Administrador de dispositivos de seguridad: Tráfico P2P del bloque en un router del Cisco IOS que usa el ejemplo de la configuración de NBAR

Contenido

Introducción

Este documento describe cómo configurar al router del ® del Cisco IOS para bloquear el tráfico entre iguales (P2P) de la red interna a Internet usando el Reconocimiento de aplicaciones basadas en la red (NBAR).

El NBAR reconoce los Network Protocol y las aplicaciones de red específicos que se utilizan en su red. Una vez que un protocolo o una aplicación es reconocido por el NBAR, usted puede utilizar la interfaz de línea de comando de calidad de servicio modular (MQC) para agrupar los paquetes asociados a esos protocolos o aplicaciones en las clases. Estas clases se agrupan en base a si los paquetes se ajustan a ciertos criterios.

Para el NBAR, el criterio es si el paquete hace juego un protocolo o una aplicación específico sabida al NBAR. Usando el MQC, el tráfico de la red con un Network Protocol (Citrix, por ejemplo) se puede poner en una clase de tráfico, mientras que el tráfico que hace juego un diverso

Network Protocol (gnutella, por ejemplo) se puede poner en otra clase de tráfico. Más adelante, el tráfico de la red dentro de cada clase se puede dar el tratamiento apropiado usando una política de tráfico (correspondencia de políticas). Refiera el tráfico de la red que clasifica usando la sección NBAR de la *guía de configuración de las soluciones de la Calidad de servicio de Cisco IOS* para más información sobre el NBAR.

prerrequisitos

Requisitos

Antes de que usted configure el NBAR para bloquear el tráfico P2P, usted debe habilitar el Cisco Express Forwarding (CEF).

Utilice el **cef del IP** en el modo de configuración global para habilitar el CEF:

```
Hostname(config)#ip cef
```

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 2801 Router con la versión 12.4(15)T del Cisco IOS ® Software
- Versión 2.5 del (SDM) del administrador de dispositivo Security de Cisco

Nota: Refiera a la configuración básica del router usando el SDM para permitir que al router configure el SDM.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Descripción del Reconocimiento de aplicaciones basadas en la red (NBAR)

El Network-Based Application Recognition (NBAR) es un motor de clasificación que reconoce y clasifica una amplia variedad de protocolos y de aplicaciones. Cuando el NBAR reconoce y clasifica un protocolo o una aplicación, la red se puede configurar para aplicar el Calidad de Servicio (QoS) apropiado para esa aplicación o tráfico con ese protocolo.

El NBAR realiza estas funciones:

- **Identificación de las aplicaciones y de los protocolos (capa 4 para acodar 7)**El NBAR puede clasificar las aplicaciones que utilizan:(TCP) del protocolo transfer control y números del

puerto estáticamente asignados del User Datagram Protocol (UDP).Protocolos IP NON-UDP y del no TCP.Números del puerto dinámicamente asignados TCP y UDP negociados durante el establecimiento de la conexión. La inspección con estado se requiere para la clasificación de las aplicaciones y de los protocolos. La inspección con estado es la capacidad de descubrir las conexiones de datos que serán clasificadas pasando los controles de conexión sobre el puerto de la conexión de datos en donde se hacen las asignaciones.Clasificación de subpuertos: Clasificación del HTTP (los URL, imitan o los nombres del host) y del tráfico computacional de la arquitectura de la independiente de las aplicaciones del Citrix (ICA) basado en el nombre de la aplicación publicado.Clasificación basada en la inspección de paquetes profunda y los atributos específicos a la aplicación múltiples. La clasificación del payload del Real-Time Transport Protocol (RTP) se basa en este algoritmo en el cual el paquete se clasifique como RTP basado en los atributos múltiples en el encabezado RTP.

- **Descubrimiento del protocolo**El descubrimiento del protocolo es una característica de uso general NBAR que recoge la aplicación y las estadísticas de protocolo (cuentas de paquetes, cuentas de bytes, y velocidades de bits) por la interfaz. Las herramientas de administración basadas GUI pueden visualizar gráficamente esta información, sondeando las estadísticas SNMP del Management Information Base paladio NBAR (MIB). Como con cualquier característica del establecimiento de una red, es importante entender el funcionamiento y las características del scalability antes de desplegar la característica en una red de producción. En las plataformas basadas en software, las métricas se consideran que son impacto de la utilización de la CPU y la velocidad de datos sostenible mientras que se habilita esta característica. Para configurar el NBAR para descubrir el tráfico para todos los protocolos que se sepan al NBAR en una interfaz particular, utilice el comando ip nbar protocol-discovery en el modo de configuración de la interfaz o el modo de configuración de VLAN. Para inhabilitar la detección del tráfico, no utilice el **ningún comando ip nbar protocol-discovery**.

Configure el bloqueo entre iguales del tráfico (P2P)

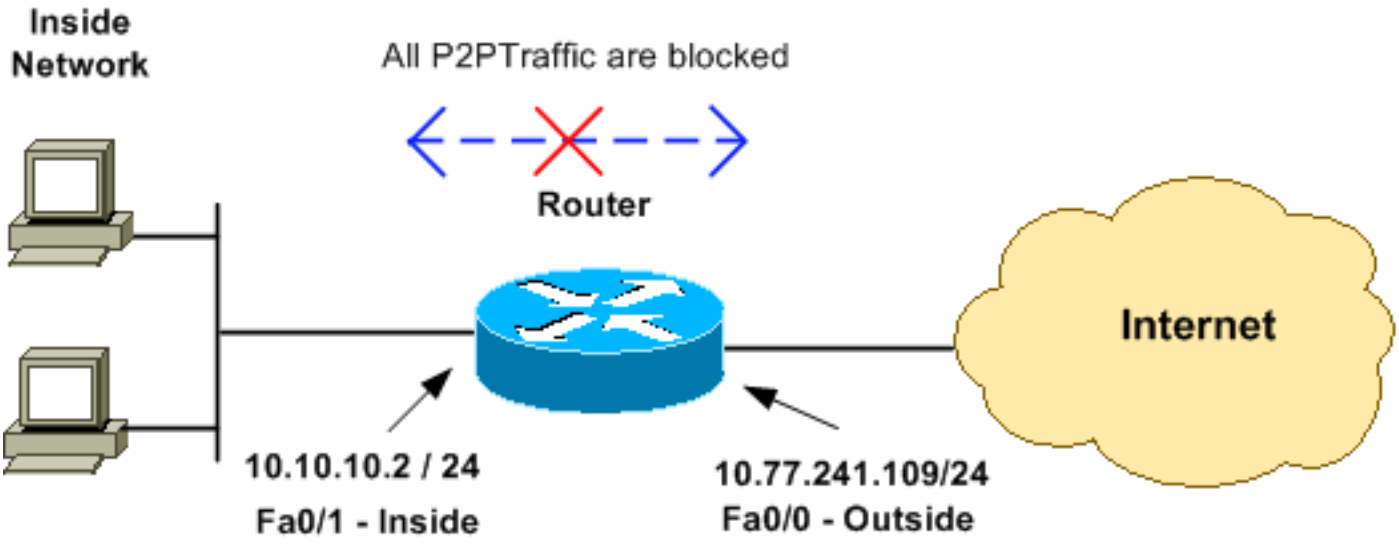
En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Un cierto tráfico P2P no puede ser totalmente bloqueado debido a la naturaleza de su protocolo P2P. Estos protocolos P2P cambian dinámicamente sus firmas para desviar cualquier motor DPI que intente bloquear totalmente su tráfico. Por lo tanto, Cisco recomienda que usted limita el ancho de banda en vez totalmente de bloquearlos. (Estrangule el ancho de banda para este tráfico. Dé muy menos ancho de banda; sin embargo, deje la conexión ir a través.)

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuración del router

Configuración para bloquear el tráfico P2P en el router del Cisco IOS

```
R1#show run
Building configuration...

Current configuration : 4543 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
logging buffered 4096
enable secret 5 $1$bKq9$AHOxTgk6d3hcMGn6jTGxs/
!
aaa new-model
!
!
!
!
aaa session-id common
!--- IP CEF should be enabled at first to block P2P
traffic. !--- P2P traffic cannot be blocked when IPC CEF
is disabled. ip cef
!
!--- Configure the user name and password with Privilege
level 15 !--- to get full access when using SDM for
configuring the router. username cisco123 privilege 15
password 7 121A0C0411045D5679
secure boot-image
secure boot-config
archive
 log config
  hidekeys
!
!
!
!--- Configure the class map named p2p to match the P2P
protocols !--- to be blocked with this class map p2p.
```

```
class-map match-any p2p

!--- Mention the P2P protocols to be blocked in order to
block the !--- P2P traffic flow between the required
networks. edonkey, !--- fasttrack, gnutella, kazaa2,
skype are some of the P2P !--- protocols used for P2P
traffic flow. This example !--- blocks these protocols.
match protocol edonkey
 match protocol fasttrack
 match protocol gnutella
 match protocol kazaa2
 match protocol winmx
 match protocol skype

!--- The access list created is now mapped with the
class map P2P !--- to specify the interesting traffic.
match access-group 102
!
!
!--- Here the policy map named SDM-QoS-Policy-2 is
created, and the !--- configured class map p2p is
attached to this policy map. !--- Drop is the command to
block the P2P traffic.

policy-map SDM-QoS-Policy-2
 class p2p
   drop
!
!
!
!--- Below is the basic interface configuration on the
router. interface FastEthernet0/0 ip address
10.77.241.109 255.255.255.192 duplex auto speed auto !
interface FastEthernet0/1 ip address 10.10.10.2
255.255.255.0 !--- The command ip nbar protocol-
discovery enables NBAR !--- protocol discovery on this
interface where the QoS !--- policy configured is being
used.

 ip nbar protocol-discovery
 duplex auto
 speed auto
!--- Use the service-policy command to attach a policy
map to !--- an input interface so that the interface
uses this policy map.

 service-policy input SDM-QoS-Policy-2
!
ip route 10.77.241.0 255.255.255.0 10.10.10.2
ip route 10.77.0.0 255.255.0.0 10.77.241.65
!
!--- Configure the below commands to enable SDM !---
access to the Cisco routers. ip http server
ip http authentication local
no ip http secure-server
!
!--- Configure the access lists and map them to the
configured class map. !--- Here the access list 102 is
mapped to the class map p2p. The access !--- lists are
created for both Incoming and outgoing traffic through
!--- the inside network interface.

access-list 102 remark SDM_ACL Category=256
access-list 102 remark Outgoing Traffic
```

```
access-list 102 permit ip 10.10.10.0 0.0.0.255
10.77.241.0 0.0.0.255
access-list 102 remark Incoming Traffic
access-list 102 permit ip 10.77.241.0 0.0.0.255
10.10.10.0 0.0.0.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
 password 7 02250C520807082E01165E41
line vty 0 4
 exec-timeout 0 0
 password 7 05080F1C22431F5B4A
 transport input all
!
!
webvpn cef
end
```

Configure al router con el SDM

Configuración de SDM del router

Complete estos pasos para configurar el bloqueo del tráfico P2P en un router del Cisco IOS:

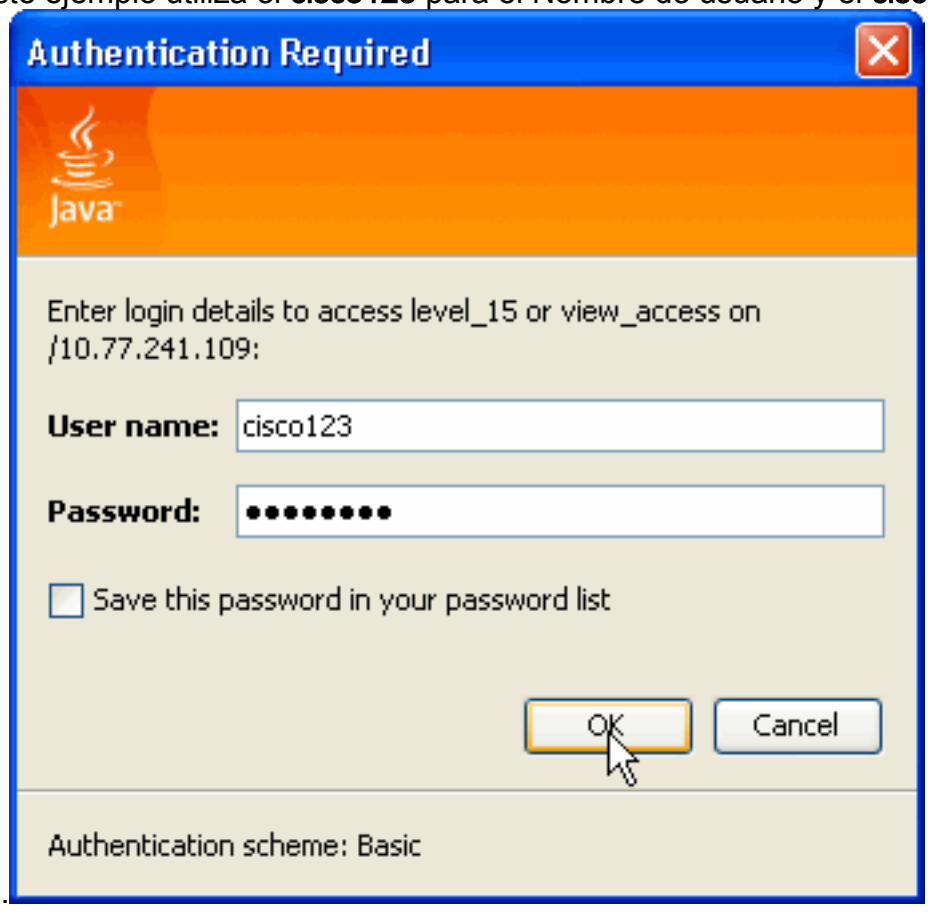
Nota: Para configurar el NBAR para descubrir el tráfico para todos los protocolos que se sepan al NBAR en una interfaz particular, el comando ip nbar protocol-discovery debe ser utilizado en el modo de configuración de la interfaz o el modo de configuración de VLAN para habilitar la detección del tráfico. Proceda con la configuración de SDM después de configurar el descubrimiento del protocolo en la interfaz necesaria donde política de calidad de servicio (QoS) configurado se está utilizando.

```
Hostname#config t
               Hostname(config)#interface fastEthernet 0/1
               Hostname(config-if)#ip nbar protocol-discovery
               Hostname(config-if)#end
```

1. Abra un hojeador, y ingrese el IP Address del router que se ha configurado para el acceso del SDM. Por ejemplo, **<SDM_Router_IP_Address de https:// >**Aseegurese autorizar cualquier advertencia que su navegador le dé relacionado con la autenticidad de certificados SSL. Nombre de usuario predeterminado y la contraseña son ambos espacio en blanco.El router visualiza esta ventana para permitir la descarga de la aplicación del SDM. Este ejemplo carga la aplicación sobre la computadora local y no se ejecuta en los subprogramas

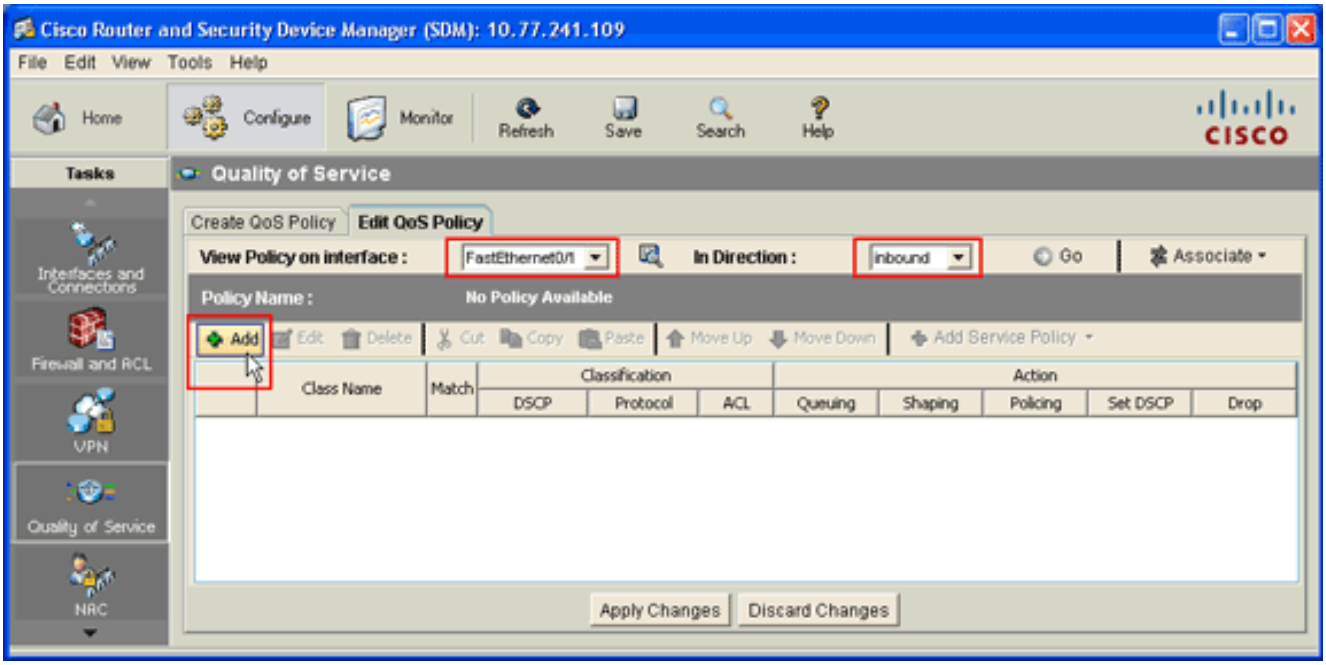
java.La descarga del SDM ahora comienza.

2. Una vez que las descargas del lanzador del SDM, completan los pasos ordenados por los prompts para instalar el software y funcionar con el lanzador del SDM de Cisco.
3. Ingrese un Nombre de usuario y una contraseña, si usted especificó uno, y haga clic la **AUTORIZACIÓN**.Este ejemplo utiliza el **cisco123** para el Nombre de usuario y el **cisco123** como la contraseña.

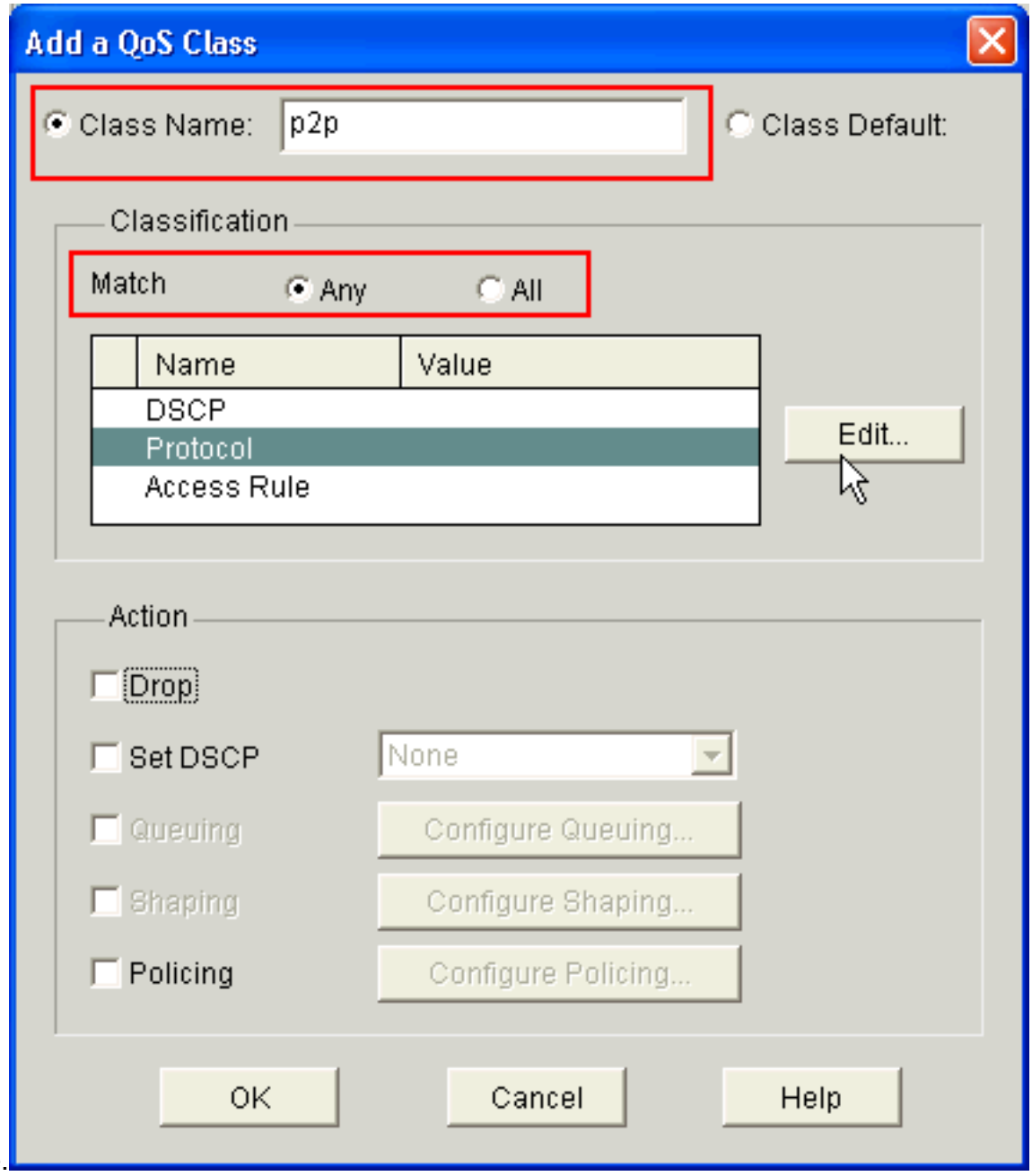


4. Elija la **configuración > la calidad de servicio**, y haga clic la lengueta del **editar política de**

calidad de servicio (QoS) en el Home Page del SDM.

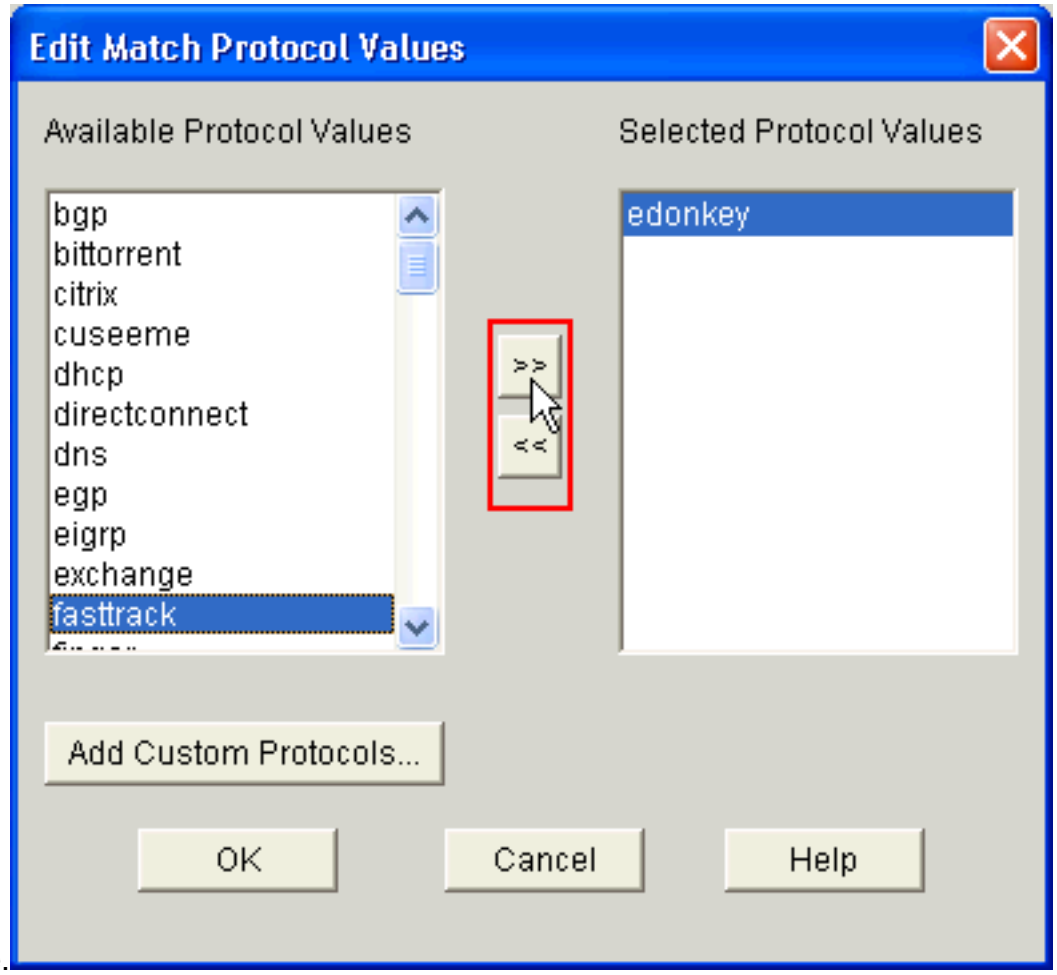


5. De la directiva de la visión en la lista desplegable de la interfaz, elija el nombre de la interfaz, y después elija el flujo de la dirección del tráfico (entrante o saliente) del en la lista desplegable de la dirección.En este ejemplo, la interfaz es *FastEthernet0/1*, y la dirección es *entrante*.
6. El tecleo **agrega** para agregar una nueva clase de QoS para la interfaz.El agregar un cuadro de diálogo de la clase de QoS



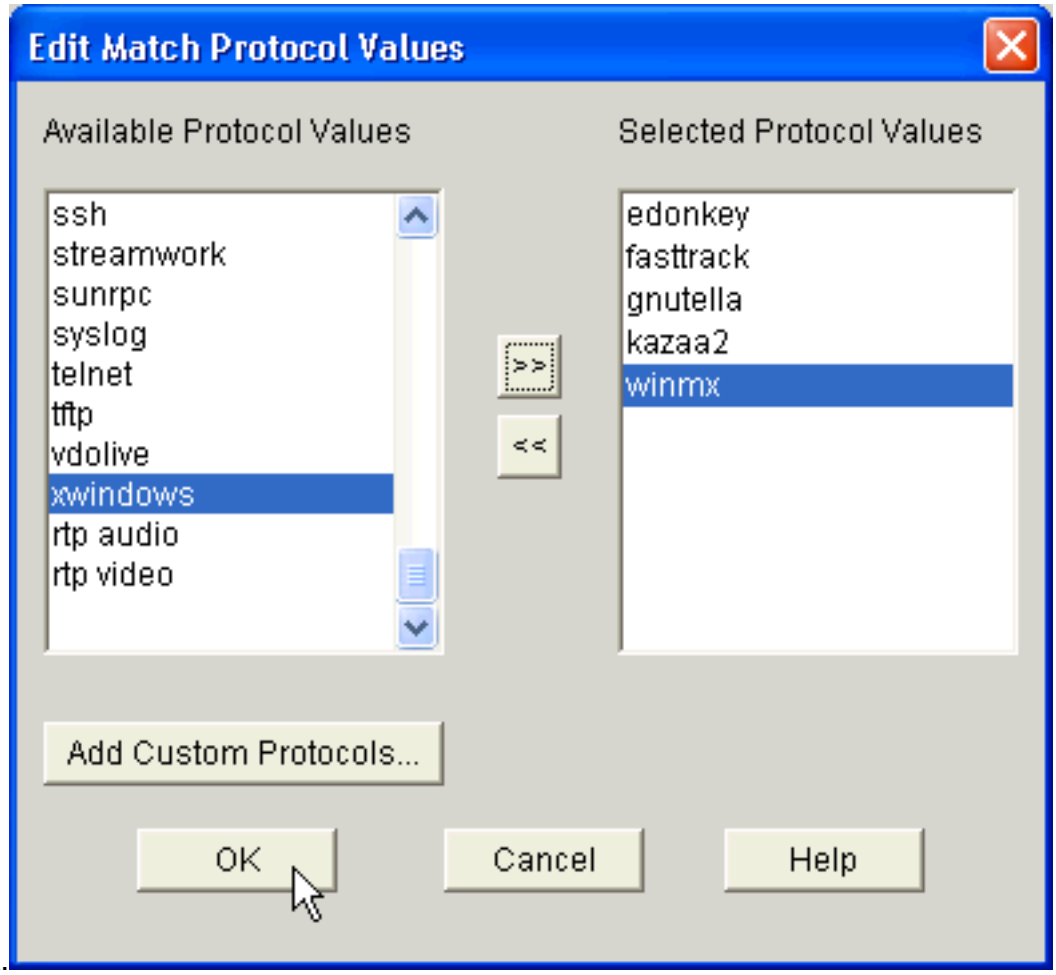
aparece.

7. Si usted quiere crear una nueva clase, haga clic el botón de radio del **nombre de la clase**, y ingrese un nombre para su clase. Si no, haga clic el botón de radio del **valor por defecto de la clase** si usted quiere utilizar la clase predeterminada.Este ejemplo crea una nueva clase nombrada *p2p*.
8. En el área de la clasificación, haga clic el **cualquier** botón de radio o **todo el** botón de radio para la opción de la coincidencia.Este los ejemplos utilizan la *cualquier* opción de la coincidencia, que funcione con el comando p2p del match-any del clase-mapa en el router.
9. Seleccione el **protocolo** en la lista de Classifcation, y el tecleo **edita** para editar el parámetro del protocolo.El cuadro de diálogo de los valores del protocolo de la coincidencia del editar

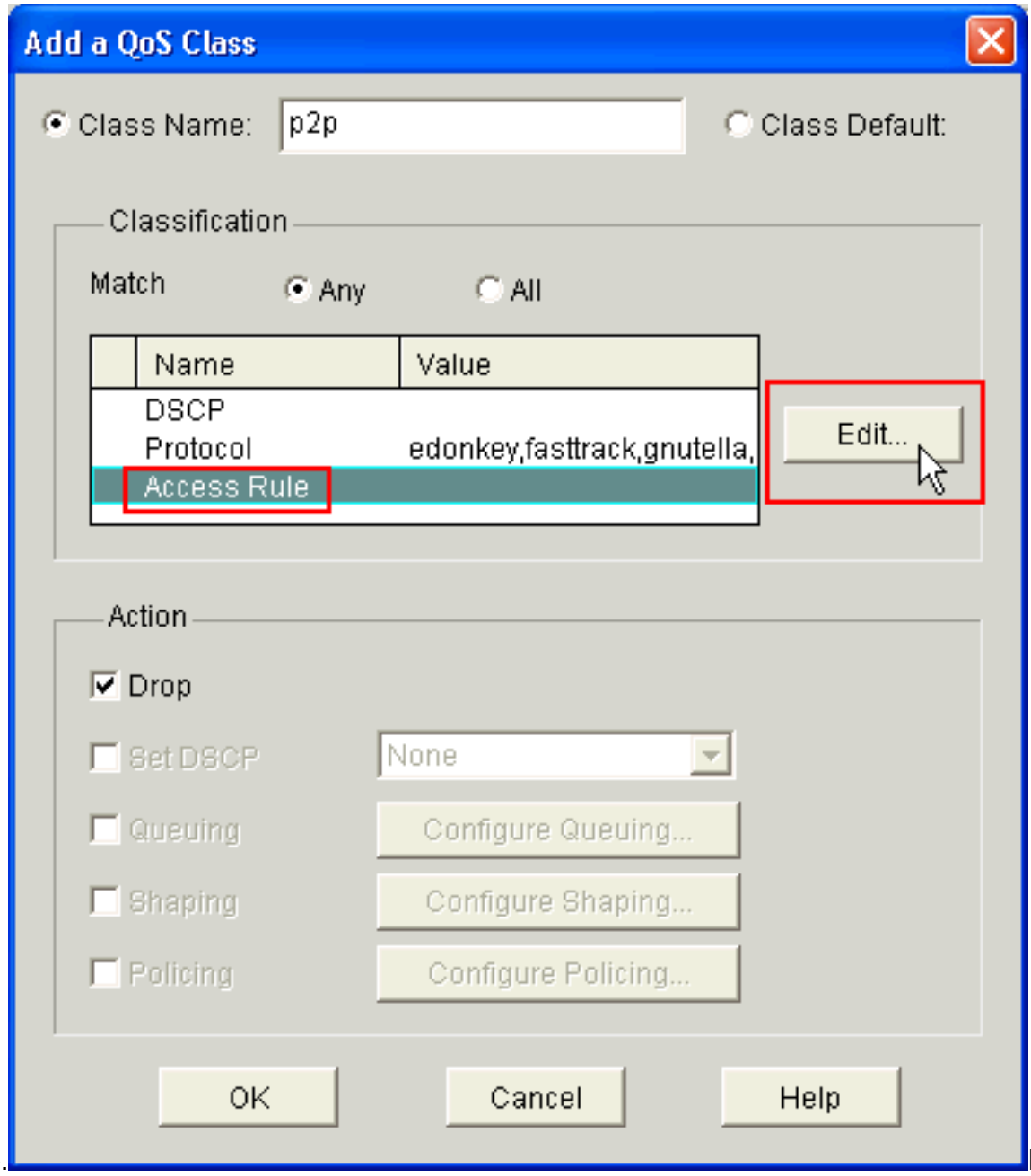


aparece.

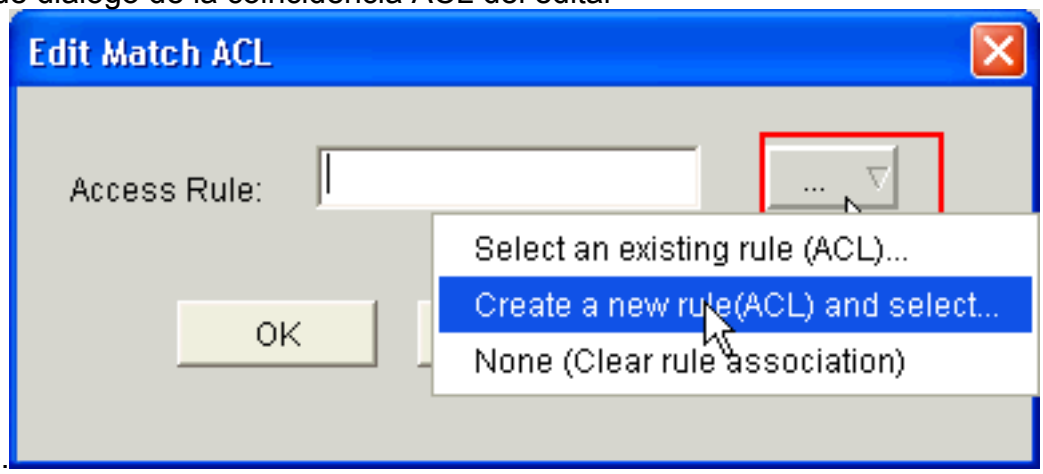
10. De la lista de valores del protocolo disponible, seleccione cada protocolo P2P que usted quiera bloquear, y haga clic el botón de la flecha correcta (**>>**) para mover cada protocolo a la lista de valores del protocolo seleccionada.**Nota:** Para clasificar el tráfico P2P con el NBAR, vaya a la página de descarga del software, y descargue el últimos software y archivos Léame del módulo del idioma descriptivo del protocolo P2P (PDLM). El P2P PDLM disponible para la descarga incluye WinMx, Bittorrent, Kazaa2, el Gnutella, el eDonkey, la vía rápida, y Napster. Dependiendo de su IOS, usted puede ser que no necesite las últimas versiones PDLM puesto que algo pudo ser integrado en su IOS (por ejemplo, vía rápida y Napster). Una vez que está descargado, copie los PDLM al flash del router, y cargúelos en el IOS configurando el **<flash_device nbar del pdlm del IP >: <filename >.pdlm**. Publique el **comando show ip nbar pdlm** para asegurarse que se ha cargado con éxito. Una vez que está cargado, usted puede utilizarlos en las sentencias de protocolo de la coincidencia bajo su configuración de asignación de la clase.



11. Haga clic en OK.
12. En el agregar un cuadro de diálogo de la clase de QoS, las **reglas de acceso** selectas de la lista de la clasificación, y un tecleo **editan** para crear una nueva regla de acceso. Usted puede también asociar una regla de acceso existente a la correspondencia de la clase

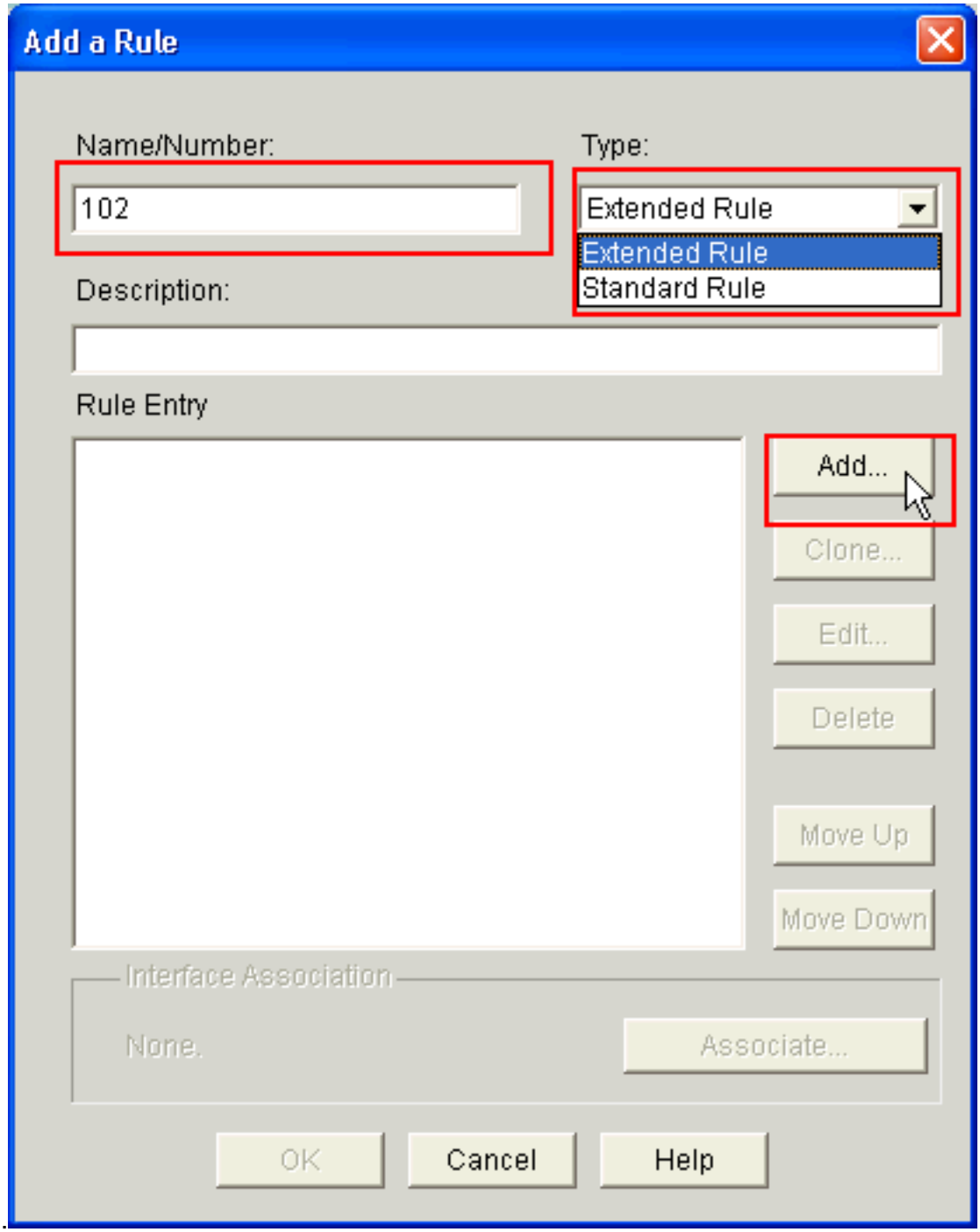


p2p.El cuadro de diálogo de la coincidencia ACL del editar



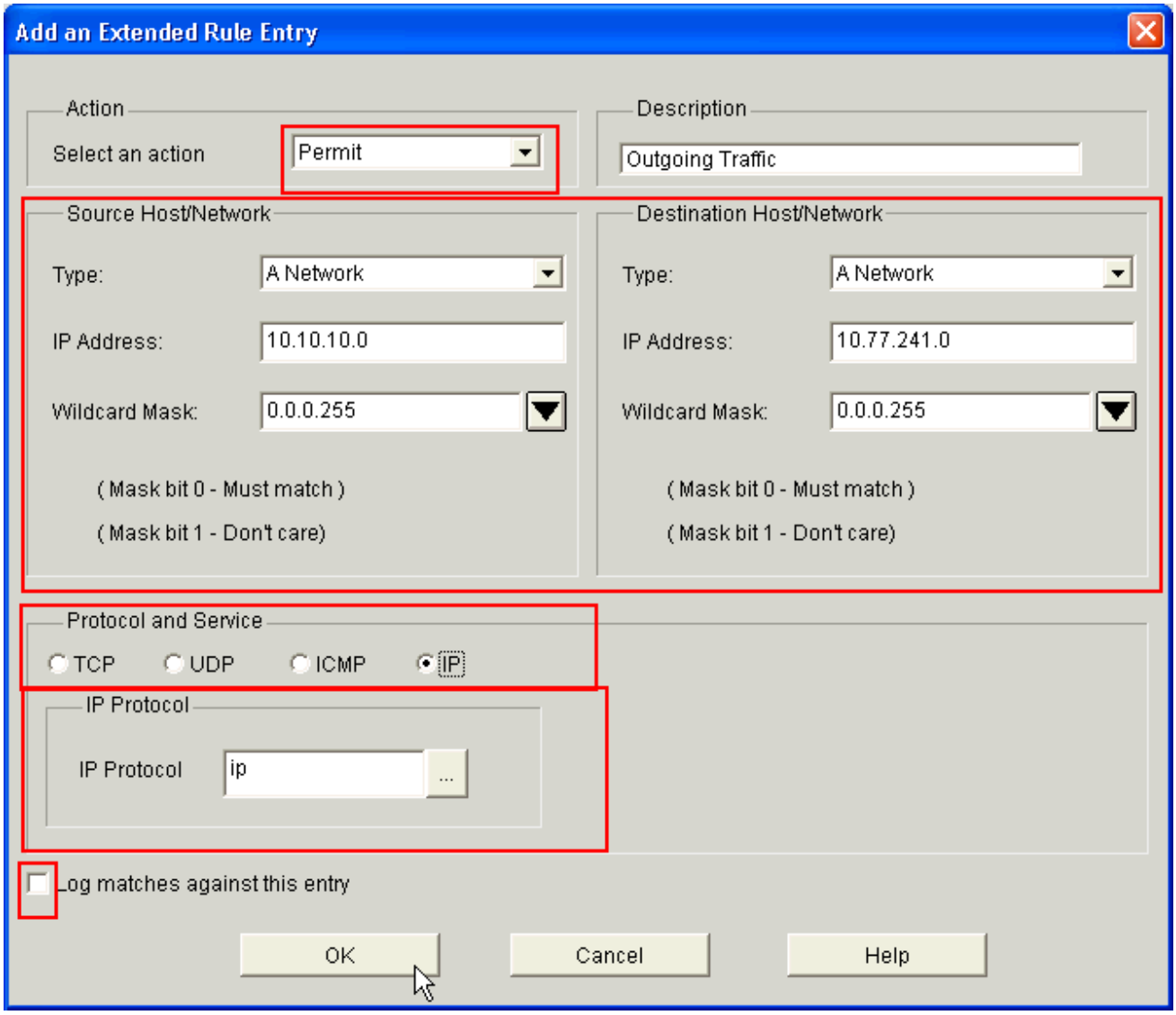
aparece.

13. Haga clic el botón de la regla de acceso (**...**), y elija la opción adecuada. Este ejemplo crea un nuevo ACL.El agregar un cuadro de diálogo de la regla

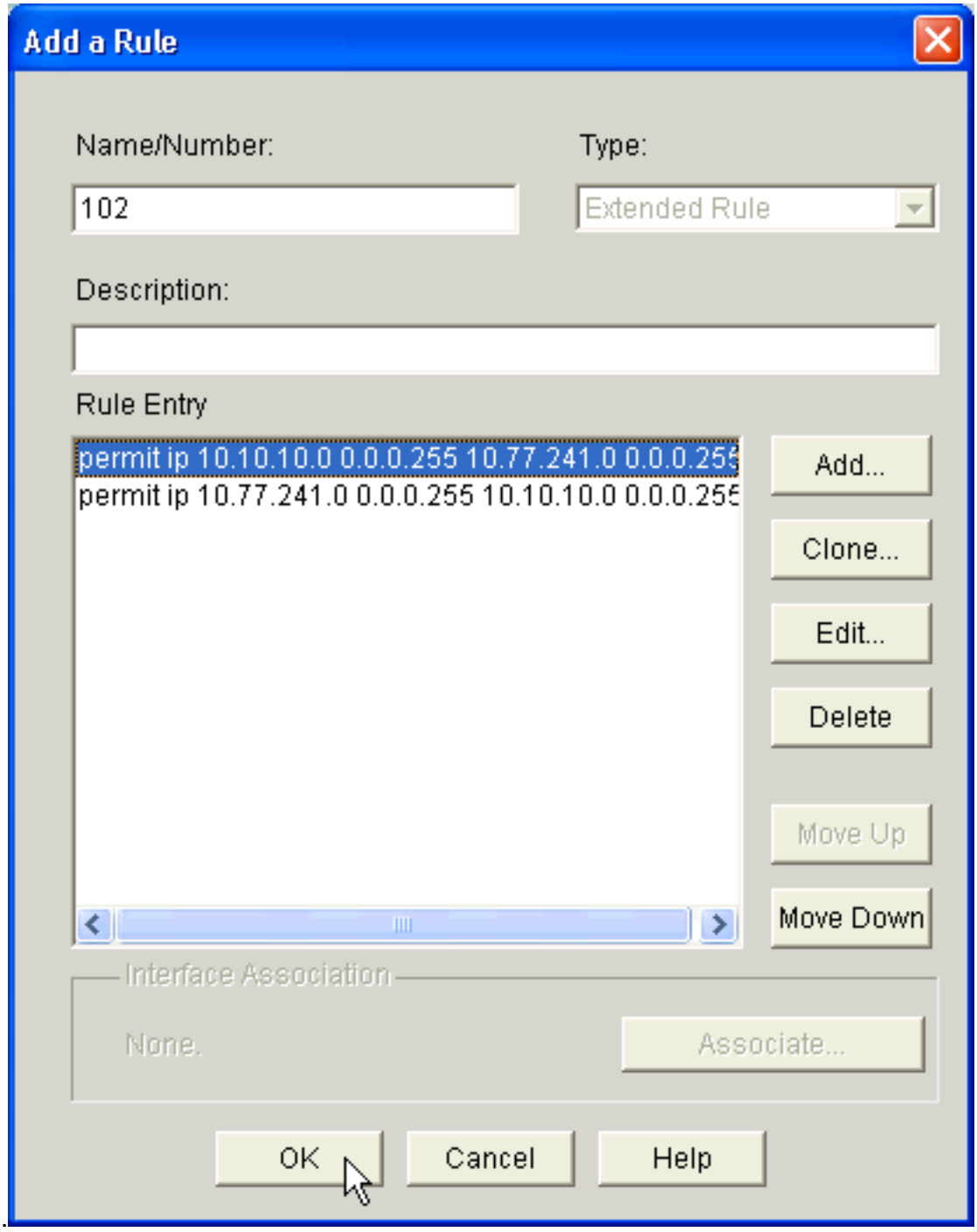


aparece.

14. En el agregar un cuadro de diálogo de la regla, ingresa el nombre o el número del ACL que se creará en el nombre/el campo de número del ACL.
15. De la lista desplegable del tipo, elija el tipo de ACL que se creará (*regla ampliada* o *regla estándar*).
16. El tecleo **agrega** para agregar los detalles al ACL 102.El agregar un cuadro extendido del cuadro de diálogo de entrada de la regla
    aparece.

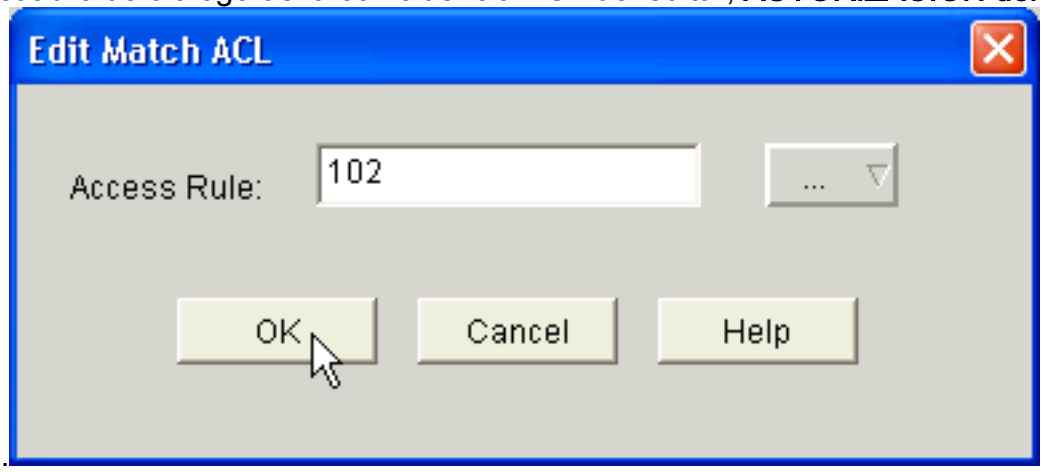


17. En el agregar un cuadro extendido del cuadro de diálogo de entrada de la regla, elige una acción (cualquier *permit or deny*) del selecto una lista desplegable de la acción que indique si la regla ACL si el permit or deny el tráfico entre la fuente y las redes de destino. Esta regla está para el tráfico saliente de la red interna a la red externa.
18. Ingrese las áreas de la información para la fuente y las redes de destino en el /Network del host de origen y del /Network de la computadora principal de destino respectivamente.
19. En el protocolo y la área de servicio, haga clic el botón Appropriate Radio Button. Este ejemplo utiliza el IP.
20. Si usted quiere registrar los paquetes que corresponden con contra esta regla ACL, marque las **coincidencias del registro contra esta** casilla de verificación de la **entrada**.
21. Haga clic en OK.
22. En el agregar un cuadro de diálogo de la regla, **AUTORIZACIÓN del**



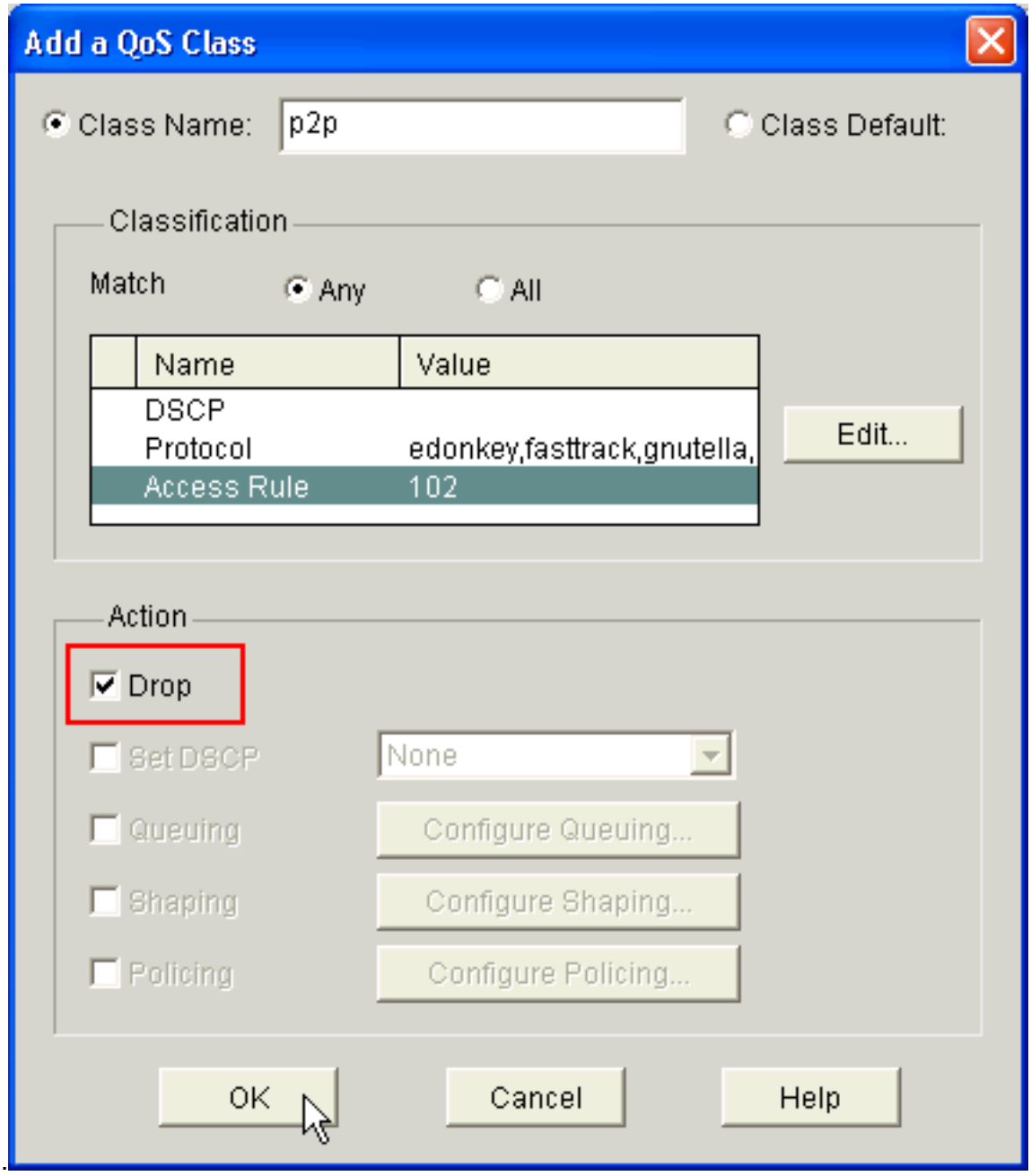
tecleo.

23. En el cuadro de diálogo de la coincidencia ACL del editar, **AUTORIZACIÓN del**



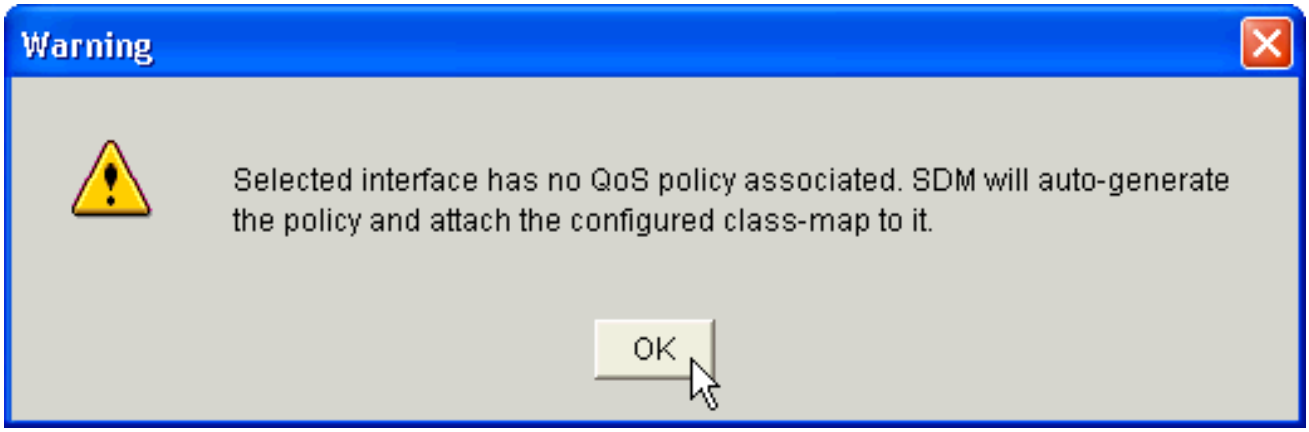
tecleo.

24. En el agregar un cuadro de diálogo de la clase de QoS, marca la casilla de verificación del **descenso** para forzar al router a bloquear el tráfico



P2P.

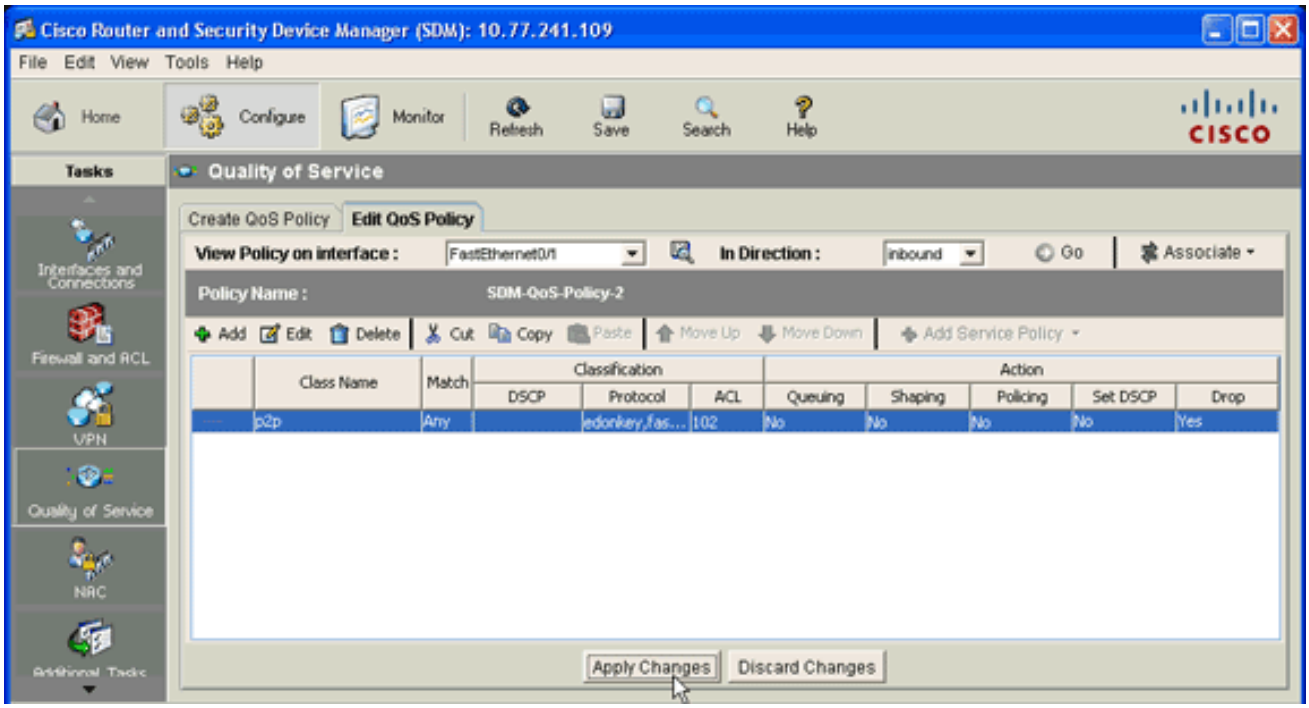
25. Haga clic en OK.El mensaje de advertencia siguiente se muestra por abandono mientras que ningún política de calidad de servicio (QoS) se asocia a la interfaz.



El SDM auto-generará política de calidad de servicio (QoS) y asociará la correspondencia de la clase configurada a la directiva. El equivalente del comando line interface(cli) de este paso de la configuración de SDM es:`R1(config)#`**`policy-map SDM-QoS-Policy-2`**
`R1(config-pmap)#`**`class p2p`**
`R1(config-pmap-c)#`**`drop`**

```
R1(config-pmap-c)#end
R1#
```

26. En la lengueta del editar política de calidad de servicio (QoS), el tecleo **aplica los cambios** para entregar la configuración al router.



Firewall de la aplicación — Característica inmediata de la aplicación del tráfico de mensajes en las versiones deL Cisco IOS 12.4(4)T y posterior

Aplicación inmediata del tráfico de mensajes

El Firewall de la aplicación — La característica inmediata de la aplicación del tráfico de mensajes permite a los usuarios para definir y para aplicar una directiva que especifique se permite a qué tipos de tráfico de Instant Messenger en la red. Usted puede controlar a los mensajeros múltiples (a saber AOL, YAHOO, y MSN) simultáneamente cuando está configurado en la **directiva del appfw** bajo **aplicación im**. Por lo tanto, las funciones adicionales siguientes pueden también ser aplicadas:

- Configuración de las reglas del examen del Firewall
- Inspección de paquetes profunda del payload (que busca los servicios tales como charla del texto)

Nota: La característica Firewall-inmediata de la aplicación del tráfico de mensajes de la aplicación se soporta en las versiones deL Cisco IOS 12.4(4)T y posterior.

Directiva de la aplicación de la mensajería instantánea

El Firewall de la aplicación utiliza una directiva de la aplicación, que consiste en una colección de firmas estáticas, para detectar las violaciones de seguridad. Una firma estática es una colección de parámetros que especifiquen las condiciones del protocolo que deben ser cumplidas antes de que se tomen medidas. Estas condiciones y reacciones del protocolo son definidas por el usuario

final vía el CLI para formar una directiva de la aplicación.

El Firewall de la aplicación del Cisco IOS se ha aumentado para soportar las directivas nativas inmediatas de la aplicación del mensajero. Así, el Firewall Cisco IOS puede ahora detectar y prohibir las conexiones del usuario a los servidores de Instant Messenger para AOL Instant Messenger (AIM), Yahoo! Servicios de mensajería del instante del mensajero, y de MSN Messenger. Estas funciones controlan todas las conexiones para los servicios admitidos, incluyendo el texto, la Voz, el vídeo, y las capacidades de la transferencia de archivos. Las tres aplicaciones pueden ser negadas o ser permitidas individualmente. Cada servicio puede ser controlado individualmente para permitir el servicio de la texto-charla, y la Voz, la transferencia de archivos, el vídeo, y los otros servicios son restrictos. Estas funciones aumentan la capacidad del examen de la aplicación existente para controlar el tráfico de aplicación de Instant Messenger (IM) se ha disfrazado que pues tráfico HTTP (red). Refiera al Firewall de la aplicación - Aplicación inmediata del tráfico de mensajes para más información.

Nota: Si se bloquea una aplicación IM, se reajusta la conexión y un mensaje de Syslog se genera, como apropiado.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- muestre a IP el pdlm nbar — Para visualizar el PDLM funcionando por el NBAR, utilice el **comando show ip nbar pdlm** en el modo EXEC privilegiado:`Router#show ip nbar pdlm`

```
The following PDLMs have been loaded:
flash://edonkey.pdlm
flash://fasttrack.pdlm
flash://gnutella.pdlm
flash://kazaa2.pdlm
```

- muestre a IP la versión nbar — Para el mostrar información sobre la versión del software NBAR en su Cisco IOS Release o la versión de un NBAR PDLM en su router del Cisco IOS, utiliza el **comando version nbar del IP de la demostración** en el modo EXEC privilegiado:`R1#show ip nbar version`

```
NBAR software version:  6

1   base                 Mv: 2
2   ftp                  Mv: 2
3   http                 Mv: 9
4   static               Mv: 6
5   tftp                 Mv: 1
6   exchange             Mv: 1
7   vdolive              Mv: 1
8   sqlnet               Mv: 1
9   rcmd                 Mv: 1
10  netshow              Mv: 1
11  sunrpc               Mv: 2
12  streamwork           Mv: 1
13  citrix               Mv: 10
14  fasttrack            Mv: 2
15  gnutella             Mv: 4
16  kazaa2               Mv: 7
```

```
17  custom-protocols     Mv: 1
18  rtsp                 Mv: 4
19  rtp                  Mv: 5
20  mgcp                 Mv: 2
21  skinny               Mv: 1
22  h323                 Mv: 1
23  sip                  Mv: 1
24  rtcp                 Mv: 2
25  edonkey              Mv: 5
26  winmx                Mv: 3
27  bittorrent           Mv: 4
28  directconnect        Mv: 2
29  skype                Mv: 1


{<No.>}<PDLM name> Mv: <PDLM Version>, {Nv: <NBAR Software Version>; <File name>
}{Iv: <PDLM Interdependency Name>   - <PDLM Interdependency Version>}
```

- show policy-map interface — Para visualizar las estadísticas de paquete de todas las clases que se configuren para todas las políticas de servicio en la interfaz especificada o la subinterfaz o en un circuito virtual permanente (PVC) específico en la interfaz, utilice el **comando show policy-map interface** en el modo EXEC privilegiado:`R1#show policy-map interface fastEthernet 0/1`

```
 FastEthernet0/1

  Service-policy input: SDM-QoS-Policy-2

    Class-map: p2p (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol edonkey
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol fasttrack
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol gnutella
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol kazaa2
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol winmx
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: access-group 102
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol skype
        0 packets, 0 bytes
        5 minute rate 0 bps
      drop

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

- **muestre el directiva-mapa de los ejecutar-config** — Para visualizar todas las configuraciones de correspondencia de políticas así como la configuración de asignación de la política predeterminada, utilice el **comando policy-map de los ejecutar-config de la demostración**:`R1#show running-config policy-map`

```
Building configuration...
```

```
Current configuration : 57 bytes
!
policy-map SDM-QoS-Policy-2
 class p2p
   drop
!
end
```

- **muestre el clase-mapa de los ejecutar-config** — Para visualizar la información sobre la configuración de asignación de la clase, utilice el **comando class-map de los ejecutar-config de la demostración**:`R1#show running-config class-map`

```
Building configuration...

Current configuration : 178 bytes
!
class-map match-any p2p
 match protocol edonkey
 match protocol fasttrack
 match protocol gnutella
 match protocol kazaa2
 match protocol winmx
 match access-group 102
!
end
```

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **lista de acceso de la demostración** — Para visualizar la configuración del accesslist que se ejecuta en el router del Cisco IOS, utilice el **comando show access-list**:`R1#show access-lists`

```
Extended IP access list 102
    10 permit ip 10.10.10.0 0.0.0.255 10.77.241.0 0.0.0.255
    20 permit ip 10.77.241.0 0.0.0.255 10.10.10.0 0.0.0.255
```

Información Relacionada

- Guía de configuración de la Seguridad de Cisco IOS, versión 12.4-Support
- Reconocimiento de aplicaciones basadas en la red (NBAR)
- Reenvío express de Cisco (CEF)
- Soporte Técnico y Documentación - Cisco Systems