren sin sufrir cambios.
<b>certificado de la CA</b>	Certificado digital concedido a una autoridad certificadora (CA) por otra autoridad certificadora.
<b>certificado digital</b>	Representación digital firmada criptográficamente de los atributos de usuario o dispositivo que enlazan una clave con una identidad. Un certificado exclusivo vinculado a una clave pública proporciona la prueba de que no se ha desvelado la clave. Una autoridad certificadora fiable emite y firma el certificado que vincula una clave pública a su propietario. Generalmente, los certificados incluyen el nombre y la clave pública del propietario, así como el número de serie del certificado y la fecha de vencimiento de éste. También pueden contener más información. Consulte <a href="#">X.509</a> .
<b>certificado X.509</b>	Certificado digital estructurado según las directrices X.509.
<b>CET</b>	Cisco Encryption Technology (Tecnología de cifrado de Cisco). Cifrado del nivel de red de propiedad introducido en Cisco IOS, versión 11.2. CET proporciona cifrado de datos de la red en el nivel de paquetes IP e implementa los estándares siguientes: DH, DSS y DES de 40 y de 56 bits.
<b>CHAP</b>	Challenge Handshake Authentication Protocol (Protocolo de autenticación por desafío mutuo). Función de seguridad admitida en líneas que usan la encapsulación PPP y evita accesos no autorizados. CHAP no evita por sí el acceso no autorizado, sino que simplemente identifica el extremo remoto. Es el router o el servidor de acceso el que determina si se permite acceder al usuario. Consulte también <a href="#">PAP</a> .
<b>chargen</b>	Character Generation (Generación de caracteres). Mediante TCP, servicio que envía un flujo continuo de caracteres hasta que el cliente lo detiene. Mediante UDP, el servidor envía un número aleatorio de caracteres cada vez que el cliente envía un datagrama.
<b>ciclo de vida</b>	Consulte <a href="#">fecha de vencimiento</a> .
<b>cifrado</b>	Algoritmo de cifrado y descifrado.
<b>cifrado</b>	Aplicación de un algoritmo específico a datos para modificar la apariencia de éstos y convertirlos en incomprensibles para aquellos que no estén autorizados a ver la información.



<b>cifrado asimétrico</b>	Conocido también como <i>sistemas de clave pública</i> , este sistema permite a cualquiera acceder a la clave pública de cualquier usuario y, por consiguiente, enviar un mensaje a dicho usuario mediante la clave pública.
<b>cifrado de bloque</b>	Algoritmo de cifrado que utiliza un cifrado simétrico de 64 bits para operar en bloques de datos de tamaño fijo. Consulte <a href="#">cifrado</a> .
<b>cifrado de clave pública</b>	En los sistemas de cifrado de clave pública, todos los usuarios tienen tanto una clave pública como una privada. Cada usuario privado mantiene su propia clave privada y no la comparte con nadie. Dicha clave se usa para generar una firma digital única y para descifrar información cifrada con la clave pública. Por otra parte, la clave pública de un usuario estará disponible para todos los usuarios con el fin de cifrar información destinada a dicho usuario o verificar su firma digital. En ocasiones se denomina “criptografía de clave pública”.
<b>cifrar</b>	Producir criptográficamente texto cifrado a partir de texto sin formato.
<b>Cisco SDM</b>	Administrador del dispositivo de seguridad de Cisco. Cisco SDM es una herramienta de software basada en el explorador Web, diseñada para configurar LAN, WAN y funciones de seguridad en un router. Consulte el apartado <a href="#">Pasos iniciales</a> para obtener más información.
<b>clave</b>	Cadena de bits utilizada para cifrar y descifrar datos o para calcular message digest.
<b>clave compartida</b>	Clave secreta compartida por todos los usuarios de una sesión de comunicación basada en claves simétricas.
<b>clave de sesión</b>	Clave que sólo se utiliza una vez.
<b>clave distribuida</b>	Clave criptográfica compartida dividida en trozos que se entregan por separado a participantes diferentes.

<b>clave previamente compartida</b>	<p>Uno de los tres métodos de autenticación ofrecidos en IPSec; los otros dos son “nonces” cifrados mediante RSA y firmas RSA. Las claves compartidas previamente permiten a uno o varios clientes utilizar secretos compartidos individualmente para autenticar túneles cifrados en una gateway mediante IKE. Dichas claves se utilizan, por lo general, en redes pequeñas de un máximo de 10 clientes y no es preciso implicar a una CA para la seguridad.</p> <p>El intercambio de claves Diffie-Hellman combina claves públicas y privadas para crear un secreto compartido y utilizarlo como autenticación entre pares IPSec. El secreto compartido puede compartirse entre dos o varios pares. En cada par participante, es preciso especificar un secreto compartido como parte de una política IKE. Por lo general, la distribución de esta clave previamente compartida se efectúa mediante un canal fuera de banda seguro. Si se usa una clave previamente compartida y uno de los pares participantes no está configurado con dicha clave, no se podrá establecer la SA IKE. Para una SA IPSec, una SA IKE es un requerimiento previo. Todos los pares deben tener configurada una clave previamente compartida.</p> <p>El certificado digital y las claves previamente compartidas en modo de comodín (que permiten que uno o varios clientes utilicen un secreto compartido para autenticar los túneles cifrados en una gateway) son alternativas a las claves previamente compartidas. Tanto los certificados digitales como las claves previamente compartidas en modo de comodín son más escalables que las claves previamente compartidas.</p>
<b>clave privada</b>	Consulte <a href="#">cifrado de clave pública</a> .
<b>clave secreta</b>	Consulte <a href="#">clave simétrica</a> .
<b>clave simétrica</b>	Las claves simétricas se utilizan para descifrar información previamente cifrada.
<b>claves asimétricas</b>	Pareja de claves criptográficas relacionadas matemáticamente. La clave pública cifra información que sólo la clave privada puede descifrar, y viceversa. Asimismo, la clave privada firma datos que sólo la clave pública puede autenticar.
<b>claves RSA</b>	Un par de claves asimétricas RSA es un conjunto de claves privadas y públicas coincidentes.

<b>CLI</b>	Command-Line Interface (Interfaz de la línea de comandos). Interfaz principal que permite especificar comandos de configuración y de supervisión para el router. Consulte la Guía de configuración del router que se dispone a configurar para obtener información acerca de los comandos que puede especificar en el CLI.
<b>CNS</b>	Cisco Networking Services (Servicios de red de Cisco). Conjunto de servicios que admite una implementación de red escalable, así como suministro de servicios, supervisión, seguridad de servicio y configuración.
<b>comp-lzs</b>	Algoritmo de compresión IP.
<b>conexión VPN</b>	VPN sitio a sitio. Una VPN sitio a sitio está formada por un conjunto de conexiones VPN entre pares, en el que los atributos de definición de cada conexión incluyen la información de configuración y de dispositivos siguiente: <ul style="list-style-type: none"><li>- Un nombre de conexión</li><li>- Opcionalmente, una política IKE y la clave previamente compartida</li><li>- Un par IPSec</li><li>- Una lista de uno o varios hosts o subredes remotos a los que protegerá la conexión</li><li>- Una regla IPSec que define qué tráfico debe cifrarse</li><li>- Una lista de conjuntos de transformación que define cómo se cifra el tráfico protegido</li><li>- Una lista de las interfaces de red del dispositivo al que se aplica la conexión</li></ul>
<b>Configuración, Config, Archivo Config</b>	Archivo del router que contiene los valores, preferencias y propiedades que puede administrar mediante Cisco SDM.
<b>confidencialidad de datos</b>	Resultado del cifrado de datos que evita revelar información a procesos, entidades o individuos no autorizados. Esta información puede ser datos del nivel de aplicaciones o bien parámetros de comunicación. Consulte <a href="#">confidencialidad del flujo de tráfico o análisis del tráfico</a> .
<b>confidencialidad del flujo de tráfico o análisis del tráfico</b>	Concepto de seguridad que evita la revelación no autorizada de parámetros de comunicación. La implementación satisfactoria de este concepto oculta a las partes no autorizadas, las direcciones IP de origen y de destino, la longitud del mensaje y la frecuencia de comunicación.

<b>conjunto de transformación</b>	Combinación aceptable de protocolos de seguridad, algoritmos y otras configuraciones que se aplica en tráfico protegido por IPSec. Durante la negociación de la asociación de seguridad IPSec, los pares acuerdan utilizar un conjunto de transformación determinado para proteger un flujo de datos concreto.
<b>Contexto SSL VPN</b>	Un contexto de WebVPN proporciona los recursos necesarios para configurar el acceso seguro a una intranet corporativa y a otros tipos de redes privadas. Un contexto WebVPN debe incluir un gateway WebVPN asociado. Un contexto de WebVPN puede servir para una o más políticas de grupo de WebVPN.
<b>contraseña</b>	Cadena de caracteres (u otro origen de datos) protegida y secreta asociada a la identidad de un usuario o entidad específico.
<b>control de acceso, regla de control de acceso</b>	Información introducida en la configuración que permite especificar el tipo de tráfico que se desea permitir o denegar en una interfaz. Por defecto, se deniega el tráfico que no se permite explícitamente. Las reglas de control de acceso están formadas por entradas de control de acceso (ACE).
<b>contraseña de revocación</b>	Contraseña proporcionada a una CA cuando se solicita que ésta revoque el certificado digital de un router. En ocasiones, se denomina <i>contraseña de desafío</i> .
<b>cookie</b>	Una cookie es una función del explorador Web que almacena o recupera información, como las preferencias del usuario, en un almacén persistente. En Netscape e Internet Explorer, las cookies se implementan guardando un pequeño archivo de texto en el disco duro local. El archivo puede cargarse la siguiente vez que ejecute un subprograma Java o visite un sitio Web. De esta forma, se puede guardar información exclusiva para el usuario entre sesiones. El tamaño máximo de un cookie es de alrededor de 4 KB.
<b>CPE</b>	Customer premises equipment (Equipo del sitio del cliente).
<b>criptografía</b>	Técnicas matemáticas y científicas utilizadas para mantener los datos privados, auténticos, sin modificar y sin repudiar.
<b>CRL</b>	Certificate Revocation List (Lista de revocaciones de certificados). Lista mantenida y firmada por una autoridad certificadora (CA) de todos los certificados digitales que no hayan caducado pero que estén revocados.
<b>custodio de claves</b>	Tercero fiable que guarda las claves criptográficas.

---

<b>D</b>	
<b>DES</b>	Data Encryption Standard (Estándar de cifrado de datos). Algoritmo criptográfico estándar desarrollado y estandarizado por el NIST (National Institute of Standards and Technology) de los EE.UU. Utiliza una clave de cifrado secreta de 56 bits. El algoritmo DES está incluido en varios estándares de cifrado.
<b>descifrado</b>	Aplicación inversa de un algoritmo de cifrado a datos cifrados, por lo que se restaura el estado original y sin cifrar de los datos.
<b>detección de reproducciones</b>	Función de seguridad IPSec estándar que combina números de secuencias con autenticación, a fin de que el destinatario de una comunicación pueda rechazar los paquetes antiguos o duplicados y evitar, de esta manera, ataques de reproducción.
<b>DHCP</b>	Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de hosts). Proporciona un mecanismo para asignar dinámicamente direcciones IP a hosts, a fin de que las direcciones se puedan volver a utilizar cuando los hosts ya no las necesiten.
<b>digest</b>	Salida de una función hash.
<b>Dirección IP</b>	Las direcciones IP de versión 4 tienen una longitud de 32 bits o 4 bytes. Este “espacio” de red se utiliza para designar un número de red, un número de subred opcional y un número de host. Los 32 bits están agrupados en cuatro octetos (8 bits binarios), representados por cuatro números decimales separados por puntos. La parte de la dirección utilizada para especificar el número de red, el de la subred y el del host se especifica mediante la <a href="#">máscara de subred</a> .
<b>DLCI</b>	Data-Link Connection Identifier (Identificador de conexión de enlace de datos). En las conexiones Frame Relay, el identificador de una conexión de enlace de datos determinada entre dos puntos finales.
<b>DMVPN</b>	Dynamic multipoint virtual private network (Red privada virtual multipunto dinámica). Red privada virtual en la que los routers se ordenan en un hub lógico y topología de spoke, y en la que los hubs cuentan con conexiones GRE de punto a punto sobre IPSec con el hub. DMVPN usa GRE y NHRP para permitir el flujo de paquetes a destinos de la red.

<b>DMVPN única</b>	Un router con una configuración DMVPN única tiene una conexión con un hub DMVPN y un túnel GRE configurado para comunicaciones DMVPN. Las direcciones del túnel GRE para el hub y los spokes deben estar en la misma subred.
<b>DMZ</b>	Demilitarized Zone (Zona desmilitarizada). Una DMZ es una zona búfer situada entre Internet y las redes privadas. Puede tratarse de una red pública usada normalmente para servidores de correo electrónico, <a href="#">FTP</a> y Web a los que acceden los clientes externos en Internet. Mediante la colocación de estos servidores de acceso público en una red aislada y separada, se proporciona una medida de seguridad adicional a la red interna.
<b>DN</b>	Nombre completo. Identificador único de un cliente de la autoridad certificadora, incluido en todos los certificados del cliente recibidos de la autoridad certificadora. Generalmente, el DN incluye el nombre del usuario, el de la compañía u organización del usuario, el código de dos letras del país del usuario, una dirección de correo electrónico usada para ponerse en contacto con el usuario, el número de teléfono del usuario, el número de departamento del usuario y la ciudad en la que éste reside.
<b>DN, Diffie-Hellman</b>	Protocolo de criptografía de clave pública que permite a dos partes establecer un secreto compartido a través de canales de comunicaciones que no son seguros. Diffie-Hellman se utiliza en Intercambio de claves por Internet ( <a href="#">IKE</a> ) para establecer claves de sesión y es un componente del intercambio de claves <a href="#">Oakley</a> .
<b>DNS</b>	Domain Name System (Sistema o servicio de nombres de dominio). Servicio de Internet que traduce nombres de dominios compuestos por letras, en direcciones IP compuestas por números.
<b>DPD</b>	Detección del par muerto. DPD determina si un par todavía está activo enviando mensajes “keepalive” periódicos al par que se supone debe responder. Si el par no responde en un tiempo especificado, se finaliza la conexión.
<b>DRAM</b>	Dynamic Random Access Memory (Memoria de acceso aleatorio dinámica). Memoria RAM que almacena información en capacitadores que deben actualizarse periódicamente.
<b>DSCP</b>	Differentiated Services Code Point (Punto de código de servicios diferenciados). Los marcados de DSCP se pueden usar para clasificar el tráfico de <a href="#">QoS</a> . Consulte también <a href="#">NBAR</a> .

<b>DSLAM</b>	Digital Subscriber Line Access Multiplexer (Multiplexor de acceso a la línea de suscriptor digital).
<b>DSS</b>	Digital Signature Standard (Estándar de firma digital). Denominado también <i>DSA</i> (Digital Signature Algorithm, algoritmo de firma digital), el algoritmo DSS forma parte de varios estándares de clave pública para firmas criptográficas.
<b>duración de la clave</b>	Atributo de un par de claves que especifica un período de tiempo durante el cual se considera válido el certificado que contiene el componente público de dicho par de claves.

---

## E

<b>EAPoUDP</b>	Protocolo de autenticación extensible sobre protocolo de datagrama de usuario (UDP). EOU en su forma abreviada. Este protocolo lo utiliza un cliente y un <a href="#">NAD</a> para realizar la validación de <a href="#">gestión de estado</a> .
<b>Easy VPN</b>	Una solución de gestión VPN centralizada basada en Cisco Unified Client Framework. Un Easy VPN de Cisco consta de dos componentes: un cliente Easy VPN remoto de Cisco y un servidor Easy VPN de Cisco.
<b>ECHO</b>	Consulte <a href="#">ping</a> , <a href="#">ICMP</a> .
<b>eDonkey</b>	También conocido como eDonkey 2000 o ED2K, es una red sumamente grande para compartir archivos entre pares. eDonkey implementa el protocolo de transmisión de archivos de origen múltiple (MFTP).
<b>EIGRP</b>	EIGRP (Enhanced Interior Gateway Routing Protocol). Versión avanzada de IGRP desarrollada por Cisco Systems. Proporciona eficiencia de rendimiento y propiedades de convergencia superiores, además de combinar las ventajas de los protocolos de estado de enlace con las de los protocolos de vectores de distancia.
<b>encapsulación</b>	Ajuste de datos en un encabezado de protocolo particular. Por ejemplo, los datos de Ethernet se ajustan en un encabezado de Ethernet específico antes del tránsito de red. Asimismo, cuando se establece un bridge entre redes diferentes, toda la estructura de una red se coloca simplemente en el encabezado que utiliza el protocolo de nivel de enlace de los datos de la otra red.

<b>enrutamiento dinámico</b>	Enrutamiento que se ajusta automáticamente a la topología de red o cambios de tráfico. También se denomina “enrutamiento adaptativo”.
<b>enrutamiento RFC 1483</b>	<p>RFC1483 describe dos métodos diferentes de transportar tráfico de interconexión de red sin conexión a través de una red ATM: unidades de datos de protocolo enrutadas (PDU) y PDU con bridge. Cisco SDM admite la configuración del enrutamiento RFC 1483 y permite configurar dos tipos de encapsulación: AAL5MUX o AAL5SNAP.</p> <p><b>AAL5MUX:</b> la encapsulación AAL5 MUX sólo admite un único protocolo (IP o IPX) por PVC.</p> <p><b>AAL5SNAP:</b> la encapsulación AAL5 LLC/SNAP (Logical Link Control/Subnetwork Access Protocol) admite ARP inverso e incorpora el LLC/SNAP que precede al datagrama de protocolo. Esto permite a los diversos protocolos atravesar la misma PVC.</p>
<b>ERR</b>	Event Risk Rating (Índice de riesgo de evento). ERR se usa para controlar el nivel en que un usuario elige tomar medidas para minimizar los positivos falsos.
<b>ESP</b>	Encapsulating Security Payload (Carga útil de seguridad encapsulada). Protocolo IPSec que proporciona confidencialidad e integridad de datos. Conocido también como Encapsulating Security Payload, ESP proporciona confidencialidad, autenticación del origen de los datos, detección de reproducciones, integridad sin conexión, integridad de secuencias parciales y confidencialidad del flujo de tráfico limitado.
<b>esp-3des</b>	Transformación de ESP (Encapsulating Security Payload) con el algoritmo de cifrado DES de 168 bits (3DES o Triple DES).
<b>esp-des</b>	Transformación de ESP (Encapsulating Security Payload) con el algoritmo de cifrado DES de 56 bits.
<b>ESP-MD5-HMAC</b>	Transformación de ESP (Encapsulating Security Payload) con el algoritmo de autenticación SHA de variante MD5.
<b>esp-null</b>	Transformación de ESP (Encapsulating Security Payload) que no proporciona cifrado ni confidencialidad.



<b>ESP_SEAL</b>	ESP con el algoritmo de cifrado SEAL (algoritmo de cifrado de software) de clave de 160 bits. Esta versión se introdujo en la versión 12.3(7)T. Para poder utilizar esta función, es preciso que el router no tenga el cifrado IPSec de hardware activado.
<b>ESP-SHA-HMAC</b>	Transformación de ESP (Encapsulating Security Payload) con el algoritmo de autenticación SHA de variante HMAC.
<b>estado, completa de estado, Inspección completa de estado</b>	Los protocolos de red mantienen determinados datos, llamados información de estado, a ambos extremos de una conexión de red entre dos hosts. La información de estado es necesaria para implementar funciones de protocolo como, por ejemplo, envíos garantizados de paquetes, secuenciación de datos, control de flujo e ID de sesión o de transacción. En cada paquete se envía información de estado del protocolo mientras se utiliza cada protocolo. Por ejemplo, un explorador Web conectado a un servidor Web utilizará HTTP y los protocolos TCP/IP compatibles. Cada nivel de protocolo mantiene información de estado en los paquetes que envía y recibe. Los routers inspeccionan la información de estado de cada paquete para verificar que ésta se encuentra actualizada y es válida para todos los protocolos que contiene. Esta operación recibe el nombre de “inspección completa de estado” y ha sido diseñada para crear una potente barrera ante determinados tipos de amenazas contra la seguridad de los equipos.
<b>Ethernet</b>	Protocolo LAN ampliamente utilizado, inventado por Xerox Corporation y desarrollado por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet utilizan CSMA/CD y se ejecutan a través de una variedad de tipos de cables a 10 Mbps o 100 Mbps. Ethernet es similar a la serie de estándares IEEE 802.3.
<b>extremo descendente</b>	El extremo de transmisión ascendente del túnel.
<b>extremo descendente</b>	El extremo de recepción descendente de un túnel.

---

**F**

<b>fasttrack</b>	Red para compartir archivos en que las funciones de indización se asignan dinámicamente a los pares conectados, llamados supernodos.
<b>fecha de vencimiento</b>	La fecha de vencimiento indicada en un certificado o clave indica el final de su duración. Dicho certificado o clave dejarán de ser fiables una vez haya pasado la fecha de vencimiento.
<b>finger</b>	Herramienta de software que sirve para determinar si una persona tiene una cuenta en un sitio Internet específico. Varios sitios no permiten solicitudes de finger entrantes.
<b>firewall</b>	Un router o servidor de acceso, o varios de ellos, designados como búfer entre cualquier red pública conectada y una red privada. Un router que actúe como firewall utilizará listas de acceso así como otros métodos para asegurarse de la seguridad de la red privada.
<b>firma</b>	Elemento de datos en IOS IPS que detecta un patrón específico de uso incorrecto en la red.
<b>firma digital</b>	Método de autenticación que permite descubrir fácilmente las falsificaciones de datos y evita la repudiación. Asimismo, el uso de firmas digitales permite verificar que una transmisión se ha recibido intacta. Por lo general, se incluye un sello de la hora de transmisión.
<b>firmas RSA</b>	Uno de los tres métodos de autenticación ofrecidos en IPSec; los otros dos son “nonces” cifrados mediante RSA y claves previamente compartidas. Asimismo, se trata de uno de los tres FIPS (Federal Information Processing Standards) o algoritmos aprobados para generar y verificar firmas digitales. Los otros algoritmos aprobados son DSA y Elliptic Curve DSA.
<b>Flash memoria flash</b>	Chip de memoria que conserva datos sin electricidad. Según el caso, se pueden almacenar y escribir imágenes de software en la memoria flash, así como arrancar las imágenes desde dicha memoria.

<b>Frame Relay</b>	Protocolo del nivel de enlace de los datos conmutados, estándar del sector, que gestiona varios circuitos virtuales mediante encapsulación HDLC entre dispositivos conectados. Frame Relay es más eficiente que X.25, protocolo del que generalmente se considera un sustituto.
<b>FTP</b>	File Transfer Protocol (Protocolo de transferencia de archivos). Parte de la pila del protocolo TCP/IP utilizada para transferir archivos entre hosts.

---

## G

<b>gateway por defecto</b>	El gateway de última oportunidad. Gateway al que se enruta el paquete cuando la dirección de destino no coincide con ninguna entrada de la tabla de enrutamiento.
<b>Gateway SSL VPN</b>	Un gateway de WebVPN proporciona una dirección IP y un certificado para un contexto de WebVPN. La
<b>gestión de claves</b>	Creación, distribución, autenticación y almacenamiento de claves de cifrado.
<b>gestión de estado</b>	En una implementación <a href="#">NAC</a> , el estado de un host que intenta acceder a la red. El software de agente de gestión de estado que se ejecuta en el host se comunica con el <a href="#">NAD</a> para informar del cumplimiento del host de la política de seguridad de la red.
<b>global externa</b>	Dirección IP asignada a un host situado fuera de la red por el propietario de dicho host. La dirección se ha asignado desde una dirección enrutable globalmente o un espacio de red.
<b>global interna</b>	Dirección IP de un host situado dentro de una red, tal y como aparece para los dispositivos situados fuera de ésta.
<b>gnutella</b>	Protocolo descentralizado para compartir archivos P2P. Mediante un cliente Gnutella instalado, los usuarios pueden buscar, descargar y subir archivos en Internet.

- GRE** Generic Routing Encapsulation (Encapsulación genérica de enrutamiento)  
Protocolo de creación de túneles desarrollado por Cisco que puede encapsular una amplia variedad de tipos de paquetes de protocolos dentro de túneles IP, creando un enlace de punto a punto virtual a routers de Cisco situados en puntos remotos de una interred IP. Gracias a la conexión de subredes de varios protocolos a un entorno con una base de protocolo único, la creación de túneles IP mediante GRE permite la expansión de la red en un entorno de protocolo único.
- GRE sobre IPSec** Esta tecnología usa IPSec para cifrar paquetes GRE.
- G.SHDSL** Conocido también como G.991.2, G.SHDSL es un estándar internacional para DSL simétrica desarrollado por la International Telecommunications Union. G.SHDSL se ocupa de enviar y recibir flujos de datos simétricos a alta velocidad a través de un único par de cables de cobre a velocidades que oscilan entre 192 kbps y 2,31 Mbps.
- 
- H**
- H.323** Estándar que permite realizar videoconferencias a través de LAN (redes de área local) y otras redes conmutadas de paquetes, así como vídeo por Internet.
- hash** Proceso unidireccional que convierte las entradas de cualquier tamaño en salidas de suma de comprobación de tamaño fijo llamadas *message digest* o simplemente *digest*. Este proceso no es reversible, por lo que no se pueden crear ni modificar datos para obtener un digest específico.
- HDLC** High-Level Data Link Control (Control del enlace de datos de alto nivel). Protocolo de nivel de enlace de los datos síncrono y orientado a bits desarrollado por la ISO (International Standards Organization). HDLC especifica un método de encapsulación de datos en enlaces en serie síncronos mediante sumas de comprobación y caracteres de trama.
- HMAC** Código de autenticación de mensajes basado en funciones hash criptográficas. HMAC puede usarse con cualquier función hash criptográfica iterativa como, por ejemplo, MD5, SHA-1, combinada con una clave compartida secreta. La fuerza criptográfica de HMAC dependerá de las propiedades de la función hash subyacente.

<b>HMAC-MD5</b>	Códigos de autenticación de mensajes basados en hash con MD5 (RFC 2104). Versión con clave de MD5 que permite a dos partes validar la información transmitida mediante un secreto compartido.
<b>host</b>	Equipo, como un PC u otro dispositivo informático como un servidor, asociado a una dirección IP individual y, opcionalmente, a un nombre. Nombre de cualquier dispositivo en una red TCP/IP que tenga una dirección IP. Asimismo, cualquier dispositivo de una red al que se pueda asignar una dirección. El término <i>nodo</i> incluye dispositivos como routers e impresoras que, normalmente, no se denominan <i>hosts</i> .
<b>host proxy de suscripción</b>	Servidor proxy de un servidor de suscripción de certificados.
<b>HTTP</b>	Hypertext Transfer Protocol (Protocolo de transferencia de hipertexto),
<b>HTTPS</b>	Hypertext Transfer Protocol, Secure (Protocolo de transferencia de hipertexto seguro). Protocolo utilizado por los exploradores y servidores Web para transferir archivos como archivos de texto o de gráficos.
<b>hub</b>	En una red <a href="#">DMVPN</a> el hub es un enrutador con una conexión <a href="#">IPSec</a> punto a punto a todos los routers spoke de la red. Se trata del centro lógico de una red DMVPN.
<b>huella dactilar</b>	La “huella dactilar” de un certificado de la CA es la cadena de caracteres alfanuméricos que se obtiene de un hash MD5 de todo el certificado CA. Las entidades que reciban un certificado de la CA pueden verificar su autenticidad comparándolo con su “huella dactilar” conocida. El objetivo de esta autenticación es asegurarse de la integridad de las sesiones de comunicación evitando ataques del tipo “man-in-the-middle”.
<hr/>	
<b>ICMP</b>	Internet Control Message Protocol (Protocolo de mensajes de control por Internet). Protocolo de Internet de nivel de red que informa sobre los errores y proporciona otra información pertinente al procesamiento de paquetes IP.
<b>identidad del certificado</b>	Un certificado X.509 contiene información relativa a la identidad del dispositivo o entidad que lo posee. En cada instancia posterior de verificación de pares y autenticación, se examina la información de identificación. No obstante, las identidades de los certificados pueden ser objeto de ataques de spoofing.

<b>IDM</b>	IDS Device Manager (Administrador del dispositivo IDS) IDM es software que se utiliza para gestionar sensores IDS.
<b>IDS</b>	Sistema de detección de intrusiones Cisco IPS ejecuta un análisis en tiempo real del tráfico de red a fin de detectar anomalías y usos erróneos por medio de una biblioteca de firmas con la que puede comparar el tráfico. Cuando encuentra anomalías o actividad no autorizada, puede terminar la condición, bloquear tráfico de hosts atacantes y enviar alertas al IDM.
<b>IEEE</b>	Institute of Electrical and Electronics Engineers (Instituto de ingenieros en electricidad y electrónica).
<b>IETF</b>	Internet Engineering Task Force (Grupo de trabajo de ingeniería de Internet).
<b>IGMP</b>	Internet Group Management Protocol (Protocolo de administración de grupos de Internet). IGMP es un protocolo usado por los sistemas IPv4 para informar acerca de la pertenencia a multidifusiones IP a los routers de multidifusión cercanos
<b>IKE</b>	Internet Key Exchange (Intercambio de claves por Internet). Se trata de un estándar de protocolo de gestión de claves usado junto con IPSec y otros estándares. Se puede configurar IPSec sin IKE, aunque lo mejora proporcionando funciones adicionales, flexibilidad y facilidad de configuración para el estándar IPSec. IKE permite autenticar los pares IPSec, negocia claves IPSec y asociaciones de seguridad IPSec.  Para que pueda pasar tráfico IPSec, es preciso que cada router, firewall o host pueda verificar la identidad de su par. Esta operación puede efectuarse manualmente mediante la introducción de claves previamente compartidas o un servicio de la CA. IKE es un protocolo híbrido que implementa los intercambios de claves Oakley y Skeme dentro de la infraestructura ISAKMP (Internet Security Association and Key Management Protocol). ISAKMP, Oakley y Skeme son protocolos de seguridad implementados por IKE.
<b>IM</b>	Mensajería instantánea. Servicio de comunicación en tiempo real en que ambas partes están en línea al mismo tiempo. Los servicios de IM más populares son Yahoo! Messenger (YM), Microsoft Networks Messenger y AOL Instant Messenger (AIM).

<b>IMAP</b>	Internet Control Message Protocol (Protocolo de mensajes de control por Internet). Protocolo utilizado por los clientes para comunicarse con un servidor de correo electrónico. Definido en RFC 2060, IMAP permite que los clientes eliminen, cambien el estado y manipulen mensajes en el servidor de correo electrónico, además de recuperarlos.
<b>índice de fidelidad</b>	Número entre 1 y 100 que indica el nivel de confianza que tiene el evaluador con respecto a que la firma generará una alerta precisa.
<b>integridad de datos</b>	Supuesta precisión de los datos transmitidos; es decir, autenticidad del remitente y ausencia de alteración de datos.
<b>intercambio de claves</b>	Método seguido por dos o más partes para intercambiar claves de cifrado. El protocolo IKE proporciona uno de tales métodos.
<b>Intercambio de claves Diffie-Hellman</b>	Protocolo de criptografía de clave pública que permite a dos partes establecer un secreto compartido a través de canales de comunicación que no son seguros. Diffie-Hellman se utiliza en Intercambio de claves por Internet ( <a href="#">IKE</a> ) para establecer claves de sesión y es un componente del intercambio de claves <a href="#">Oakley</a> . El software de Cisco IOS admite grupos Diffie-Hellman de 768 bits y 1.024 bits.
<b>interfaz</b>	Conexión física entre una red determinada y el router. La interfaz de LAN del router se conecta con la red local a la que proporciona servicio el router. El router cuenta con una o varias interfaces WAN que se conectan con Internet.
<b>Interfaz de capa 3</b>	La interfaz de capa 3 admite el enrutamiento de interred. VLAN es un ejemplo de una interfaz de capa 3 lógica. Un puerto Ethernet es un ejemplo de una interfaz de capa 3 física.
<b>interfaz física</b>	Interfaz de router admitida por un módulo de red instalada en el chasis del router o que forma parte del hardware básico del router.
<b>interfaz lógica</b>	Interfaz creada únicamente por configuración, que no es una interfaz física del router. Las interfaces de marcación y las de túnel son interfaces lógicas.
<b>Internet</b>	Red global que utiliza IP, protocolos de Internet. No se trata de una LAN. Consulte también <a href="#">intranred</a> .
<b>intranred</b>	Red interna. <a href="#">LAN</a> que utiliza <a href="#">IP</a> , y protocolos de Internet como, por ejemplo <a href="#">SNMP</a> , <a href="#">FTP</a> y <a href="#">UDP</a> . Consulte también <a href="#">red</a> , <a href="#">Internet</a> .

<b>IOS</b>	Software de Cisco IOS. Software del sistema Cisco que proporciona funciones comunes, escalabilidad y seguridad para todos los productos de la arquitectura CiscoFusion. Cisco IOS permite una instalación automatizada, integrada y centralizada, así como la gestión de intrarredes. Por otro lado, permite asegurar la compatibilidad de una amplia variedad de protocolos, soportes, servicios y plataformas.
<b>IOS IPS</b>	Sistema de prevención de intrusiones de Cisco IOS. IOS IPS compara el tráfico con una amplia base de datos de firmas de intrusión y puede rechazar los paquetes intrusos, así como ejecutar otras acciones, basándose en la configuración. Las firmas están incorporadas en las imágenes del IOS que admiten esta función y se pueden almacenar firmas adicionales en archivos de firmas locales o remotos.
<b>IPS</b>	
<b>IP</b>	Protocolo de Internet. Los protocolos de Internet son la familia de protocolos de sistema abierto (no de propiedad) más conocida del mundo ya que pueden utilizarse para establecer una comunicación entre cualquier conjunto de redes interconectadas y sirven tanto para comunicaciones WAN como LAN.
<b>IPSec</b>	Infraestructura basada en estándares abiertos que brinda confidencialidad, integridad y autenticación de datos entre pares participantes. IPSec proporciona estos servicios de seguridad en el nivel de IP. Por otro lado, utiliza IKE para gestionar la negociación de protocolos y algoritmos basada en la política local y para generar las claves de cifrado y de autenticación que IPSec utilizará. IPSec puede emplearse para proteger uno o varios flujos de datos entre un par de host, entre un par de gateways de seguridad o entre una gateway de seguridad y un host.
<b>IRB</b>	Enrutamiento o establecimiento de bridge integrado. IRB permite enrutar un protocolo concreto entre interfaces enrutadas y grupos de puentes con un único router de switch.
<b>ISAKMP</b>	Internet Security Association and Key Management Protocol (Protocolo de la asociación de seguridad en Internet y gestión de claves) es la base de IKE. ISAKMP autentica los pares que se comunican, crea y gestiona asociaciones de seguridad y define técnicas de generación de claves.

---

**K**

<b>kazaa2</b>	Servicio para compartir archivos par a par.
---------------	---



---

**L**

<b>L2TP</b>	Layer 2 Tunneling Protocol (Protocolo de arquitectura de túneles de nivel 2). Protocolo de seguimiento de estándares IETF (Internet Engineering Task Force) definido en RFC 2661 que proporciona la creación de túneles de PPP. Basado en las mejores funciones de L2F y PPTP, L2TP proporciona un método de implementación de VPDN operativo en todo el sector. Se ha propuesto L2TP como alternativa a IPSec, aunque en ocasiones se utiliza junto con IPSec para proporcionar servicios de autenticación.
<b>LAC</b>	L2TP Access Concentrator (Concentrador de acceso L2TP) Dispositivo que termina las llamadas a sistemas remotos y sesiones de túnel PPP entre sistemas remotos y LNS.
<b>LAN</b>	Local Area Network (Red de área local). Red que reside en una ubicación o pertenece a una organización y que normalmente, aunque no siempre, utiliza protocolos IP u otros protocolos de Internet. No se trata de Internet global. <i>Consulte también <a href="#">intranet</a>, <a href="#">red</a>, <a href="#">Internet</a>.</i>
<b>LAPB</b>	Link Access Procedure, Balanced (Proceso de acceso a enlaces con balance).
<b>LBO</b>	Line Build Out (Adición de resistencia a líneas).
<b>LEFS</b>	Sistema de archivos de valor mínimo.
<b>lista de excepciones</b>	En una implementación de <a href="#">NAC</a> , lista de hosts con direcciones estáticas con permiso para omitir el proceso NAC. Estos hosts pueden estar en la lista de excepciones ya que no tienen instalados agentes de <a href="#">gestión de estado</a> , o debido a que son hosts del tipo impresora o teléfonos IP de Cisco.
<b>lista de revocaciones de certificados (CRL) X.509.</b>	Lista de los números de certificado revocados. Una CRL X.509 es aquella que cumple una de las dos definiciones de formato CRL en X.509.
<b>LLQ</b>	Low latency queuing (Servicio de cola de baja latencia).
<b>LNS</b>	L2TP network server (Servidor de red L2TP). Dispositivo que puede terminar túneles L2TP desde un LAC y sesiones PPP a sistemas remotos mediante sesiones de datos L2TP.

<b>local exterior</b>	Dirección IP de un host exterior tal como aparece para la red interior. No es obligatorio que sea una dirección legítima; se trata de una dirección asignada desde un espacio de dirección enrutable en el interior.
<b>local interna</b>	Dirección IP configurada asignada a un host situado dentro de la red.
<b>longevidad de la asociación de seguridad</b>	Tiempo predeterminado durante el cual una SA está en vigor.

---

## M

<b>MAC</b>	Message Authentication Code (Código de autenticación de mensajes). Suma de comprobación criptográfica del mensaje utilizada para verificar la autenticidad del mismo. Consulte <a href="#">hash</a> .
<b>mapa criptográfico</b>	En Cisco SDM, los mapas criptográficos especifican qué tráfico debe proteger IPSec, adónde tiene que enviarse este tráfico protegido y qué conjuntos de transformación de IPSec deben aplicarse a este tráfico.
<b>mapa de clase</b>	
<b>mapa de parámetro</b>	Los mapas de parámetros especifican el comportamiento de inspección del firewall de política de zona con los parámetros como protección de denegación de servicio, temporizadores de sesión y conexión, y configuración de registro. Los mapas de parámetros también se pueden aplicar a los mapas de clase y política de capa 7 para definir el comportamiento específico de la aplicación, como objetos HTTP, requisitos de autenticación POP3 e IMAP, y otra información específica de la aplicación.
<b>mapa de política</b>	Un mapa de política consta de acciones configuradas que se tomarán con respecto al tráfico. El tráfico se define en los mapas de clases asociadas.
<b>mapa de ruta</b>	Los mapas de ruta permiten controlar la información que se agrega a la tabla de enrutamiento. Cisco SDM crea automáticamente mapas de ruta para evitar que NAT traduzca direcciones de origen específicas, cuando esto impidiese que algunos paquetes cumplieran criterios de una regla IPSec.

<b>máscara</b>	Máscara de 32 bits que especifica cómo se deberá dividir una dirección de Internet en las partes correspondientes a red, subred y host. La máscara de red tiene unos (1) en las posiciones de los bits de la dirección de 32 bits que deben utilizarse para las partes de la red y de la subred, mientras que tiene ceros (0) para la parte correspondiente al host. La máscara debe contener como mínimo la porción de la red estándar (tal como determina la clase de dirección) y el campo subred debe estar al lado de la porción correspondiente a la red. La máscara se configura con el decimal equivalente del valor binario.
<b>máscara de subred</b>	
<b>máscara de red</b>	
<b>máscara de red</b>	

### Ejemplos:

Decimal: 255.255.255.0

Binario: 11111111 11111111 11111111 00000000

Los primeros 24 bits proporcionan la dirección de red y de subred, mientras que los últimos 8 indican la dirección de host.

Decimal: 255.255.255.248

Binario: 11111111 11111111 11111111 11111000

Los primeros 29 bits proporcionan la dirección de red y de subred, mientras que los últimos 3 indican la dirección de host.

Consulte también [Dirección IP](#), [TCP/IP](#), [host](#), [host/red](#).

<b>máscara comodín</b>	Máscara de bits utilizada en las reglas de acceso, las reglas IPsec y las reglas NAT para especificar las porciones de la dirección IP del paquete que deben coincidir con la dirección IP de la regla. Una máscara inversa contiene 32 bits, el mismo número de bits que una dirección IP. Un valor de bit de 0 en una máscara comodín especifica que el bit situado en la misma posición de la dirección IP del paquete debe coincidir con el bit indicado en la dirección IP de la regla. El valor 1 especifica que el bit correspondiente de la dirección IP del paquete puede ser 1 ó 0; es decir, que a la regla “le es indiferente” el valor del bit. Una máscara inversa de 0.0.0.0 especifica que los 32 bits de la dirección IP del paquete deben coincidir con la dirección IP de la regla. Una máscara inversa de 0.0.255.0 especifica que 16 primeros bits y los 8 últimos bits deben coincidir, pero que el tercer octeto puede tener cualquier valor. Si la dirección IP de una regla es 10.28.15.0 y la dirección de la máscara es 0.0.255.0, la dirección IP 10.28.88.0 coincidirá con la dirección IP de la regla y la dirección IP 10.28.15.55 no coincidirá.
------------------------	--

<b>MD5</b>	Message Digest 5. Función de hash unidireccional que produce un hash de 128 bits. Tanto MD5 como el algoritmo de hash seguro (SHA) son variaciones en MD4 y están diseñados para reforzar la seguridad del algoritmo de hash MD4. Cisco utiliza hash para tareas de autenticación dentro de la estructura de IPSec. MD5 verifica la integridad y autentica el origen de una comunicación.
<b>MD5</b>	Message Digest 5. Algoritmo de hash unidireccional que produce un hash de 128 bits. Tanto MD5 como el algoritmo de hash seguro (SHA) son variaciones en MD4 y están diseñados para reforzar la seguridad del algoritmo de hash MD4. Cisco utiliza hash para tareas de autenticación dentro de la estructura de IPSec. También se utiliza para autenticar mensajes en SNMP v.2. MD5 verifica la integridad de la comunicación, autentica el origen y comprueba la escala de tiempo.
<b>message digest</b>	Cadena de bits que representa un bloque de datos más grande. Esta cadena define un bloque de datos basándose en el proceso de su contenido preciso mediante una función hash de 128 bits. Los message digests se utilizan para generar firmas digitales. Consulte <a href="#">hash</a> .
<b>mGRE</b>	Multipunto <a href="#">GRE</a> .
<b>modo agresivo</b>	Modo que se establece en SA de ISAKMP que simplifica la negociación IKE (fase 1) entre dos o varios pares IPSec. El modo agresivo es más rápido que el modo principal, aunque no es tan seguro. Consulte “modo principal” y “modo rápido”.
<b>modo rápido</b>	En Oakley, nombre del mecanismo utilizado después de establecer una asociación de seguridad para negociar los cambios en los servicios de seguridad como, por ejemplo, claves nuevas.
<b>módulo de red</b>	Tarjeta de interfaz de red instalada en el chasis del router para agregar funciones a éste. Los módulos de red Ethernet e <a href="#">IDS</a> son ejemplos de ello.
<b>motor de firmas</b>	Un motor de firmas es un componente de IOS IPS diseñado para admitir varias firmas en cierta categoría. Un motor se compone de un analizador y un inspector. Cada motor cuenta con un conjunto de parámetros legales que tienen intervalos o conjuntos de valores permitidos.
<b>MTU</b>	Maximum Transmission Unit (Unidad de transmisión máxima) Tamaño de paquete máximo, indicado en bytes, que puede transmitir o recibir una interfaz.

---

<b>N</b>	
<b>NAC</b>	Network Admission Control (Control de admisión a la red). Método para controlar el acceso a una red y evitar la entrada de virus informáticos. Mediante diferentes protocolos y productos de software, NAC verifica el estado de los hosts cuando intentan acceder a la red y gestiona la petición según el estado del host, denominado <i>gestión de estado</i> . Los hosts infectados se pueden colocar en cuarentena; a los hosts sin software de protección contra virus actualizado se les puede pedir que obtengan actualizaciones, y a los hosts no infectados con protección contra virus actualizada se les puede permitir el acceso a la red. Consulte también <a href="#">ACL</a> , <a href="#">gestión de estado</a> y EAPoUDP.
<b>NAD</b>	Network Access Device (Dispositivo de acceso a la red). En una implementación de NAC, el dispositivo que recibe una petición del host para iniciar sesión en la red. Un NAD, por lo general un router, colabora con el software del agente de gestión de estado que se ejecuta en el host, con el software de protección contra virus, así como con ACS y servidores de gestión y corrección de estado de la red para controlar el acceso a la misma y evitar las infecciones por virus informáticos.
<b>NAS</b>	Servidor de acceso a la red. Plataforma que actúa de interfaz entre Internet y la red telefónica pública conmutada (PSTN).  Gateway que conecta dispositivos asíncronos a una LAN o WAN mediante software de emulación de terminales y redes. Ejecuta el enrutado síncrono y asíncrono de los protocolos admitidos.
<b>NAT</b>	Network Address Translation (Traducción de direcciones de red). Mecanismo que sirve para reducir la necesidad de utilizar direcciones IP globalmente únicas. NAT permite a una organización con direcciones que no son globalmente únicas conectarse a Internet traduciendo dichas direcciones a un espacio de dirección que puede enrutarse globalmente.
<b>Traducción de direcciones de red</b>	
<b>NBAR</b>	Network-based Application Recognition (Reconocimiento de aplicaciones basadas en la red). Método utilizado para clasificar el tráfico de <a href="#">QoS</a> .
<b>Negociación de IKE</b>	Método para efectuar intercambios seguros de claves privadas en redes que no son seguras.

<b>NetFlow</b>	Función de algunos routers que les permite dividir en categorías de flujos los paquetes entrantes. Dado que los paquetes de un flujo a menudo se pueden tratar igual, esta clasificación se puede utilizar para saltar parte del trabajo del router y acelerar su operación de cambio.
<b>NHRP</b>	Next Hop Resolution protocol (Protocolo de resolución de próximo salto). Protocolo de cliente y servidor utilizado en redes <a href="#">DMVPN</a> , en el que el router hub es el servidor y los spokes son los clientes. El hub mantiene una base de datos NHRP de las direcciones de la interfaz pública de cada spoke. Cada uno de éstos registra su dirección real cuando arranca y consulta a la base de datos NHRP cuáles son las direcciones reales de los spokes de destino para crear túneles directos a ellos.
<b>no cifrado</b>	Sin cifrar.
<b>nombre de dominio</b>	Nombre familiar y fácil de recordar de un host de Internet que corresponde a la dirección IP.
<b>NTP</b>	Network Time Protocol (Protocolo de hora de red). Protocolo que permite sincronizar los relojes del sistema en dispositivos de la red. NTP es un protocolo <a href="#">UDP</a> .
<b>NVRAM</b>	Non-volatile random access memory (Memoria de acceso aleatorio no volátil).

---

## O

<b>Oakley</b>	Protocolo basado en Diffie-Hellman y diseñado para ser un componente compatible de ISAKMP, que permite establecer claves secretas para que las utilicen las partes autenticadas.
<b>OFB</b>	Output Feedback (Retroalimentación de salida). Función de IPsec que vuelve a alimentar salida cifrada (por lo general cifrada por DES, aunque no necesariamente) en la entrada original. El texto sin formato se cifra directamente con la clave simétrica. Esto produce un flujo de números pseudoaleatorios.
<b>OSPF</b>	Open Shortest Path First (Abrir la ruta más corta en primer lugar). Algoritmo de enrutamiento IGP jerárquico de estado de enlace propuesto como sucesor a RIP en la comunidad de Internet. Entre las funciones de OSPF figuran el enrutamiento menos costoso y de varias vías y el balance de cargas.

---

<b>P</b>	
<b>P2P</b>	Consulte <a href="#">Par-a-Par</a> .
<b>PAD</b>	Packet Assembler/Disassembler (Ensamblador/desensamblador de paquetes). Dispositivo utilizado para conectar dispositivos sencillos (como terminales de modo de carácter) que no admiten las funciones completas de un protocolo determinado en una red. Los PAD colocan en búfer los datos y ensamblan y desensamblan los paquetes enviados a tales dispositivos finales.
<b>PAM</b>	Port to Application Mapping (Asignación puerto a aplicación). PAM permite personalizar los números de puertos TCP o UDP para los servicios o aplicaciones de la red. El PAM utiliza esta información para admitir entornos de red que ejecuten servicios utilizando puertos que no sean los puertos registrados o conocidos asociados con una aplicación.
<b>PAP</b>	Password Authentication Protocol (Protocolo de autenticación de contraseña). Permite a los pares autenticarse entre sí. PAP pasa la contraseña y el nombre de host o de usuario sin cifrar. Consulte también CHAP.
<b>par</b>	En IKE, los pares son routers que actúan como proxies para los participantes en un túnel IKE. En IPSec, los pares son dispositivos o entidades que se comunican con seguridad ya sea mediante el intercambio de claves o de certificados digitales.
<b>Par-a-Par</b>	Tipo de diseño de red en que todos los hosts comparten capacidades aproximadamente equivalentes. También conocido como P2P; muchas redes para compartir archivos utilizan las redes par a par.
<b>par de claves</b>	Consulte <a href="#">cifrado de clave pública</a> .
<b>par de zonas</b>	Un par de zonas le permite especificar un flujo de tráfico unidireccional entre dos zonas de seguridad. Consulte también zona de seguridad
<b>PAT</b>	Port Address Translation (Traducción de direcciones de puerto). La PAT dinámica permite que parezca que varias sesiones salientes se originan en una sola <a href="#">dirección IP</a> . Con PAT activada, el router selecciona un número de puerto único desde la dirección IP de PAT para cada ranura de traducción saliente (xlate). Esta función es útil cuando el proveedor de servicios de Internet no puede asignar suficientes direcciones IP únicas a conexiones salientes. Antes de utilizar una dirección PAT, se recurre a las direcciones del conjunto global.
<b>PAT dinámico</b>	

<b>PAT estática</b>	Static Port Address Translation (Traducción de direcciones de puerto estática). Una dirección estática asigna una dirección IP local a una dirección IP global. Una PAT estática es una dirección estática que también asigna un puerto local con un puerto global. Consulte también <a href="#">PAT</a> .
<b>PEM</b>	Formato de correo con privacidad mejorada. Formato de almacenamiento de certificados digitales.
<b>Perfil IKE</b>	Grupo de parámetros de <a href="#">ISAKMP</a> que se puede asignar a distintos túneles de seguridad IP.
<b>PFS</b>	Perfect Forward Secrecy (Confidencialidad directa perfecta). Propiedad de algunos protocolos de acuerdo de claves asimétricas que permiten el uso de diferentes claves en diferentes momentos de una sesión, a fin de asegurarse de que si se revela alguna clave, no se pondrá en peligro toda la sesión.
<b>ping</b>	Solicitud <a href="#">ICMP</a> enviada entre hosts para determinar si un host está accesible en la red.
<b>PKCS12</b>	Public Key Cryptography Standard Number 12 (Estándar de criptografía de clave pública número 12). Formato de almacenamiento de información de certificados digitales. Consulte también <a href="#">PEM</a> .
<b>PKCS7</b>	Public Key Cryptography Standard Number 7 (Estándar de criptografía de clave pública número 7).
<b>PKI</b>	Public-Key Infrastructure (Infraestructura de clave pública). Sistema de autoridades certificadoras (CA) y autoridades de registro (RA) que proporciona compatibilidad para utilizar una criptografía de claves asimétricas en la comunicación de datos mediante funciones como la gestión de certificados, archivos, claves y tokens.  Puede ser también cualquier estándar que permita el intercambio de claves asimétricas.  Este tipo de intercambio permite al destinatario del mensaje confiar en la firma de dicho mensaje y permite al remitente cifrarlo de forma adecuada para el destinatario elegido. Consulte gestión de claves



<b>política de reflejo de la VPN</b>	<p>Política VPN en un sistema remoto que contiene valores compatibles con una política local y que permite al sistema remoto establecer una conexión VPN con el sistema local. Algunos valores de la política de reflejo deben coincidir con los de la política local y algunos valores como, por ejemplo, la dirección IP del par, deben ser el valor inverso del valor correspondiente en la política local.</p> <p>Se pueden crear políticas de reflejo para que los administradores remotos las utilicen cuando configuren conexiones VPN de sitio a sitio. Para obtener información acerca de cómo generar una política de reflejo, consulte <a href="#">Generar el reflejo...</a></p>
<b>Política de grupo SSL VPN</b>	<p>Las políticas de grupo de WebVPN definen la página del portal y los enlaces para los usuarios incluidos en dichas políticas. Una política de grupo de WebVPN se configura en un contexto de WebVPN.</p>
<b>política IKE global</b>	<p>Política IKE que es general para todo un dispositivo, en vez de influir sólo en una única interfaz de dicho dispositivo.</p>
<b>política IPSec</b>	<p>En Cisco SDM, se denomina política IPSec a un conjunto con nombre de <a href="#">mapa criptográfico</a> asociado a una conexión VPN.</p>
<b>POP3</b>	<p>Post Office Protocol, versión 3. Protocolo utilizado para recuperar correos electrónicos desde servidores de correo electrónico.</p>
<b>PPP</b>	<p>Point-to-Point Protocol (Protocolo punto a punto). Proporciona conexiones de router a router y de host a red a través de circuitos síncronos y asíncronos. PPP posee mecanismos de seguridad incorporados como CHAP y PAP.</p>
<b>PPPoA</b>	<p>Protocolo punto a punto sobre Modo de transferencia asíncrona (ATM). Principalmente implementado como parte de ADSL, PPPoA se basa en RFC1483, operando en modo Logical Link Control-Subnetwork Access Protocol (LLC-SNAP) o VC-Mux.</p>
<b>PPPoE</b>	<p>Point-to-Point Protocol over Ethernet (Protocolo punto a punto sobre la encapsulación de Ethernet). PPP encapsulado en tramas de Ethernet. PPPoE permite a hosts de una red Ethernet conectarse a hosts remotos mediante un módem de banda ancha.</p>

- PPTP** Point-to-Point Tunneling Protocol (Protocolo de arquitectura de túneles punto a punto). Crea túneles iniciados por el cliente encapsulando paquetes en datagramas IP que se transmitirán a través de redes basadas en TCP/IP. Se puede utilizar como alternativa a los protocolos de arquitectura de túneles L2F y L2TP. Protocolo propiedad de Microsoft.
- Protocolo L2F** Layer 2 Forwarding Protocol (Protocolo de envío de nivel 2). Protocolo que admite la creación de redes de acceso telefónico privadas virtuales seguras en Internet.
- pseudoaleatorio** Secuencia ordenada de bits que superficialmente parece similar a una secuencia realmente aleatoria de los mismos bits. Se designa “nonce” a la clave generada a partir de un número pseudoaleatorio.
- PVC** Permanent Virtual Circuit or connection (Circuito o conexión Virtual Permanente). Circuito virtual establecido permanentemente. Los PVC permiten ahorrar ancho de banda asociado al establecimiento de circuitos y reducir el consumo en situaciones en las que es preciso que determinados circuitos virtuales existan permanentemente. En terminología ATM, recibe el nombre de conexión virtual permanente.

---

**Q**

- QoS** Quality of Service (Calidad de servicio). Método que permite garantizar el ancho de banda para tipos de tráfico especificados.

---

<b>R</b>	
<b>RA</b>	Registration Authority (Autoridad de registro). Entidad que actúa como componente opcional en los sistemas PKI y sirve para registrar o verificar información que las autoridades certificadoras (CA) utilizan cuando emiten certificados o ejecutan otras funciones de gestión de certificados. Es posible que la misma CA ejecute todas las funciones RA, aunque por lo general se mantienen separadas. Las tareas RA varían considerablemente, aunque pueden incluir la asignación de nombres completos, la distribución de tokens y la ejecución de funciones de autenticación personal.
<b>RADIUS</b>	Remote Authentication Dial-In User Service. Protocolo de cuentas y autenticación para servidor de acceso que utiliza UDP como protocolo de transporte. Consulte también <a href="#">TACACS+</a> .
<b>RCP</b>	Remote Copy Protocol (Protocolo de copia remota). Permite a los usuarios copiar archivos desde un sistema de archivos o a un sistema de archivos que reside en un host o servidor remoto de la red. El protocolo RCP utiliza TCP para asegurar una envío fiable de los datos.
<b>recuperación de claves</b>	Método fiable por el que la información cifrada se puede descifrar en caso de que se pierda o se destruya la clave de descifrado.
<b>red</b>	Una red es un grupo de dispositivos de computación que comparten parte de un espacio de la dirección IP y no un host único. Una red está formada por varios “nodos” o dispositivos con dirección IP, a los que es posible referirse como <i>hosts</i> . Consulte también Internet, Intranet, IP, LAN.
<b>regla</b>	Información agregada a la configuración para definir la política de seguridad en forma de declaraciones condicionales, que instruyen al router acerca de cómo reaccionar cuando se produce una situación determinada.
<b>regla de inspección</b>	Regla de inspección <a href="#">CBAC</a> que permite al router inspeccionar el tráfico saliente especificado para que pueda permitir el tráfico de vuelta del mismo tipo que está asociado a una sesión iniciada en la LAN. Si hay un firewall instalado y no se ha configurado una regla de inspección, es posible que se rechace el tráfico entrante asociado a una sesión iniciada dentro en el firewall.

<b>regla estándar</b>	En Cisco SDM, tipo de regla de acceso o regla NAT. Las reglas estándar comparan la dirección IP de origen de un paquete con sus criterios de dirección IP para determinar si se produce una coincidencia. Las reglas estándar utilizan máscaras inversas para determinar las partes de la dirección IP que deben coincidir.
<b>regla implícita</b>	Regla de acceso que el router crea automáticamente basándose en reglas por defecto o como consecuencia de reglas definidas por el usuario.
<b>regla IPSec</b>	Regla utilizada para especificar qué tráfico protegerá IPSec.
<b>reglas ampliadas</b>	Tipo de regla de acceso. Las reglas ampliadas pueden examinar una mayor variedad de campos del paquete para determinar una coincidencia. Las reglas ampliadas pueden examinar el origen de un paquete y las direcciones IP, el tipo de protocolo, los puertos de origen y de destino y otros campos del paquete.
<b>relleno</b>	En los sistemas criptográficos, <i>relleno</i> se refiere a caracteres aleatorios, espacios en blanco, ceros y nulos agregados al principio y al final de los mensajes, para ocultar la longitud real de éstos o para satisfacer los requisitos de tamaño de bloque de datos de algunos cifrados. El relleno también permite oscurecer la ubicación en la que realmente se inicia la codificación criptográfica.
<b>repudiación</b>	En los sistemas criptográficos, se entiende por “repudiación” la denegación efectuada por una de las entidades participantes en una comunicación, de haber participado en toda la comunicación o en parte de ella.
<b>retrobuclé</b>	En una prueba de retrobuclé, se envían señales y se redirigen a su origen, desde algún punto de la ruta de comunicaciones. Las pruebas de retrobuclé se utilizan a menudo para determinar la capacidad de uso de las interfaces de red.
<b>RIP</b>	Routing Information Protocol (Protocolo de información de enrutamiento). Protocolo de enrutamiento que utiliza el número de routers que un paquete debe atravesar para llegar a destino, como valor métrico de enrutamiento.
<b>ruta</b>	Ruta por una interred.
<b>RPC</b>	Remote Procedure Call (Llamada de procedimiento remoto). Las RPC son llamadas de procedimiento creadas o especificadas por los clientes y ejecutadas en los servidores y cuyos resultados se devuelven a los clientes a través de la red. Consulte también “arquitectura cliente/servidor”.

<b>RR</b>	Risk Rating (Índice de riesgo). RR es un valor entre 0 y 100 que representa la cuantificación numérica del riesgo asociado con un evento particular en la red.
<b>RSA</b>	Rivest, Shamir y Adelman, inventores de esta técnica de intercambio de claves criptográficas, basada en crear factor para grandes números. RSA también es el nombre de la técnica en sí, puede utilizarse para cifrar y autenticar y está incluido en varios protocolos de seguridad.
<b>ruta estática</b>	Ruta configurada explícitamente e introducida en la tabla de enrutamiento. Las rutas estáticas tienen preferencia ante las rutas elegidas por los protocolos de enrutamiento dinámico.

---

## S

<b>SA</b>	<p>Security Association (Asociación de seguridad). Conjunto de parámetros de seguridad sobre el que se ponen de acuerdo dos pares para proteger una sesión específica de un túnel en particular. Tanto IKE como IPSec utilizan SA, aunque las SA son independientes entre sí.</p> <p>Las IPSec SA son unidireccionales y únicas en cada protocolo de seguridad. La IKE SA sólo es utilizada por IKE y, a diferencia de la IPSec SA, que es bidireccional. IKE negocia y establece las SA en nombre de IPSec. Los usuarios también pueden establecer manualmente las IPSec SA.</p> <p>En los casos de canalizaciones de datos protegidas, es preciso disponer de un conjunto de SA, una por dirección por protocolo. Por ejemplo, si dispone de una canalización que admite ESP (Encapsulating Security Protocol) entre pares, es preciso una ESP SA por cada dirección. Las SA se identifican de forma única mediante la dirección de destino (punto final IPSec), el protocolo de seguridad (AH o ESP) y el SPI (Security Parameter Index).</p>
<b>SAID</b>	Security Association ID (ID de la asociación de seguridad). Identificador numérico de la SA de un enlace determinado.
<b>salt</b>	Cadena de caracteres pseudoaleatorios utilizada para reforzar la complejidad criptográfica.

<b>SDEE</b>	Security Device Event Exchange. Protocolo de mensajes que puede utilizarse para generar informes acerca de eventos de seguridad, como alarmas generadas cuando un paquete coincide con las características de una firma.
<b>SDF</b>	Signature Definition File (Archivo de definición de firmas). Archivo, generalmente en formato XML, que contiene definiciones de firmas que pueden utilizarse para cargar firmas en un dispositivo de seguridad.
<b>SDP</b>	Secure Device Provisioning. SDP utiliza TTI (Trusted Transitive Introduction) para implementar fácilmente la <b>PKI</b> (infraestructura de clave pública) entre dos dispositivos finales como un cliente de Cisco IOS y un servidor de certificados de Cisco IOS.
<b>SEAF</b>	Signature Event Action Filter (Filtro de acción de evento de firma). Filtro que permite quitar acciones de un evento cuyos parámetros se encuentran entre los definidos. Por ejemplo, se puede crear un SEAF para quitar la acción Restablecer conexión TCP de un evento asociado con una dirección de atacante particular.
<b>SEAO</b>	Signature Event Action Override (Anulación de acción de evento de firma). SEAO le permite asignar un intervalo de índice de riesgo ( <b>RR</b> ) a un tipo de acción de evento IPS como una alarma. Si se produce un evento con un RR en el intervalo que asignó al tipo de acción, esa acción se agrega al evento. En este caso, se agregaría una alarma al evento.
<b>SEAP</b>	Signature Event Action Processor (Procesador de acción de evento de firma). SEAP permite filtrar y anular según la información del índice de riesgo de evento ( <b>ERR</b> ).
<b>secreto compartido</b>	Clave criptográfica.
<b>sensor IDS</b>	Un sensor IDS es hardware en el que se ejecuta Cisco IDS. Los sensores IDS pueden ser dispositivos autónomos o módulos de red instalados en los routers.
<b>servidor de la CA</b>	Servidor de la autoridad certificadora. Host de red que se utiliza para emitir o revocar certificados digitales.

<b>servicio de no repudiación</b>	Servicio de seguridad de terceros que almacena pruebas para posibles recuperaciones posteriores, relativas al origen y destino de todos los datos incluidos en una comunicación, sin almacenar los datos reales. Estas pruebas pueden utilizarse para salvaguardar a todos los participantes de dicha comunicación contra denegaciones falsas de haber enviado o de haber recibido información, efectuadas por cualquier participante.
<b>SFR</b>	Signature Fidelity Rating (Índice de fidelidad de firma). Ponderación asociada con la forma en que esta firma podría ejecutarse en ausencia de conocimiento específico del destino.
<b>SHA</b>	Como alternativa a MD5, algunos sistemas de cifrado utilizan el algoritmo de hash seguro para generar firmas digitales.
<b>SHA-1</b>	Algoritmo de hash seguro 1. Algoritmo que toma un mensaje de menos de 264 bits de longitud y produce un message digest de 160 bits. Un message digest grande proporciona seguridad contra colisiones por fuerza bruta y ataques de inversión. SHA-1 [NIS94c] es una revisión de SHA publicada en 1994.
<b>SIP</b>	Session Initiation Protocol (Protocolo de inicio de sesión). Permite sesiones de gestión de llamadas, en particular conferencias de audio de dos partes o “llamadas”. SIP funciona con SDP (Session Description Protocol) para la señalización de llamadas. SDP especifica los puertos del flujo de los soportes. Si se utiliza SIP, el router podrá admitir cualquier gateway VoIP (Voice over IP) y servidores proxy VoIP.
<b>SMTP</b>	Simple Mail Transfer Protocol (Protocolo simple de transferencia de correo). Protocolo de Internet que proporciona servicios de correo electrónico.
<b>SNMP</b>	Simple Network Management Protocol (Protocolo simple de gestión de redes). Protocolo de gestión de redes utilizado de forma prácticamente exclusiva en redes TCP/IP. SNMP proporciona un medio de controlar y supervisar los dispositivos de red, así como de gestionar configuraciones, recopilaciones estadísticas, el rendimiento y la seguridad.
<b>SPD</b>	Selective Packed Discard (Descarte selectivo de paquetes). SPD da prioridad al enrutamiento de paquetes de protocolo, así como a otros importantes “keepalive” del nivel 2 de control de tráfico, durante los períodos de congestión de cola.
<b>spoke</b>	En una red <b>DMVPN</b> , un router spoke es un punto final lógico de la red y tiene una conexión <b>IPSec</b> punto a punto con un router <b>hub</b> DMVPN.

<b>spoofing</b>	Acto por el que un paquete indica que proviene de una dirección desde la que en realidad no fue enviado. El objetivo del “spoofing” es engañar a los mecanismos de seguridad de la red, como filtros y listas de acceso.
<b>spoof</b>	
<b>SRB</b>	Source-Route Bridging (Bridge de ruta de origen). Método de bridge creado por IBM y popular en las redes Token Ring. En una red SRB, la ruta completa a un destino se predetermina, en tiempo real, antes de enviar los datos al destino.
<b>SSH</b>	Secure Shell. Aplicación que se ejecuta sobre el nivel de transporte fiable como, por ejemplo, TCP/IP, y que proporciona potentes capacidades de cifrado y autenticación. Se admite un máximo de cinco clientes SSH para el acceso simultáneo a la consola del router.
<b>SSL</b>	Secure Socket Layer (Nivel de socket seguro). Tecnología de cifrado para la Web utilizada con el fin de proporcionar transacciones seguras como, por ejemplo, la transmisión del número de la tarjeta de crédito para el comercio electrónico.
<b>SSL VPN</b>	Secure Socket Layer Virtual Private Networks (Redes privadas virtuales con nivel de socket seguro). SSL VPN es una función que permite que un router admitido por Cisco proporcione acceso seguro para clientes remotos a los recursos de la red, mediante la creación de un túnel cifrado en Internet con la conexión de banda ancha o marcación ISP que utilice el cliente remoto.
<b>subred</b>	En las redes IP, una red que comparte una dirección de subred particular. Las subredes son redes segmentadas arbitrariamente por el administrador de red para proporcionar una estructura jerárquica de varios niveles y, al mismo tiempo, blindar la subred ante la complejidad de direcciones de las redes conectadas. Consulte también “dirección IP”, “bits de subred” y “máscara de subred”.
<b>subred local</b>	Las subredes son redes IP segmentadas arbitrariamente por un administrador de red (mediante una máscara de subred) para proporcionar una estructura jerárquica de varios niveles y, al mismo tiempo, blindar la subred ante la complejidad de direcciones de las redes conectadas. La subred local es la subred asociada al extremo de la propia transmisión.
<b>subred remota</b>	Las subredes son redes IP segmentadas arbitrariamente por un administrador de red (mediante una máscara de subred) para proporcionar una estructura jerárquica de varios niveles y, al mismo tiempo, blindar la subred ante la complejidad de direcciones de las redes conectadas. Una “subred remota” es la subred que <i>no</i> está asociada al extremo de la propia transmisión.



<b>suma de comprobación</b>	Método computacional que sirve para comprobar la integridad de los datos transmitidos, calculado a partir de una secuencia de octetos como resultado de una serie de operaciones matemáticas. El destinatario vuelve a calcular el valor y lo compara a fin de verificarlo.
<b>SUNRPC</b>	SUN RPC (SUN Remote Procedure Call). RPC es un protocolo que permite que los clientes ejecuten programas o rutinas en los servidores remotos. SUNRPC es la versión de RPC que se distribuyó originalmente en la biblioteca de SUN Open Network Computing (ONC).
<hr/>	
<b>T</b>	
<b>T1</b>	Un enlace T1 es un enlace de datos capaz de transmitir datos a una velocidad de 1,5 MB por segundo.
<b>TACACS+</b>	Terminal Access Controller Access Control System Plus. Protocolo de cuentas y autenticación para servidor de acceso que utiliza TCP como protocolo de transporte.
<b>TCP</b>	TCP (Transmission Control Protocol). Protocolo de nivel de transporte orientado hacia la conexión que proporciona una transmisión dúplex de datos fiable.
<b>TCP Syn Flood Attack (Ataque de saturación Syn TCP)</b>	Este tipo de ataque se produce cuando un hacker inunda un servidor con una barrera de solicitudes de conexión. Como dichos mensajes tienen una dirección de retorno que no se puede alcanzar, no es posible establecer conexión. El volumen obtenido de conexiones abiertas sin resolver acaba saturando el servidor y puede hacer que éste deniegue servicio a solicitudes válidas, por lo que se impide que los usuarios legítimos puedan entrar en un sitio Web, acceder al correo electrónico, utilizar el servicio FTP, etc.
<b>Telnet</b>	Protocolo de emulación de terminales para redes TCP/IP como Internet. Telnet es una forma común de controlar remotamente los servidores Web.
<b>texto cifrado</b>	Datos cifrados, ilegibles, antes del descifrado.
<b>texto no cifrado</b>	Texto no cifrado. Llamado también <i>texto sin formato</i> .
<b>texto sin formato</b>	Datos normales, sin cifrar.

<b>TFTP</b>	Trivial File Transfer Protocol (Protocolo trivial de transferencia de archivos). Se trata de un sencillo protocolo utilizado para transferir archivos. Se ejecuta en UDP y se explica en profundidad en la RFC (Request For Comments) 1350.
<b>traducción de direcciones</b>	Traducción de una dirección de red o puerto a otra dirección de red o puerto. Consulte también <a href="#">Dirección IP</a> , <a href="#">NAT</a> , <a href="#">PAT</a> , <a href="#">PAT estática</a> .
<b>transformación</b>	Descripción de un protocolo de seguridad y sus algoritmos correspondientes.
<b>túnel</b>	Canal virtual situado en un medio compartido como Internet, utilizado para intercambiar paquetes de datos encapsulados.
<b>TVR</b>	Target Value Rating (Índice de valor de destino). TVR es un valor definido por el usuario que representa el valor percibido por el usuario del host de destino. Éste permite que el usuario aumente el riesgo de un evento asociado con un sistema crítico y no enfatice el riesgo de un evento en un destino de valor bajo.

---

## U

<b>UDP</b>	User Datagram Protocol (Protocolo de datagrama de usuario). Protocolo de nivel de transporte sin conexiones en el protocolo TCP/IP que pertenece a la familia de protocolos de Internet.
<b>Unity Client</b>	Cliente de un servidor Unity Easy VPN.
<b>URI</b>	Identificador de recurso universal. Tipo de identificador con formato que encapsula el nombre de un objeto de Internet y lo etiqueta con una identificación del espacio de nombre para producir un miembro del conjunto universal de nombres en espacios de nombres registrados y de direcciones que se refieren a protocolos o espacios de nombre registrados. [RFC 1630]

<b>URL</b>	Universal Resource Locator (Localizador de recursos universal). Esquema de direcciones estandarizado que permite acceder a documentos de hipertexto y otros servicios mediante un explorador. A continuación se entregan dos ejemplos:  <code>http://www.cisco.com.</code>  <code>ftp://10.10.5.1/netupdates/sig.xml</code>
<b>URL de suscripción</b>	La URL de suscripción es la ruta HTTP a una autoridad certificadora (CA) que el router de Cisco IOS debe seguir para enviar solicitudes de certificado. Dicha URL incluye un nombre DNS o una dirección IP, y puede ir seguida de una ruta completa a las secuencias de comandos de la CA.
<hr/>	
<b>V</b>	
<b>VCI</b>	Virtual Channel Identifier (Identificador del canal virtual). Una ruta virtual puede contener varios canales virtuales correspondientes a conexiones individuales. El VCI identifica el canal que se está utilizando. La combinación de VPI y VCI identifica una conexión ATM.
<b>velocidad de ráfaga</b>	La cantidad de bytes que la ráfaga de tráfico no debe exceder.
<b>velocidad de supervisión</b>	La cantidad de bits por segundo que el tráfico no debe exceder.
<b>verificación</b>	Confirmación de la identidad de una persona o proceso.
<b>VFR</b>	Ensamblaje de fragmentos virtuales. VFR permite al firewall IOS crear listas de control de acceso (ACL) dinámicamente para bloquear fragmentos IP. A menudo, los fragmentos IP no contienen la información necesaria para que las ACL estáticas puedan filtrarlos.
<b>VPI</b>	Virtual Path Identifier (Identificador de la ruta virtual). Identifica la ruta virtual utilizada por una conexión ATM.

<b>VPDN</b>	Virtual Private Dial-up Network (Red de acceso telefónico privada virtual). Sistema que permite a las redes telefónicas existir remotamente en relación con las redes domésticas y dar la apariencia de estar conectadas directamente. Las VPDN utilizan L2TP y L2F para terminar el nivel 2 y las partes superiores de la conexión de red en el gateway doméstico, en vez de utilizar el NAS (servidor de acceso a la red).
<b>VPN</b>	Virtual Private Network (Red privada virtual). Proporciona la misma conectividad de red para usuarios en una infraestructura pública que la que se hubiera obtenido en una red privada. Las VPN permiten que el tráfico IP se transfiera con seguridad a través de las redes TCP/IP públicas mediante el cifrado del tráfico de una red a otra. Las VPN utilizan una arquitectura de túneles para cifrar toda la información en el nivel IP.
<b>VPN sitio a sitio</b>	Normalmente, una VPN sitio a sitio es una red que conecta dos redes o subredes y que cumple varios criterios específicos adicionales, incluido el uso de firmas IP estáticas en ambos lados del túnel, la ausencia de software cliente de VPN en las estaciones finales de los usuarios, así como la ausencia de un hub VPN central (a diferencia de lo que ocurre en las configuraciones VPN de hub y spoke). El objetivo de las VPN sitio a sitio no es sustituir el acceso mediante llamada por usuarios remotos o en desplazamiento.
<b>VTI</b>	Interfaz de plantilla virtual.
<b>vty</b>	Virtual Type Terminal (Terminal de tipo virtual). Generalmente utilizado como líneas de terminal virtuales.

---

## W

<b>WAN</b>	Wide Area Network (Red de área ancha). Red que proporciona servicio a usuarios de una amplia área geográfica y que, a menudo, utiliza dispositivos proporcionados por portadoras comunes. Consulte también “LAN”.
<b>WINS</b>	Windows Internet Naming Service (Servicio de nombres de Internet de Windows). Sistema de Windows que determina la dirección IP asociada a un equipo determinado de una red.

---

**X**

- X.509** Estándar de certificado digital que especifica la estructura del certificado. Los campos principales son el campo de ID, tema, fechas de validez, clave pública y firma CA.
- Xauth** Autenticación ampliada de IKE. Xauth permite a todos los métodos de autenticación AAA del software Cisco IOS ejecutar la autenticación de usuarios en una fase separada, después del intercambio de la fase 1 de autenticación de IKE. El nombre de la lista de configuración AAA debe coincidir con el nombre de la lista de configuración Xauth para que se produzca una autenticación de usuario.
- Xauth es una ampliación de IKE y no sustituye la autenticación IKE.

---

**Z**

- zona** En un firewall de política basado en zona, una zona es grupo de interfaces que tienen funciones o características similares. Por ejemplo, si las interfaces FastEthernet 0/0 y FastEthernet 0/1 están conectadas a la LAN, se pueden agrupar en una zona para la LAN.
- zona de seguridad** Grupo de interfaces en las que se puede aplicar una política. Las zonas de seguridad constan de interfaces que comparten funciones o características similares. Por ejemplo, en un router, las interfaces Ethernet 0/0 y Ethernet 0/1 se pueden conectar a la LAN local. Estas dos interfaces son similares porque representan la red interna, así que se pueden agrupar en una zona para las configuraciones de firewall.
- ZPF** Firewall de política basado en zonas. En una configuración ZPF, las interfaces se asignan a las zonas y se aplica una política de inspección al tráfico que se produce entre las zonas.





# ÍNDICE

---

## Symbols

\$ETH-LAN\$ [1](#)

\$ETH-WAN\$ [4](#)

---

## Numerics

3DES [9](#)

---

## A

acciones de rechazo [18](#)

Acerca de SDM

    Versión de SDM [2](#)

activar contraseña secreta [18, 34](#)

ADSL

    modo operativo [18, 29](#)

ADSL sobre ISDN (RDSI)

    modo operativo por defecto [18](#)

    modos operativos [32](#)

ansi-dmt [29](#)

anuncio, configurar [16, 34](#)

anuncio de texto, configurar [16, 34](#)

ARP proxy, desactivar [22](#)

asignación del programador [19](#)

asistente para la auditoría de seguridad

    activar contraseña secreta y anuncio [34](#)

    configurar cuentas de usuario para  
    Telnet/SSH [33](#)

    inicio [1](#)

    registro [35](#)

    Selección de Interfaz [5](#)

    Tarjeta de informes [6](#)

autenticación

    AH [12](#)

    ESP [12](#)

    firmas digitales [23](#)

    MD5 [9](#)

    SHA\_1 [9](#)

autenticación AH [12](#)

AutoSecure [28](#)

---

## B

Bloqueo de un paso [3](#)

BOOTP, desactivar [10](#)

## C

Calidad de servicio (QoS)

    visualización de actividad **25**

CBAC, activar **26**

CDP, desactivar **11**

CEF, activar **14**

CHAP **10**

cifrado

    3DES **9**

    AES **9**

    DES **9**

cifrado AES **9**

cifrado y autenticación ESP **12**

clave compartida **23**

clave previamente compartida **7, 18, 3**

claves previamente compartidas **6**

comandos show **2**

COMP-LZS **12**

compresión IP **12**

concentrador VPN

    permitir el tráfico a través de un firewall  
    hacia **20**

Conexiones WAN

    creación en asistente **1**

    eliminación **22**

conexión Xauth **7**

Confidencialidad directa perfecta **6**

configuración del reloj **20, 45, 48**

configuración de reflejo, VPN **35**

conjunto de transformación **11, 7**

conjuntos de direcciones **9, 17**

conjuntos de transformación, varios **39**

contraseñas

    cifrado, activar **12**

    establecer la longitud mínima **15**

cuentas de usuario, Telnet **20**

cuentas de usuario para Telnet, configurar **33**

## D

definiciones de acrónimos y términos

clave **GLS1**

definiciones del glosario **GLS1**

DES **9**

DHCP **5, 25**

difusiones dirigidas por IP, desactivar **22**

Dirección IP

    dinámica **25**

    dinámico **5**

    negociado **5, 25**

    no numerado **5, 25**

    para ATM con enrutamiento RFC1483 **6**

    para ATM o Ethernet con PPPoE **5**

    para Ethernet sin PPPoE **7**

    para serie con HDLC o Frame Relay **8**

    para serie con PPP **7**

dirección IP

    próximo salto (next hop) **15**

dirección IP de próximo salto (next hop) **15**



dirección IP dinámica [5, 25](#)  
 distancia métrica [5](#)  
 división de la arquitectura en túneles [22](#)  
 DLCI [19, 44](#)  
 DMVPN [1](#)  
     clave previamente compartida [3](#)  
     hub [2](#)  
     hub principal [3](#)  
     información de enrutamiento [8](#)  
     red centro-radial (hub and spoke) [10](#)  
     red de malla completa [11](#)  
     spoke [2](#)

## E

Easy VPN [1](#)  
     Certificados digitales [3, 24](#)  
     clave de grupo [15](#)  
     clave de grupo IPSec [3](#)  
     Clave previamente compartida [3, 24](#)  
     conexión Xauth [7](#)  
     configuración de una conexión de respaldo [28](#)  
     control de túnel automático [6, 27](#)  
     control de túnel basado en tráfico [6, 27](#)  
     control de túnel manual [6, 27](#)  
     editar una conexión existente [28](#)  
     ID de conexión SSH [7](#)  
     interfaces [5](#)  
     modo de cliente [2](#)

modo de extensión de red [3](#)  
 Network Extension Plus [3, 23](#)  
 nombre de grupo IPSec [3](#)  
 nombre del grupo [15, 19, 24](#)  
 número de interfaces admitido [5, 26](#)  
 Unity Client [13, 16, 22](#)  
 encapsulación  
     Enrutamiento RFC1483 [16, 31, 34, 40](#)  
     Frame Relay [17](#)  
     HDLC [17](#)  
     IETF [19, 44](#)  
     PPP [17](#)  
     PPPoE [16, 31, 34, 40](#)  
 encapsulación genérica de enrutamiento multipunto [4](#)  
 Encapsulación IETF [19, 44](#)  
 enrutamiento  
     distancia métrica [5](#)  
     interfaz pasiva [6, 7, 8](#)  
     ruta EIGRP [7](#)  
     ruta OSPF [6](#)  
     ruta permanente [5](#)  
     ruta RIP [5](#)  
 enrutamiento de origen IP, desactivar [11](#)  
 Enrutamiento RFC1483 [16](#)  
     AAL5MUX [28, 31, 34, 40](#)  
     AAL5SNAP [28, 31, 34, 40](#)  
 entrada de regla  
     directrices [9](#)  
 enviar configuración al router [1](#)  
 equilibrio de carga [18, 25](#)

**F**

- firewall **1**
  - ACL **1**
  - activación de CBAC **26**
  - agregar entrada de aplicación **13**
  - agregar entrada de aplicación http **16**
  - agregar entrada de fragmento **15**
  - agregar entrada RPC **14**
  - Alerta de SDM **18**
  - configuración de la transmisión NAT **19**
  - configuración en una interfaz no compatible **16**
  - controles de visualización del flujo de tráfico **3**
  - escenarios **32**
  - flujo de tráfico, consulte flujo de tráfico
  - permitir el tráfico hacia un concentrador VPN **20**
  - permitir el tráfico procedente de hosts o redes específicos **18**
  - permitir un determinado tráfico **17, 18**
  - política **1**
  - visualización de actividad **14, 10**
- firmas, consulte IPS
- firmas digitales DSS **23**
- flujo de tráfico **3, 5**
  - iconos **5**
- Frame Relay **17**
  - configuración del reloj **45**
  - DLCI **44**

- Encapsulación IETF **44**
- tipo de LMI **44**

**G**

- G.SHDSL
  - modo operativo **36**
  - modo operativo, valor por defecto **18**
  - tasa de línea, por defecto **18**
  - tipo de equipamiento **36**
  - tipo de equipo, valor por defecto **18**
- GRE sobre IPsec, túnel **16**
- grupo D-H **10**
- grupo Diffie-Hellman **10**

**H**

- HDLC **17**
- hub principal **3**

**I**

- IKE **23**
  - algoritmos de autenticación **9**
  - autenticación **23**
  - clave compartida **23**
  - claves previamente compartidas **6**
  - descripción **1**
  - estado **18**

- grupo D-H [10](#)
- política [5](#)
- políticas [8, 2](#)
- visualización de actividad [13](#)
- información del router
  - acerca de este router [2](#)
- Intercambio de claves por Internet [23](#)
- interfaces
  - configuraciones disponibles para cada tipo [4](#)
  - editar asociaciones [10](#)
  - estadísticas [6](#)
  - no admitida [2](#)
  - visualización de actividad [6](#)
- interfaz de marcación, agregada con PPPoE [4](#)
- interfaz de serie
  - configuración del reloj [20](#)
- interfaz no admitida [2](#)
  - configuración como WAN [29](#)
  - configuración de NAT en [32, 19](#)
  - configuración de una VPN en [40](#)
  - configurar un firewall en [16](#)
- interfaz pasiva [6, 7, 8](#)
- interfaz WAN
  - no admitida [29](#)
- intervalo del programador [19](#)
- IPS
  - acerca de [1](#)
  - Asistente de reglas [2](#)
  - botones para configuración y administración [10](#)
  - configuración global [15](#)
  - Crear IPS [2](#)
  - desactivar (en la interfaz seleccionada) [12](#)
  - desactivar (en todas las interfaces) [12](#)
  - direcciones de tráfico [12](#)
  - filtro (ACL)
    - detalles [13](#)
    - entrante [14](#)
    - saliente [14](#)
    - seleccionar [14](#)
  - firmas
    - acciones en coincidencia [54](#)
    - acerca de [39, 45](#)
    - activar [41](#)
    - agregar [41](#)
    - árbol de firmas [39, 45, 56](#)
    - definir [58](#)
    - desactivar [41, 47](#)
    - importar [55](#)
    - información nueva [59](#)
    - OPACL de TrendMicro [41](#)
    - visualización [42, 48](#)
  - firmas incorporadas [18](#)
  - Panel de seguridad [61](#)
    - amenazas más frecuentes [61](#)
    - implementar firmas [63](#)
  - reglas [2](#)

SDF **62**

cargar **53**

en memoria del router **60**

proporcionado por IPS **59**

selección de interfaz **14**

servidor syslog **17, 24**

Ubicaciones SDF **17, 19**

VFR **13, 15**

volver a cargar (recompilar) firmas **17**

IPSec **14**

clave de grupo **3, 15**

descripción **1**

estadísticas **13**

estado del túnel **13**

nombre del grupo **15, 19, 24**

regla **11**

tipo de política **2**

visualización de actividad **13**

**L**

límites de tiempo para la traducción **9**

líneas vty

configuración de una clase de acceso **27**

LMI **19, 44**

longevidad de la asociación de seguridad **6**

**M**

mapa criptográfico **29**

conjunto de transformación **7**

dinámica **2**

longevidad de la asociación de seguridad **6**

número de secuencia **6**

pares en **7**

regla IPSec **11**

tráfico protegido **10**

mapa de ruta **28**

mapas de ruta **32, 15**

marcadores de hora, activar **13**

MD5 **9**

mensaje "keep-alive" de TCP, activar **12, 13**

mensajes de host inalcanzable ICMP,  
desactivar **23, 24**

mensajes de redireccionamiento ICMP,  
desactivar **21**

mensajes de respuesta de máscara ICMP,  
desactivar **24**

menú Archivo **1**

menú Ayuda **1**

menú Editar **1**

Menú Herramientas **1**

Menú Ver **1**

mGRE **4**

modo de cliente **2**

modo operativo ADSL

adls2 **30**

adsl2+ **30**

- ansi-dmt [29](#)
  - itu-dmt [30](#)
  - splitterless [30](#)
  - modo Supervisión [1](#)
    - aspectos generales [2](#)
    - Estado de la interfaz [6](#)
    - estado de la red VPN [13](#)
    - estado del firewall [10](#)
    - Estado del tráfico [25](#)
    - registro [32](#)
- 
- ## N
- NAT [1](#)
    - Asistente [1](#)
    - configuración con una VPN [40](#)
    - configuración en una interfaz no admitida [32, 19](#)
    - conjuntos de direcciones [9, 17](#)
    - dirección de la traducción, regla estática [19](#)
    - interfases designadas [9](#)
    - límite de tiempo de DNS [13](#)
    - límite de tiempo de ICMP [14](#)
    - límite de tiempo de la NAT dinámica [14](#)
    - límite de tiempo de PPTP [14](#)
    - límites de tiempo del flujo de TCP [14](#)
    - límites de tiempo del flujo de UDP [14](#)
    - límites de tiempo para la traducción [9, 13](#)
    - mapa de ruta [28](#)
    - mapas de ruta [15](#)
    - número máximo de entradas [14](#)
    - permitir a través de un firewall [19](#)
    - puerto de redireccionamiento [22, 25](#)
    - regla de traducción de direcciones dinámicas, de interna a externa [25](#)
    - regla de traducción de direcciones estáticas [19](#)
    - regla de traducción de direcciones estáticas, externa a interna [22](#)
    - reglas de traducción [9](#)
    - repercusión en la configuración del servicio DMZ [7](#)
    - traducir a la interfaz, regla dinámica [27, 29](#)
    - traducir a la interfaz, regla estática [20, 24](#)
    - traducir desde la interfaz, regla dinámica [26, 29](#)
    - traducir desde la interfaz, regla estática [19, 23](#)
    - y conexiones VPN [32](#)
  - NBAR
    - visualización de actividad [25](#)
  - Netflow
    - visualización de actividad [25](#)
  - NetFlow, activar [21](#)
  - NHRP
    - cadena de autenticación [5](#)
    - ID de red [6](#)
    - tiempo de espera [6](#)
  - números de secuencia, activar [13](#)

## P

- Panel de seguridad **61**
  - amenazas más frecuentes **61**
  - implementar firmas **63**
- Pantalla de Tarjeta de informes **6**
- PAP **10**
- PAT
  - configuración en el asistente para WAN **14**
  - uso en conjuntos de direcciones NAT **18**
- pequeños servidores TCP, desactivar **8**
- pequeños servidores UDP, desactivar **9**
- ping
  - envío a un par VPN **31**
- PPP **17**
- PPPoE **16, 31, 34, 40**
  - en el asistente para WAN Ethernet **4**
- preferencias, SDM **1**
- Protocolo de autenticación de contraseña, véase PAP
- Protocolo de autenticación por desafío mutuo, véase CHAP
- protocolo de enrutamiento, dinámico **32**
- protocolo de enrutamiento dinámico
  - configurar **32**
- Protocolo punto a punto sobre la encapsulación de Ethernet, véase PPPoE
- puerto de redireccionamiento **22, 25**
- PVC **17**

## R

- red centro-radial (hub and spoke) **10**
- red de malla completa **11**
- Red DMZ **6**
  - permitir un determinado tráfico a través **17**
  - servicios **6**
- red privada virtual multipunto dinámica (DMVPN) **1**
- registro
  - activación de números de secuencia y marcadores de hora **13**
  - activar **17**
  - configurar **35**
  - visualización de eventos **32**
- regla **14**
- regla de acceso
  - en una regla de traducción NAT **27, 29**
  - realizar cambios en la política de firewall **7**
- regla de inspección
  - Alerta de SDM **18**
- Regla de inspección CBAC **1**
- regla de traducción de direcciones estáticas **19**
- regla de traducción estática
  - puerto de redireccionamiento **22, 25**
- reglas
  - NAT, y conexiones VPN **32**
  - reglas ampliadas **6**
  - reglas estándar **5**

reglas ampliadas **6**  
     rangos de numeración **8**  
 reglas de acceso, ventana **4**  
 reglas definidas externamente, ventana **4**  
 Reglas de inspección CBAC **11**  
 reglas de SDM por defecto, ventana **4**  
 reglas de traducción **9**  
 reglas estándar **5**  
     rango de numeración **8**  
 reglas IPsec, ventana **4**  
 reglas NAC, ventana **4**  
 reglas NAT, ventana **4**  
 reglas no admitidas, ventana **4**  
 reglas por defecto, SDM **3**  
 RPF de unidifusión, activar **25**  
 RSA  
     cifrado **23**  
     firma digital **23**  
 ruta EIGRP **7**  
 ruta estática  
     configuración en el asistente para WAN **14**  
     configurar **11**  
     valor por defecto **4**  
 ruta estática por defecto **4**  
 ruta OSPF **6**  
 ruta permanente **5**  
 ruta RIP **5**

## S

SDEE  
     mensajes **20**  
         Error IDS **22**  
         estado IDS **21**  
     suscripciones **18, 25**  
 SDF **62**  
     cargar **53**  
     en memoria del router **60**  
     proporcionado por IPS **59**  
     ubicaciones **17, 19**  
 SDP  
     inicio **1**  
     resolución de problemas **3**  
 Secure Device Provisioning, consulte SDP **1**  
 servicio DMZ **7**  
     intervalo de direcciones **7**  
 servicio Finger, desactivar **7**  
 servicio HTTP  
     configuración de una clase de acceso **26**  
 servicio identificación IP, desactivar **10**  
 servicio MOP, desactivar **23**  
 servicio PAD, desactivar **8**  
 SHA\_1 **9**  
 Sistema de prevención de intrusiones (IPS)  
 Sistema de prevención de intrusiones (IPS) de Cisco IOS, consulte IPS  
 SNMP, desactivar **18**  
 solicitudes Gratuitous ARP, desactivar **14**

squeeze flash, no se puede realizar

comando erase flash [7](#)

SSH [7](#)

activar [27](#)

subprogramas Java, bloqueo [17](#)

syslog

configurar [35](#)

en IPS [17,24](#)

visualización [32](#)

## T

Telnet, cuentas de usuario [20](#)

terminología, definiciones [GLS1](#)

tiempo TCP Synwait [16](#)

Traducción de direcciones de puerto, véase PAT

Tráfico

visualización de actividad [25](#)

Tráfico de aplicaciones

visualización de actividad [25](#)

Tráfico de protocolos

visualización de actividad [25](#)

túnel GRE [16](#)

clave previamente compartida [18](#)

división de la arquitectura en túneles [22](#)

## V

VCI [17](#)

Ventana Reglas de acceso [4](#)

Ventana Reglas de QoS [4](#)

vista previa de los comandos, opción [1](#)

VPI [17](#)

VPN [1,25](#)

autenticación AH [12](#)

autenticación ESP [12](#)

clave previamente compartida [7](#)

Compresión IP [12](#)

configuración de la transmisión NAT [40](#)

configuración de pares de reserva [38](#)

configuración de reflejo [35](#)

configuración en el router del par [35](#)

configuración en una interfaz no compatible [40](#)

conjunto de transformación [11,7](#)

edición de un túnel existente [37](#)

eliminar túneles [30](#)

modo de transporte [12](#)

modo de túnel [12](#)

pares [7](#)

par IPSec remoto [6](#)

política de reflejo [31](#)

regla IPSec [14,11](#)

tráfico protegido [7,13,10](#)

varios dispositivos [39](#)

varios sitios o túneles [33](#)

visualización de actividad [37,13](#)