Security Device Manager: Obstrua o tráfego P2P em um roteador do Cisco IOS que usa o exemplo da configuração NBAR

Índice

Introdução

Este documento descreve como configurar o roteador do ® do Cisco IOS para obstruir o tráfego (P2P) peer-to-peer da rede interna ao Internet usando o Network Based Application Recognition (NBAR).

O NBAR reconhece os protocolos de rede e os aplicativos de rede específicos que são usados em sua rede. Uma vez que um protocolo ou um aplicativo são reconhecidos pelo NBAR, você pode usar a interface de Command-Line Qualidade de Serviço Modular (MQC) para agrupar os pacotes associados com aqueles protocolos ou aplicativos em classes. Estas classes são agrupadas com base em se os pacotes se conformam a determinados critérios.

Para o NBAR, o critério é se o pacote combina um protocolo ou um aplicativo específico conhecido ao NBAR. Usando o MQC, o tráfego de rede com um protocolo de rede (Citrix, por exemplo) pode ser colocado em uma classe de tráfego, quando o tráfego que combina um protocolo de rede diferente (gnutella, por exemplo) puder ser colocado em uma outra classe de tráfego. Mais tarde, o tráfego de rede dentro de cada classe pode ser dado o tratamento de QoS

apropriado usando uma política de tráfego (mapa de política). Consulte o tráfego de rede de classificação usando a seção NBAR do *manual de configuração das soluções da Qualidade de serviço Cisco IOS* para obter mais informações sobre do NBAR.

Pré-requisitos

Requisitos

Antes que você configure o NBAR para obstruir o tráfego P2P, você deve permitir o Cisco Express Forwarding (CEF).

Use o **cef IP no** modo de configuração global a fim permitir o CEF:

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

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 2801 Router com liberação 12.4(15)T do Cisco IOS ® Software
- Versão 2.5 do gerenciador do dispositivo de segurança da Cisco (SDM)

Nota: Refira a configuração de roteador básico usando o SDM a fim permitir que o roteador seja configurado pelo SDM.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Vista geral do Network Based Application Recognition (NBAR)

O Network-Based Application Recognition (NBAR) é um Engine de classificação que reconheça e classifique uma ampla variedade de protocolos e de aplicativos. Quando o NBAR reconhece e classifica um protocolo ou um aplicativo, a rede pode ser configurada para aplicar o Qualidade de Serviço (QoS) apropriado para esse aplicativo ou tráfego com esse protocolo.

O NBAR executa estas funções:

- **Identificação dos aplicativos e dos protocolos (camada 4 para mergulhar 7)**O NBAR pode classificar os aplicativos que se usam:Números de porta estaticamente atribuídos do protocolo transfer control (TCP) e do User Datagram Protocol (UDP).NON-UDP e protocolos IP não-TCP.Números de porta dinamicamente atribuídos TCP e UDP negociados durante o estabelecimento de conexão. A inspeção stateful é exigida para a classificação dos aplicativos e dos protocolos. A inspeção stateful é a capacidade para descobrir as conexões

de dados que serão classificadas passando as conexões de controle sobre a porta da conexão de dados onde as atribuições são feitas.Classificação de porta secundária: Classificação do HTTP (as URL, mimicam ou nomes de host) e do tráfego de computação independente da arquitetura dos aplicativos de Citrix (ICA) baseado no nome do aplicativo publicado.Classificação baseada na inspeção de pacote de informação profunda e em atributos característicos da aplicação múltiplos. A classificação do payload do Real-Time Transport Protocol (RTP) é baseada neste algoritmo em que o pacote é classificado como o RTP baseado em atributos múltiplos no cabeçalho de RTP.

- **Descoberta de protocolo**A descoberta de protocolo é uma característica de uso geral NBAR que recolha o aplicativo e as estatísticas de protocolo (contagens de pacote de informação, contagens de byte, e taxas de bits) pela relação. As ferramentas de gerenciamento baseadas GUI podem graficamente indicar esta informação, votando estatísticas de SNMP do Management Information Base paládio NBAR (MIB). Como com toda a característica dos trabalhos em rede, é importante compreender as características do desempenho e da escalabilidade antes de distribuir a característica em uma rede de produção. Nas plataformas baseada em software, o medidor que são consideradas é impacto da utilização CPU e a taxa de dados sustentável quando esta característica for permitida. A fim configurar o NBAR para descobrir o tráfego para todos os protocolos que são sabidos ao NBAR em uma interface particular, use o comando ip nbar protocol-discovery no modo de configuração da interface ou no modo de configuração de vlan. A fim desabilitar a descoberta do tráfego, não use **nenhum comando ip nbar protocol-discovery**.

Configurar a obstrução peer-to-peer do tráfego (P2P)

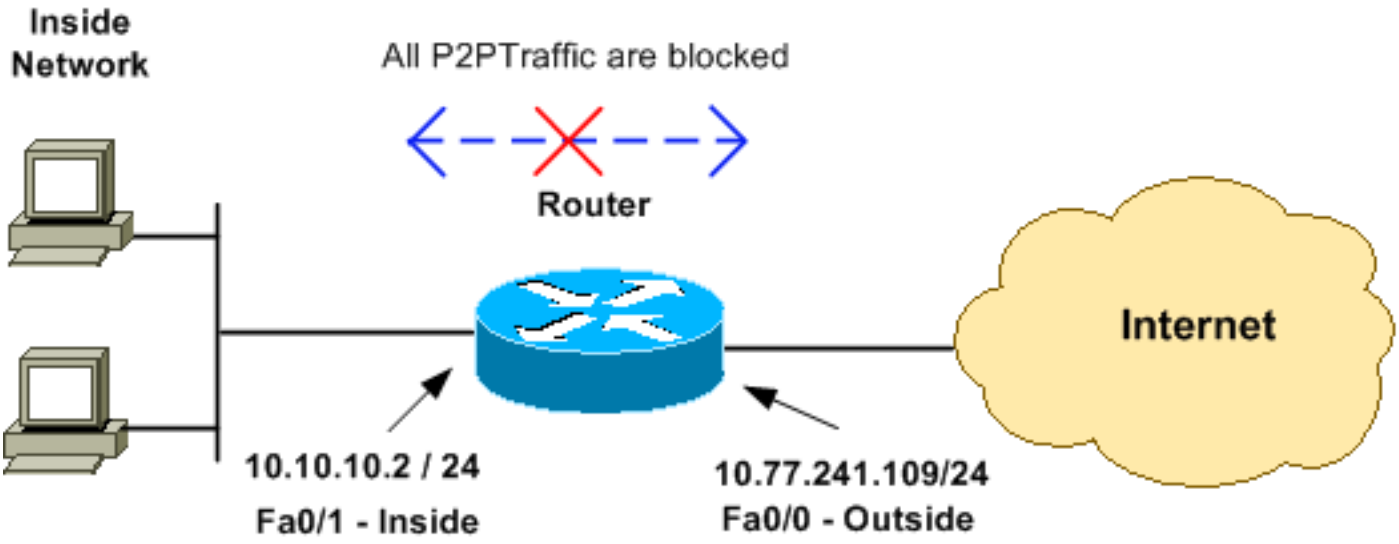
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Algum tráfego P2P não pode ser completamente obstruído devido à natureza de seu protocolo P2P. Estes protocolos P2P mudam dinamicamente suas assinaturas para contornear todos os motores DPI que tentarem obstruir completamente seu tráfego. Consequentemente, Cisco recomenda que você limita a largura de banda em vez completamente dos obstruir. (Estrangule a largura de banda para este tráfego. Dê muito menos largura de banda; contudo, deixe a conexão ir completamente.)

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configuração do roteador

Configuração para obstruir o tráfego P2P no roteador do 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
```

Configurar o roteador com SDM

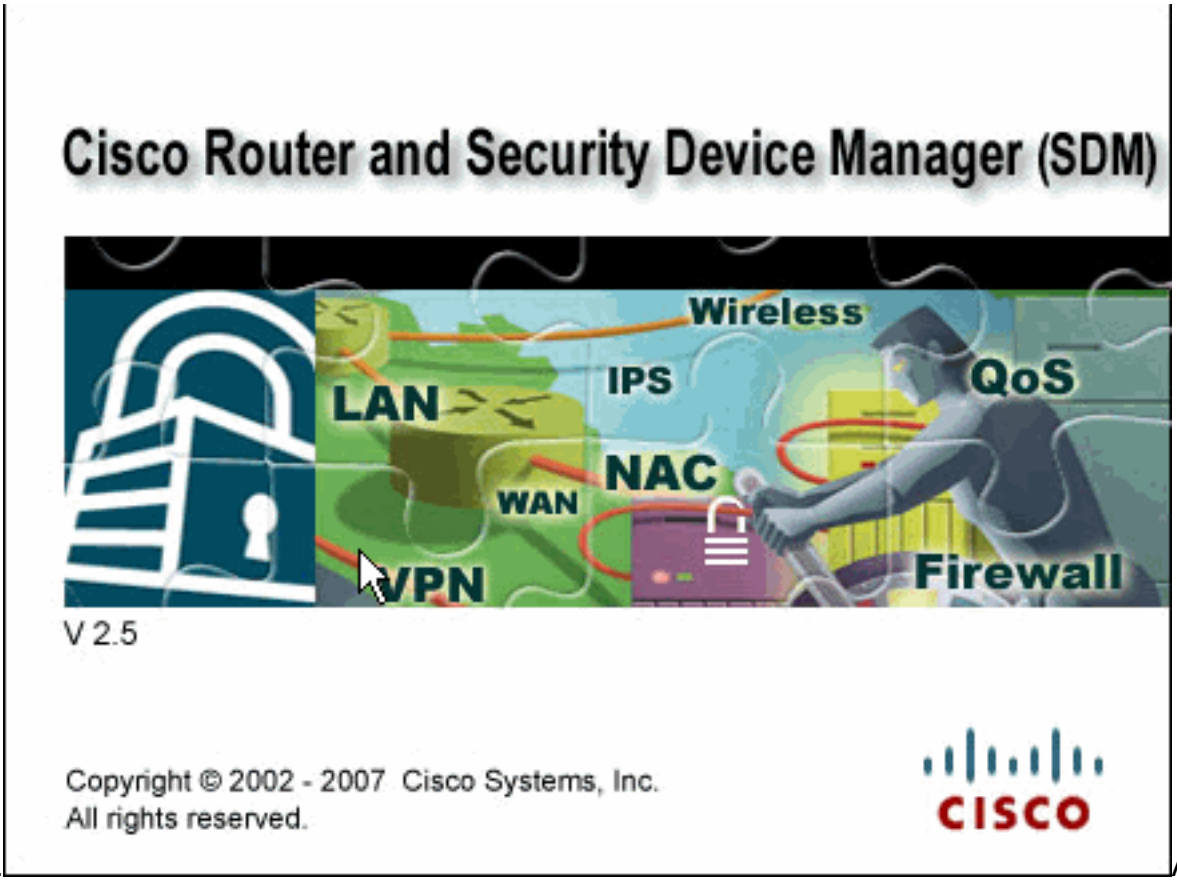
Configuração de SDM do roteador

Termine estas etapas a fim configurar a obstrução do tráfego P2P em um roteador do Cisco IOS:

Nota: A fim configurar o NBAR para descobrir o tráfego para todos os protocolos que são sabidos ao NBAR em uma interface particular, o comando ip nbar protocol-discovery deve ser usado no modo de configuração da interface ou no modo de configuração de vlan para permitir a descoberta do tráfego. Continue com a configuração de SDM após ter configurado a descoberta de protocolo na interface requerida onde a política de QoS configurada está sendo usada.

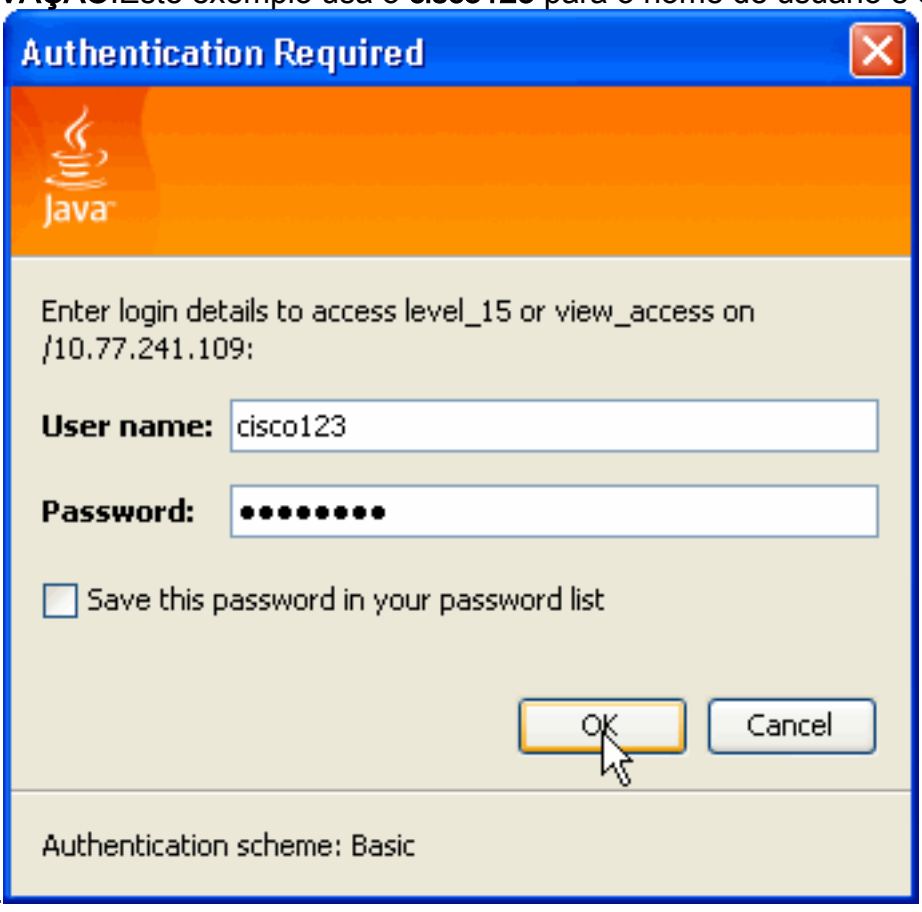
```
Hostname#config t
              Hostname(config)#interface fastEthernet 0/1
              Hostname(config-if)#ip nbar protocol-discovery
              Hostname(config-if)#end
```

1. Abra um navegador, e incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do roteador que foi configurado para o acesso SDM. Por exemplo, **<SDM_Router_IP_Address de https:// >**Certifique-se autorizar todos os avisos que seu navegador o der relativo à autenticidade de certificado de SSL. O nome de usuário padrão e a senha são ambos placa.O roteador indica este indicador para permitir a transferência do aplicativo SDM. Este exemplo carrega o aplicativo no computador local e não o é executado em um Java



applet. A transferência SDM começa agora.

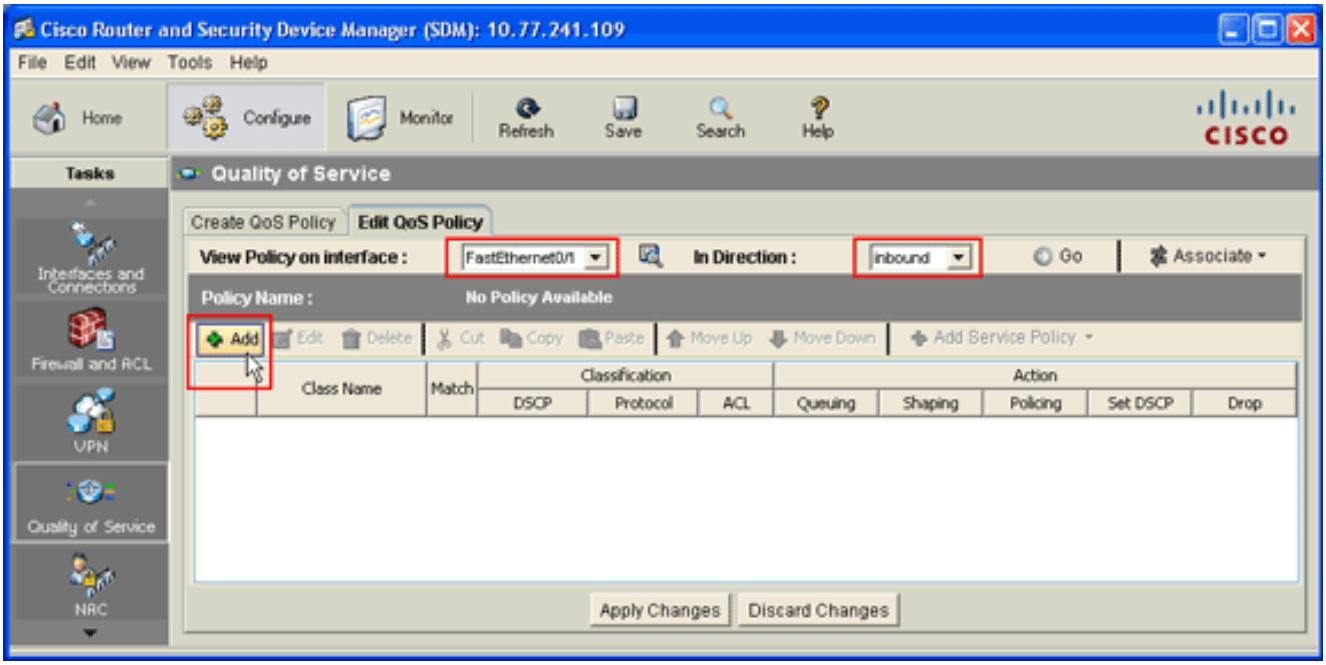
2. Uma vez as transferências do lançador SDM, terminam as etapas dirigidas pelas alertas a fim instalar o software e executar o lançador de Cisco SDM.
3. Incorpore um nome de usuário e uma senha, se você especificou um, e clique a **APROVAÇÃO**.Este exemplo usa o **cisco123** para o nome de usuário e o **cisco123** como a



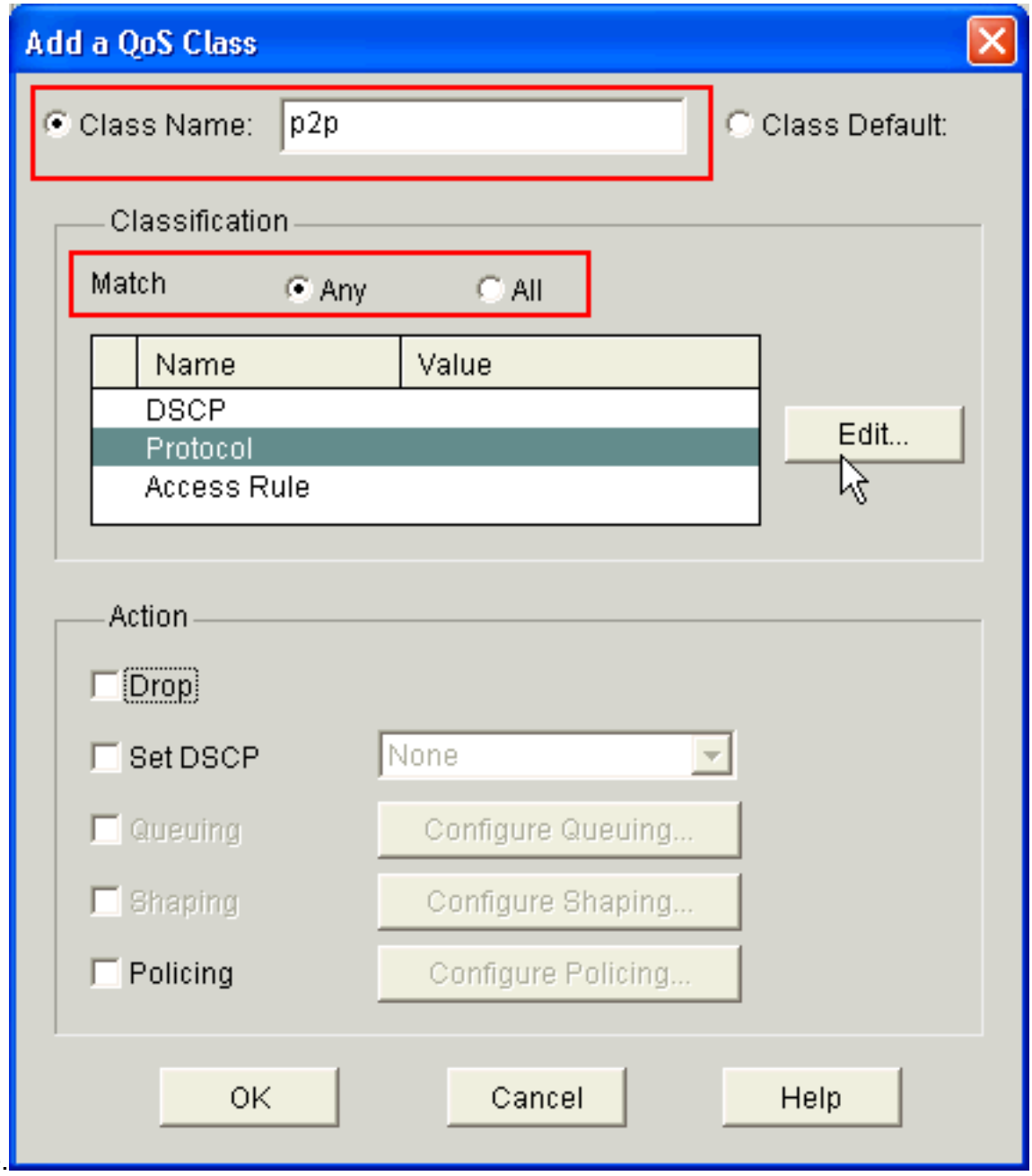
senha.

4. Escolha **configuram > Qualidade de Serviço**, e clicam a aba da **política de QoS da edição no**

Home Page
SDM.

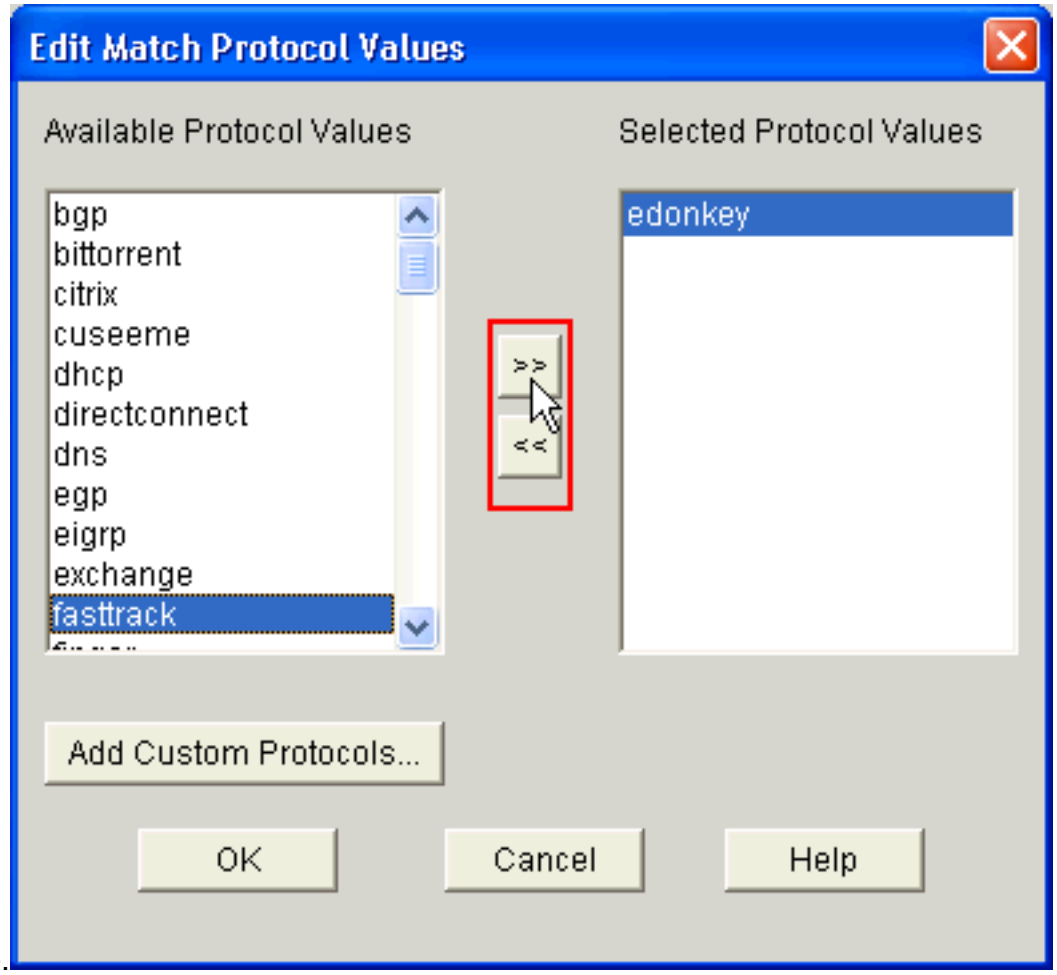


5. Da política da vista na lista de drop-down da relação, escolha o nome da relação, e escolha então o fluxo da direção de tráfego (de entrada ou de partida) do na lista de drop-down do sentido.Neste exemplo, a relação é *FastEthernet0/1*, e o sentido é *de entrada*.
6. O clique **adiciona** a fim adicionar uma classe nova de QoS para a relação.Adicionar uma caixa de diálogo da classe de QoS



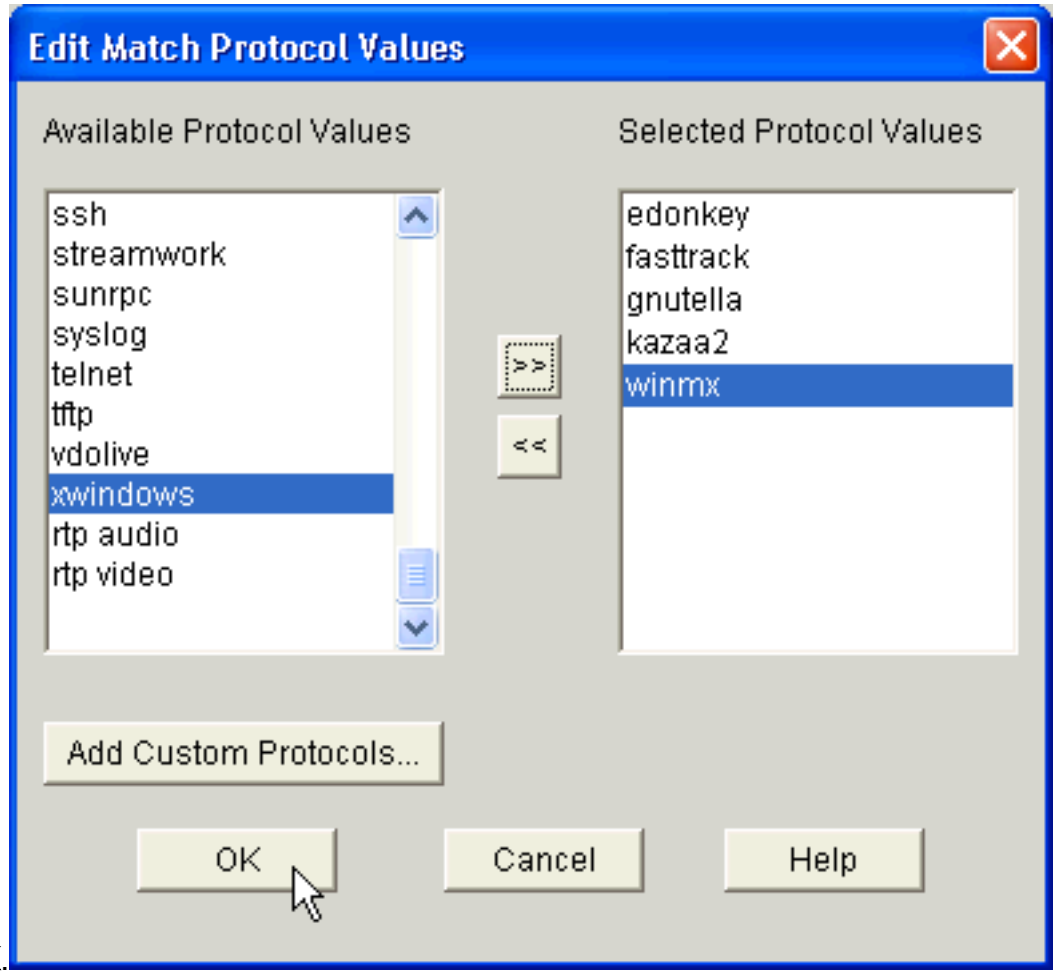
aparece.

7. Se você quer criar uma classe nova, clique o botão de rádio do **nome de classe**, e dê entrada com um nome para sua classe. Se não, clique o botão de rádio do **padrão da classe** se você quer usar a classe padrão.Este exemplo cria uma classe nova nomeada *p2p*.
8. Na área da classificação, clique **todo o** botão de rádio ou **todo o** botão de rádio para a opção do fósforo.Este os exemplos usam *toda a* opção do fósforo, que executar o comando compatível com qualquer p2p do mapa de classe no roteador.
9. Selecione o **protocolo na** lista de Classifcation, e o clique **edita** a fim editar o parâmetro de protocolo.A caixa de diálogo dos valores de protocolo do fósforo da edição

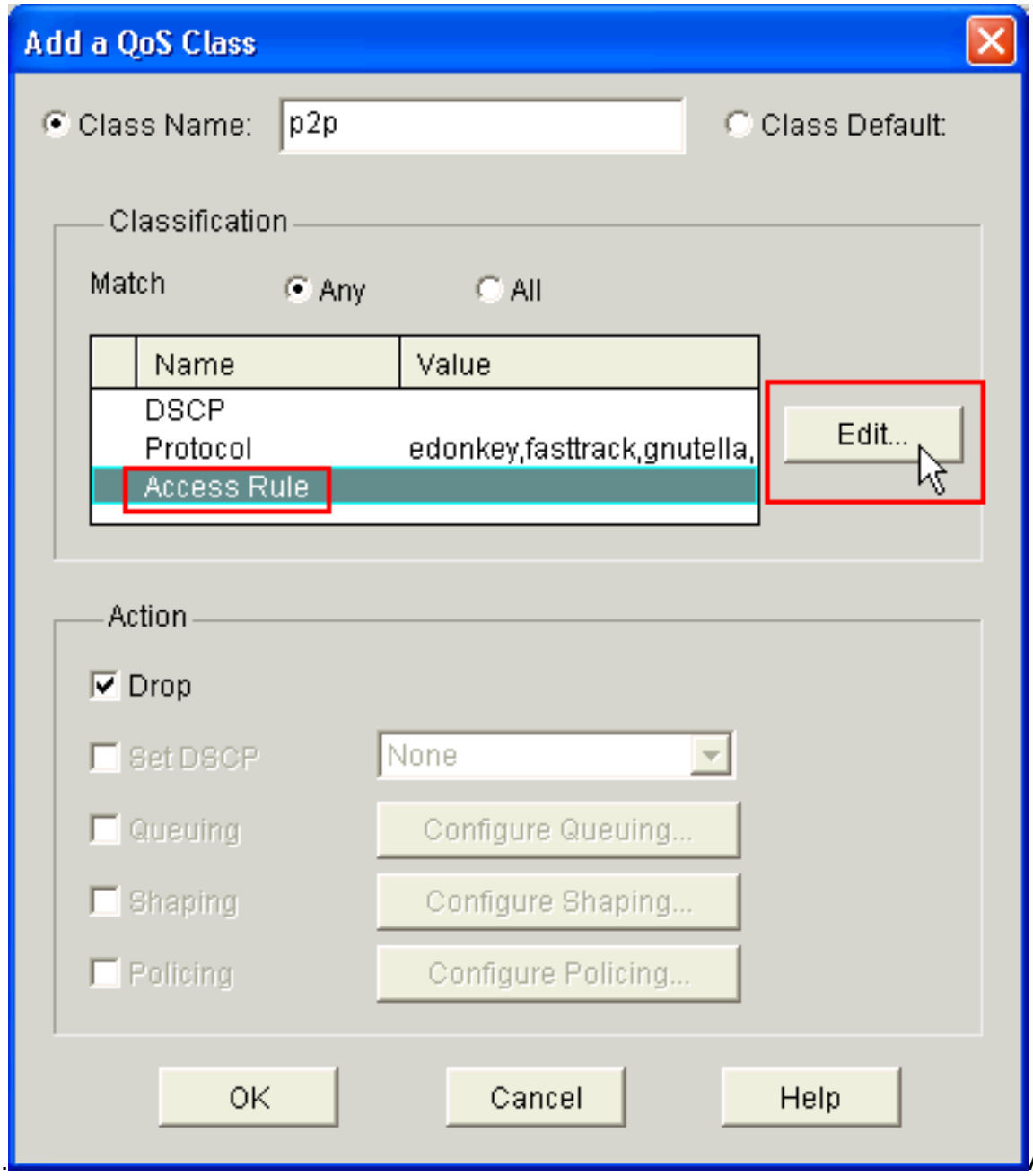


aparece.

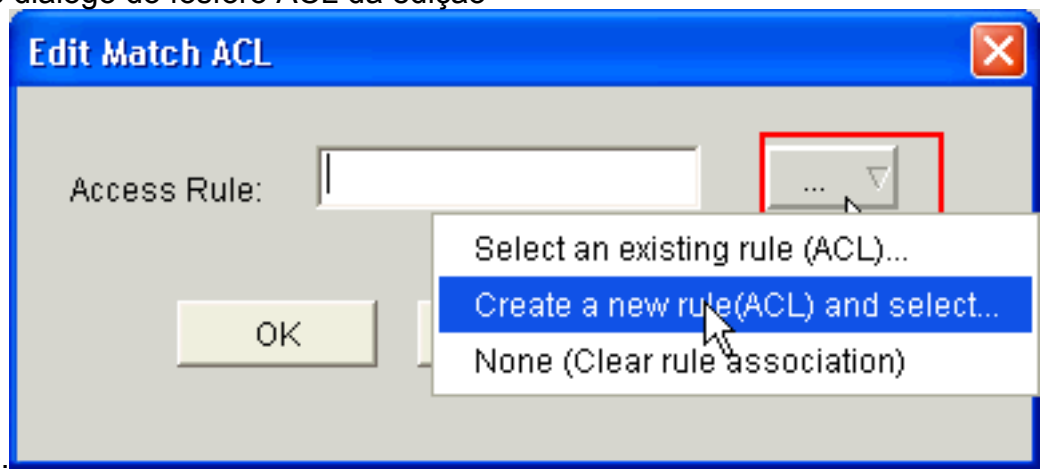
10. Da lista de valores de protocolo disponível, selecione cada protocolo P2P que você quer obstruir, e clique o botão da seta direita (**>>**) para mover cada protocolo para a lista de valores de protocolo selecionada.**Nota:** A fim classificar o tráfego P2P com NBAR, vá à página de download de software, e transfira o software e os arquivos de leia-me os mais atrasados do módulo da língua de descrição do protocolo P2P (PDLM). O P2P PDLM disponível para a transferência inclui WinMx, Bittorrent, Kazaa2, Gnutella, eDonkey, Fasttrack, e Napster. Segundo seus IO, você não pôde precisar as versões as mais atrasadas PDLM desde que alguns puderam ser integrados em seus IO (por exemplo, Fasttrack e Napster). Uma vez que transferido, copie os PDLM ao flash do roteador, e carregue-os em IO configurando o **<flash_device nbar do pdlm IP >: <filename >.pdlm**. Emita o **comando show ip nbar pdlm** a fim assegurar-se de que esteja carregado com sucesso. Uma vez que carregado, você pode usá-los nas declarações de protocolo do fósforo sob sua configuração de mapa da classe.



11. Clique em **OK**.
12. Adicionar uma caixa de diálogo da classe de QoS, umas **regras** seletas do **acesso da** lista da classificação, e um clique **editam** a fim criar uma regra nova do acesso. Você pode igualmente traçar uma regra existente do acesso ao mapa da classe

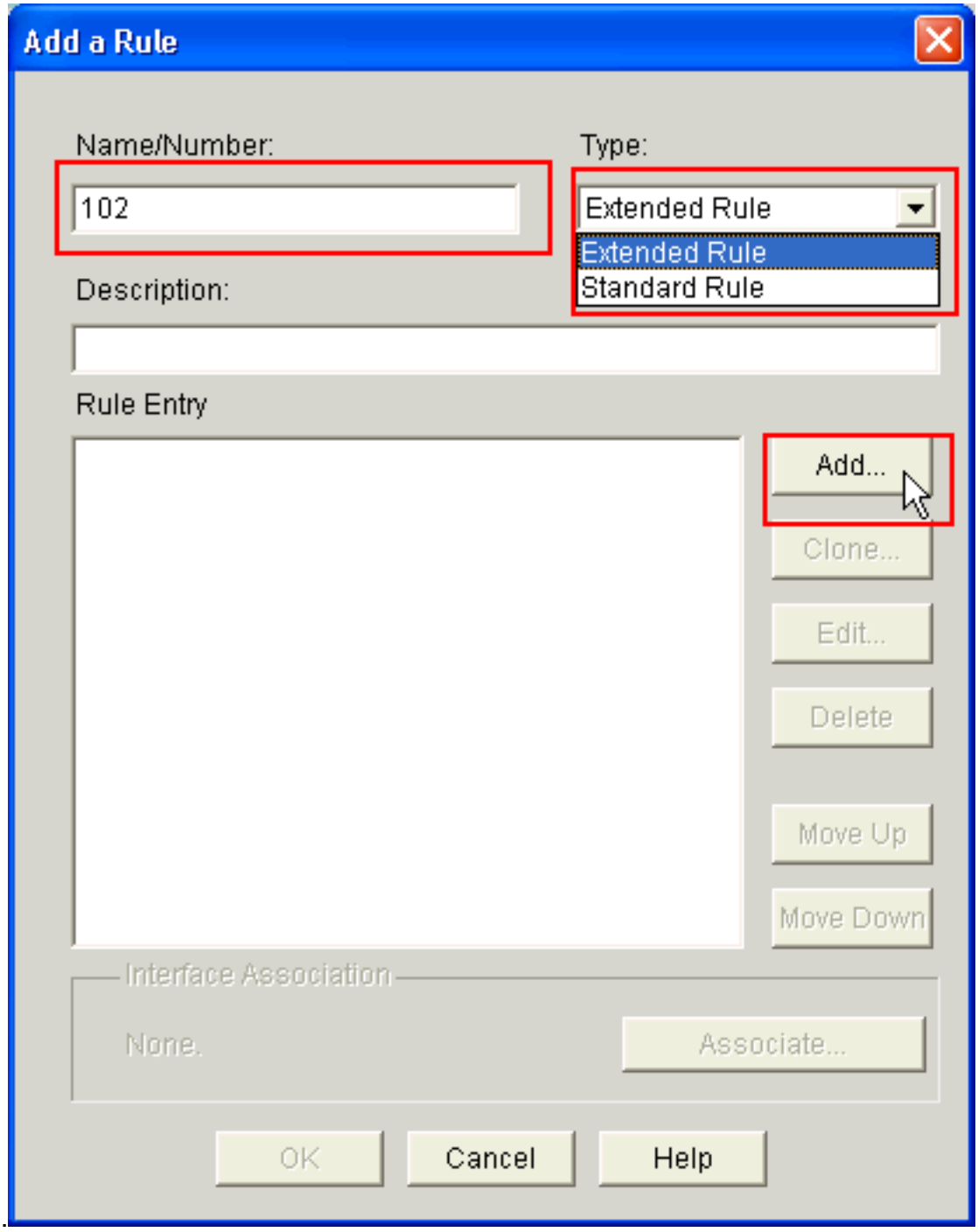


p2p.A caixa de diálogo do fósforo ACL da edição



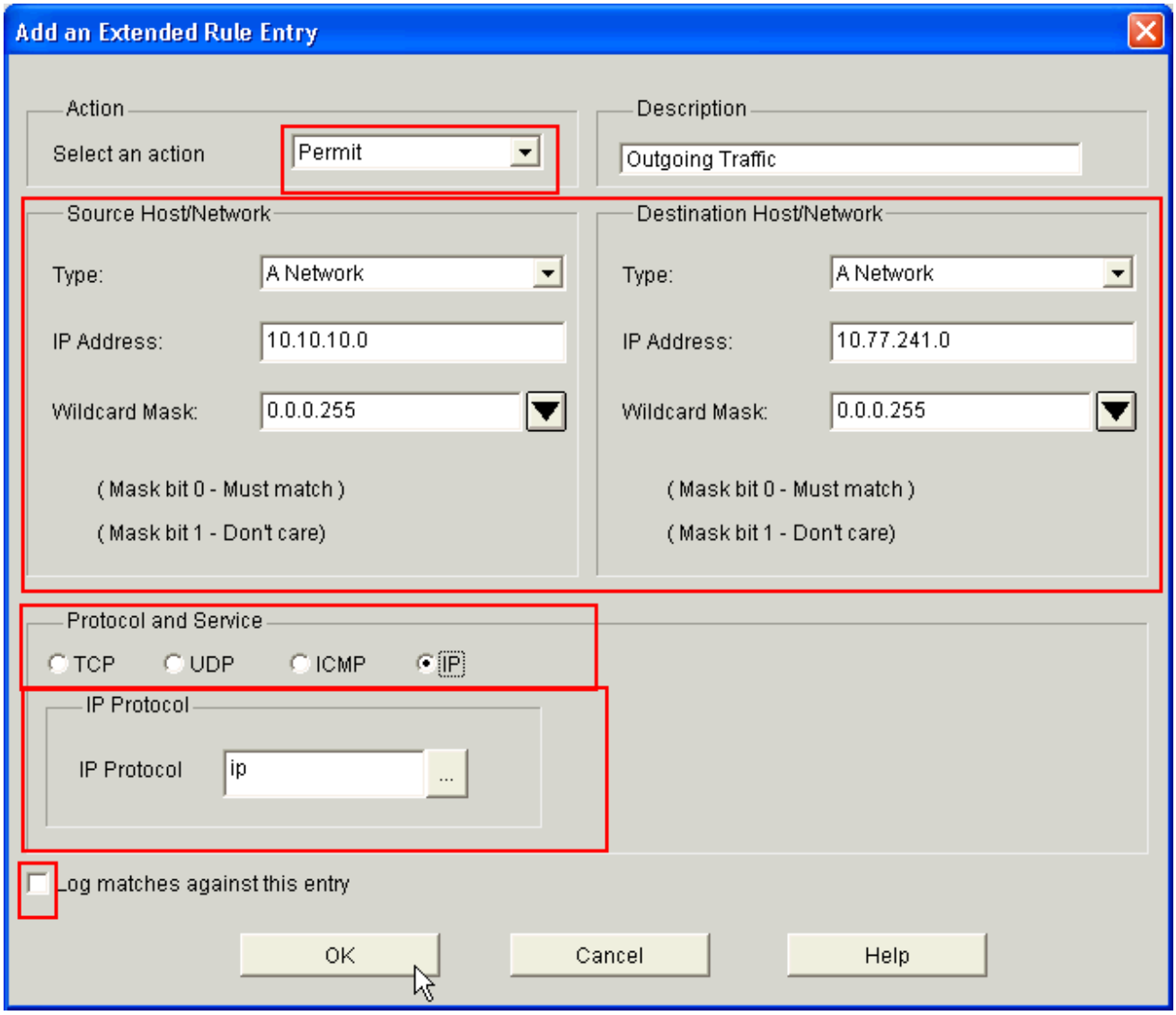
aparece.

13. Clique o botão da regra do acesso (**...**), e escolha a opção apropriada. Este exemplo cria um ACL novo.Adicionar uma caixa de diálogo da regra

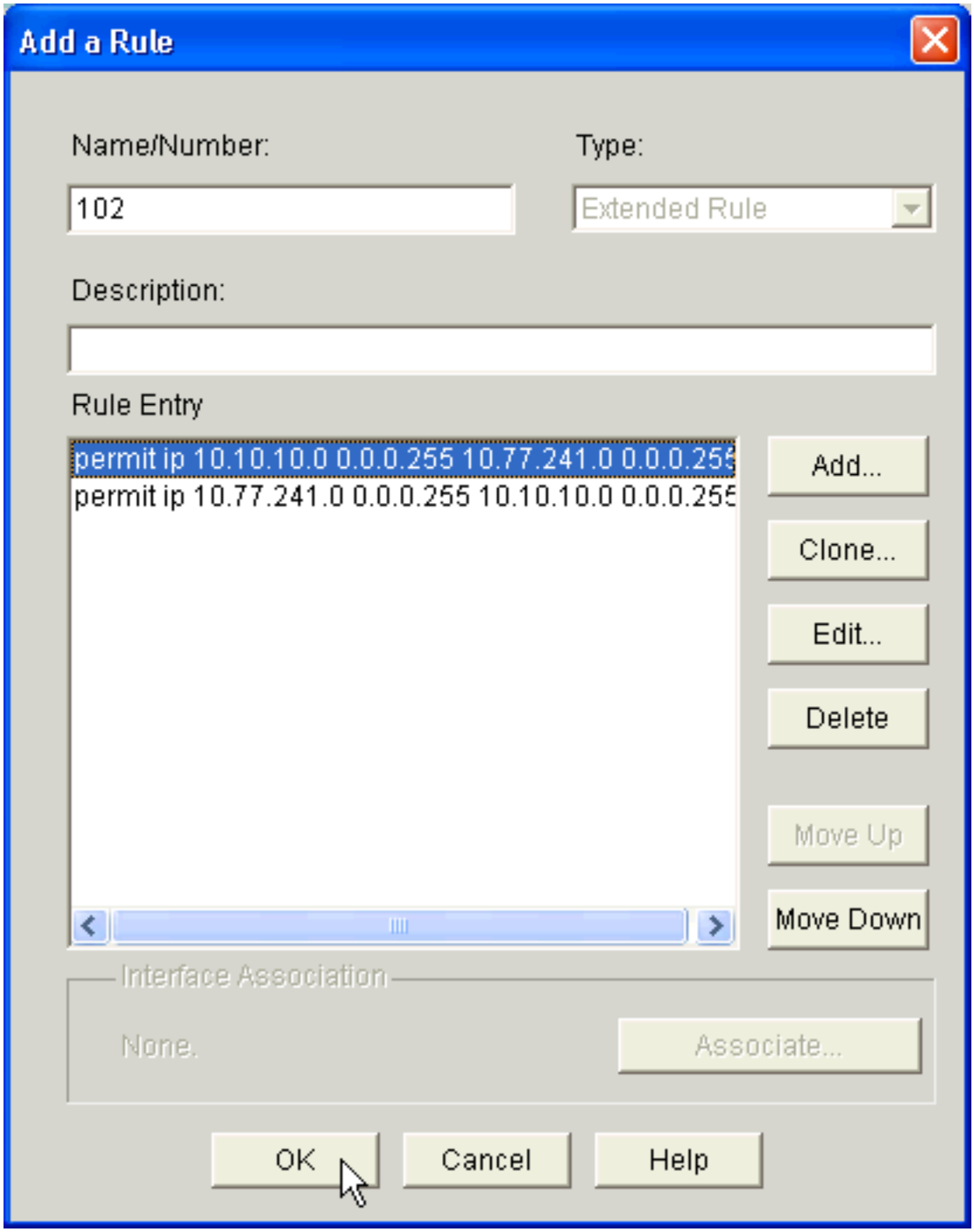


aparece.

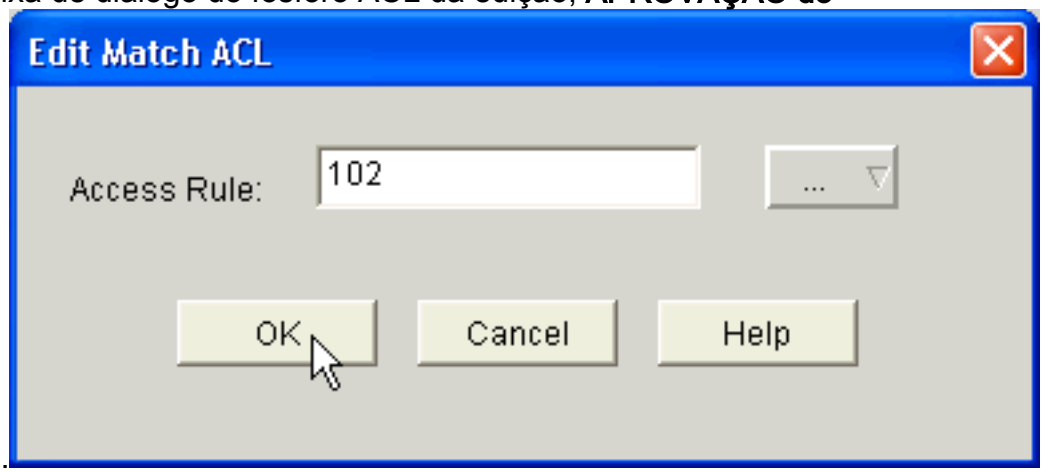
14. Adicionar uma caixa de diálogo da regra, incorpora o nome ou o número do ACL a ser criado no nome/campo de número do ACL.
15. Do tipo lista de drop-down, escolha o tipo de ACL a ser criado (*regra estendida* ou *regra do padrão*).
16. O clique **adiciona** a fim adicionar detalhes ao ACL 102.Adicionar uma caixa prolongada do diálogo de entrada da regra
    aparece.



17. Adicionar uma caixa prolongada do diálogo de entrada da regra, escolhe uma ação (um ou outro *permit or deny*) do seleto uma lista de drop-down da ação que indique se a regra ACL se o permit or deny o tráfego entre a fonte e as redes de destino. Esta regra é para o tráfego de saída da rede interna à rede externa.
18. Incorpore áreas da informação para a fonte e as redes de destino ao /Network do host de origem e do /Network do host de destino respectivamente.
19. No protocolo e na área de serviço, clique o botão Appropriate Radio Button. Este exemplo usa o IP.
20. Se você quer registrar os pacotes de harmonização contra esta regra ACL, verifique os **fósforos do log contra esta** caixa de verificação da **entrada**.
21. Clique em **OK**.
22. Adicionar uma caixa de diálogo da regra, clica a **APROVAÇÃO**.

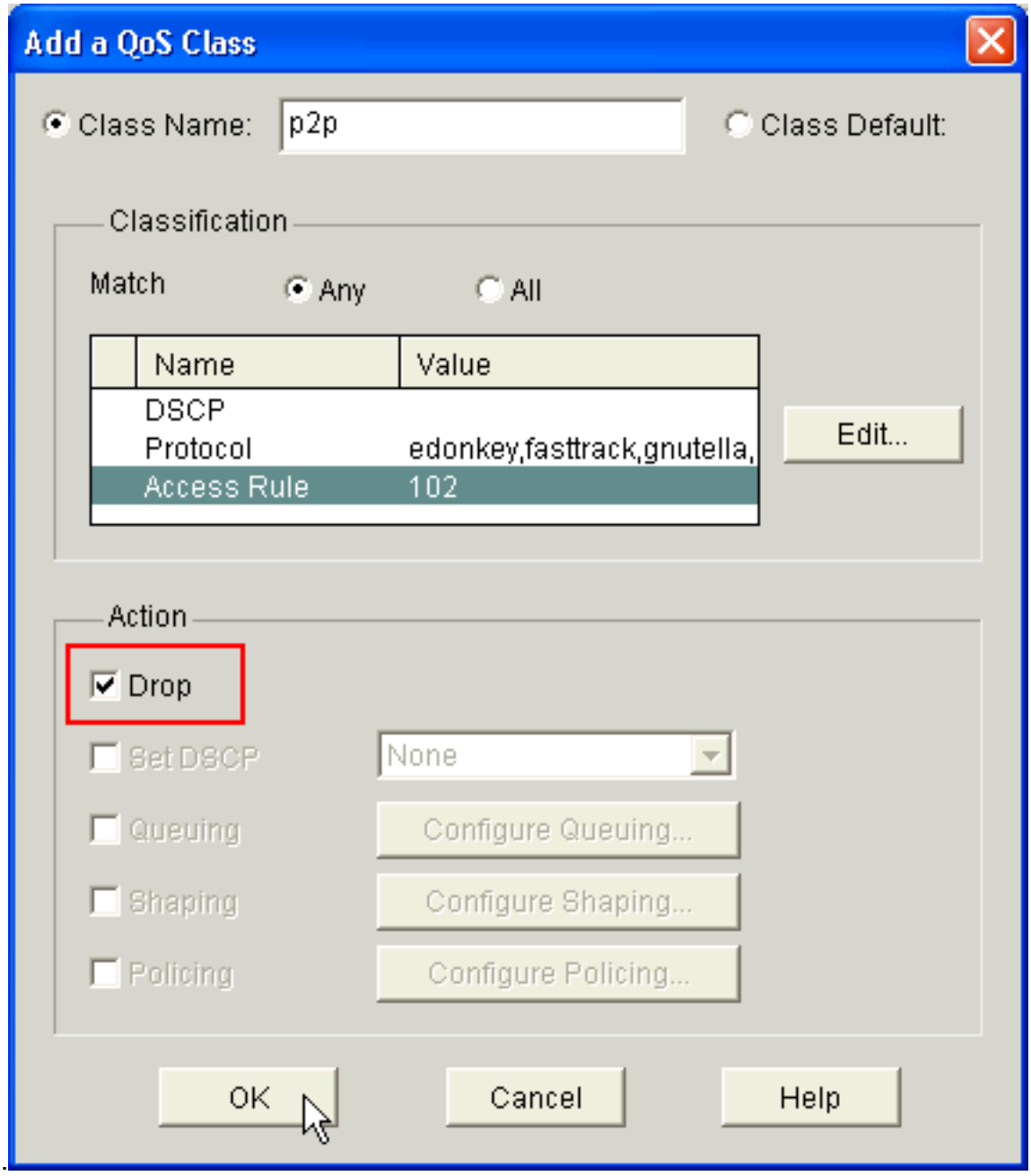


23. Na caixa de diálogo do fósforo ACL da edição, **APROVAÇÃO do**



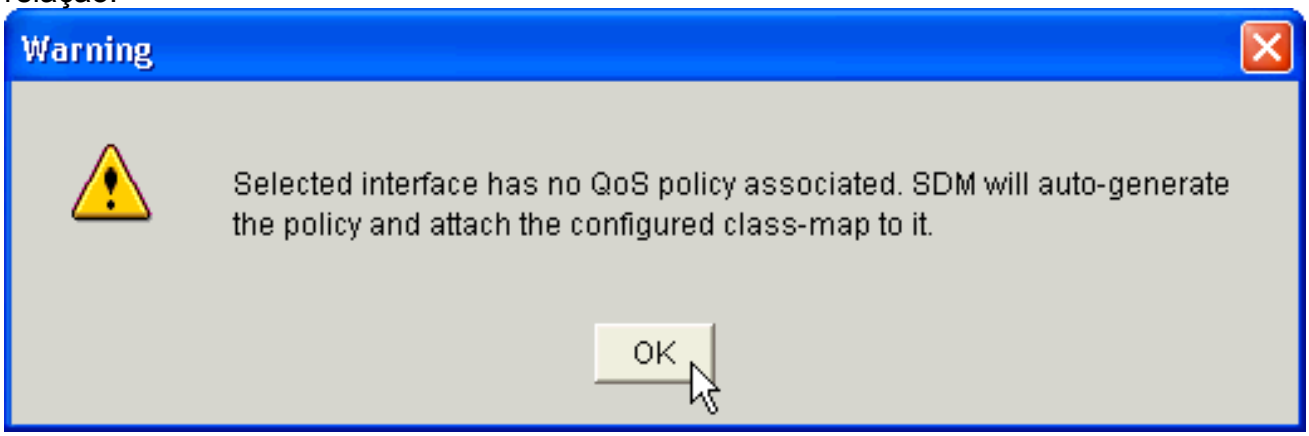
clique.

24. Adicionar uma caixa de diálogo da classe de QoS, verifica a caixa de verificação da **gota** a fim forçar o roteador a obstruir o tráfego



P2P.

25. Clique em **OK**.O seguinte mensagem de advertência é mostrado à revelia porque nenhuma política de QoS é traçada à relação.

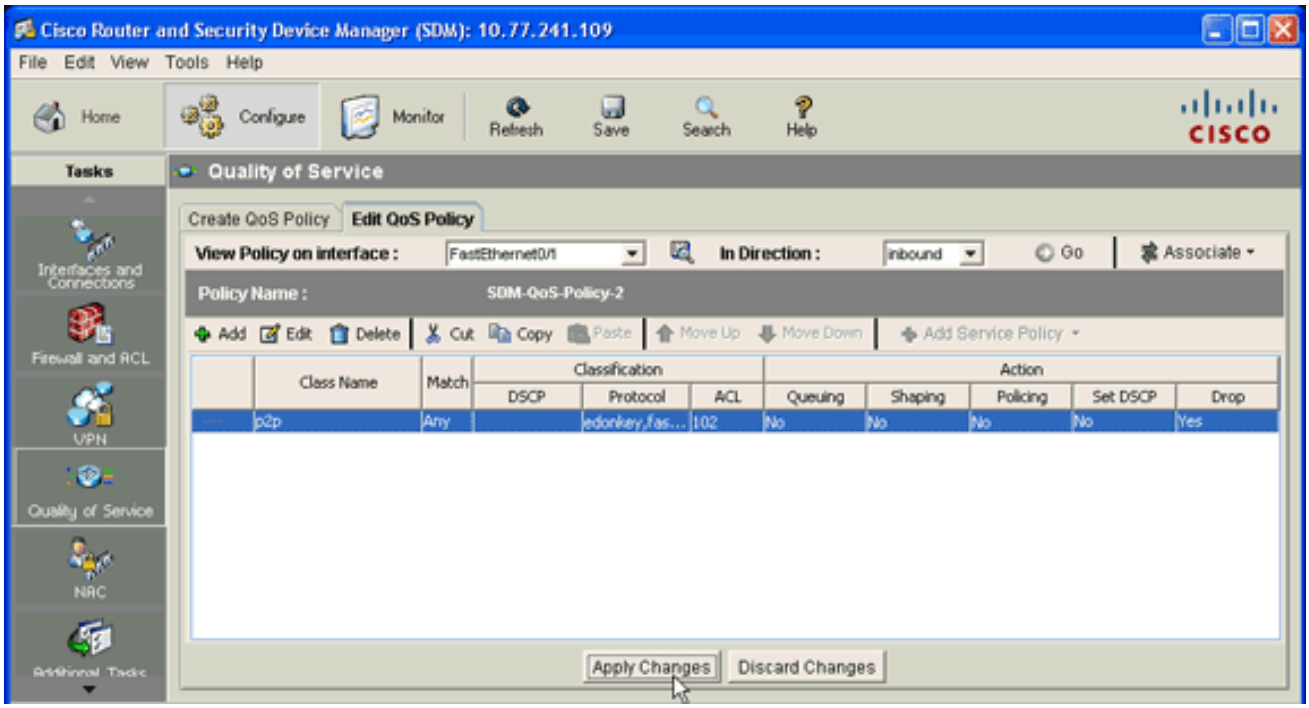


O SDM auto-gerará a política de QoS e anexará o mapa da classe configurada à política. O equivalente do comando line interface(cli) desta etapa da configuração de SDM é:

```
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. Na aba da política de QoS da edição, o clique **aplica mudanças** a fim entregar a configuração ao roteador.



Firewall do aplicativo — Característica imediata da aplicação do tráfego de mensagem nas versões do Cisco IOS 12.4(4)T e mais tarde

Aplicação imediata do tráfego de mensagem

O Firewall do aplicativo — A característica imediata da aplicação do tráfego de mensagem permite usuários de definir e reforçar uma política que especifique que tipos de tráfego de Instant Messenger são permitidos na rede. Você pode controlar os mensageiros múltiplos (a saber AOL, YAHOO, e MSN) simultaneamente quando configurado na **política do appfw** sob o **aplicativo im**. Consequentemente, a seguinte funcionalidade adicional pode igualmente ser reforçada:

- Configuração de regras da inspeção do Firewall
- Inspeção de pacote de informação profunda do payload (que procura serviços tais como o bate-papo do texto)

Nota: A característica Firewall-imediata da aplicação do tráfego de mensagem do aplicativo é apoiada nas versões do Cisco IOS 12.4(4)T e mais tarde.

Política do aplicativo de Instant Messenger

O Firewall do aplicativo usa uma política do aplicativo, que consista em uma coleção de assinaturas estáticas, para detectar violações de segurança. Uma assinatura estática é uma coleção dos parâmetros que especificam as condições do protocolo que devem ser estadas conformes antes que uma ação esteja tomada. Estas condições e reações do protocolo são definidas pelo utilizador final através do CLI para formar uma política do aplicativo.

O Firewall do aplicativo do Cisco IOS foi aumentado para apoiar políticas nativas imediatas do aplicativo do mensageiro. Assim, o Cisco IOS Firewall pode agora detectar e proibir conexões do usuário aos server de Instant Messenger para AOL Instant Messenger (AIM), Yahoo! Serviços de mensagens instantâneas do mensageiro, e do MSN Messenger. Esta funcionalidade controla todas as conexões para serviços suportados, incluindo o texto, a Voz, o vídeo, e as capacidades de transferência de arquivo. Os três aplicativos podem individualmente ser negados ou permitido. Cada serviço pode individualmente ser controlado de modo que o serviço do texto-bate-papo seja permitido, e a Voz, transferência de arquivo, o vídeo, e os outros serviços são restritos. Esta funcionalidade aumenta a capacidade da inspeção do aplicativo existente de controlar o tráfego de aplicativo de Instant Messenger (IM) que foi disfarçado porque tráfego HTTP (Web). Refira o Firewall do aplicativo - Aplicação imediata do tráfego de mensagem para mais informação.

Nota: Se um aplicativo IM é obstruído, a conexão está restaurada e um mensagem do syslog é gerado, como apropriado.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- mostre a IP o pdlm nbar — A fim indicar o PDLM no uso pelo NBAR, use o **comando show ip nbar pdlm no** modo de 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
```

- mostre a IP a versão nbar — O Exibir informação sobre a versão do software NBAR em seu Cisco IOS Release ou a versão de um NBAR PDLM em seu roteador do Cisco IOS, usa o **comando version nbar da mostra IP no** modo de 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>}
```

- mostre a relação do mapa de política — A fim indicar as estatísticas de pacote de todas as classes que são configuradas para todas as políticas de serviços na interface especificada ou na subinterface ou em uns Circuitos Virtuais Permanentes (PVC) específicos na relação, use o **comando show policy-map interface no** modo de 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
```

- **mostre o mapa de política da executar-configuração** — A fim indicar todas as configurações de mapa de política assim como configuração de mapa da política padrão, use o **comando policy-map da executar-configuração da mostra**:`R1#show running-config policy-map`

```
Building configuration...

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

```
!
end
```

- **mostre o mapa de classe da executar-configuração** — A fim indicar a informação sobre a configuração de mapa da classe, use o **comando class-map da executar-configuração da mostra**:`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

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **lista de acesso da mostra** — A fim indicar a configuração do accesslist que é executado no roteador do Cisco IOS, use o **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
```

Informações Relacionadas

- Manual de configuração do Cisco IOS Security, liberação 12.4-Support
- Network Based Application Recognition (NBAR)
- Cisco Express Forwarding (CEF)
- Suporte Técnico e Documentação - Cisco Systems