Security Device Manager : Exemple de configuration du blocage du trafic P2P sur un routeur Cisco IOS à l'aide de NBAR

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Aperçu de Reconnaissance d'application fondée sur le réseau (NBAR)
Configurez le blocage peer-to-peer du trafic (de P2P)
Diagramme du réseau
Configuration du routeur
Configurez le routeur avec SDM
Configuration SDM du routeur
Pare-feu d'application — Caractéristique instantanée d'application de trafic téléphonique dans des versions 12.4(4)T et ultérieures de Cisco IOS
Application de trafic téléphonique d'instant message
Stratégie d'application d'Instant Messenger
Vérifiez
Dépannez
Informations connexes

Introduction

Ce document décrit comment configurer le routeur de Cisco IOS® pour bloquer le trafic peer-to-peer (de P2P) du réseau intérieur à l'Internet utilisant le Reconnaissance d'application fondée sur le réseau (NBAR).

NBAR identifie les protocoles réseau et les applications réseau spécifiques qui sont utilisés dans votre réseau. Une fois qu'un protocole ou une application est identifié par NBAR, vous pouvez employer l'interface de ligne de commande de qualité de service modulaire (MQC) pour grouper les paquets associés avec ces protocoles ou applications dans des classes. Ces classes sont groupées sur la base de si les paquets se conforment à certains critères.

Pour NBAR, le critère est si le paquet apparie un protocole ou une application spécifique connue de NBAR. Utilisant le MQC, le trafic réseau avec un protocole réseau (Citrix, par exemple) peut être placé dans une classe du trafic, alors que le trafic qui apparie un protocole réseau différent (gnutella, par exemple) peut être placé dans une autre classe du trafic. Plus tard, le trafic réseau dans chaque classe peut être donné le traitement approprié de QoS à l'aide d'une stratégie de

trafic (carte de stratégie). Référez-vous le trafic réseau de classification utilisant la section NBAR du *guide de configuration de solutions de Qualité de service Cisco IOS* pour plus d'informations sur NBAR.

Conditions préalables

Conditions requises

Avant que vous configuriez NBAR pour bloquer le trafic P2P, vous devez activer le Technologie Cisco Express Forwarding (CEF).

Employez l'**ip cef** en mode de configuration globale afin d'activer le CEF :

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

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur de Cisco 2801 avec la version de logiciel 12.4(15)T de Cisco IOS®
- Cisco Security Device Manager (SDM) version 2.5

Remarque: Consultez Configuration de routeur de base à l'aide de SDM afin de permettre la configuration du routeur par SDM.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Aperçu de Reconnaissance d'application fondée sur le réseau (NBAR)

Le Reconnaissance d'application fondée sur le réseau (NBAR) est une engine de classification qui identifie et classifie une grande variété de protocoles et d'applications. Quand NBAR identifie et classifie un protocole ou une application, le réseau peut être configuré pour appliquer le Qualité de service (QoS) approprié pour cette application ou pour trafiquer avec ce protocole.

NBAR remplit ces fonctions :

- **Identification des applications et des protocoles (couche 4 pour poser 7)**NBAR peut classifier les applications qui les utilisent :Numéros de port statiquement assignés de Control Protocol (TCP) et de Protocole UDP (User Datagram Protocol) de transfert.Protocoles de Non-UDP et IP de non-tcp.Numéros de port dynamiquement assignés de TCP et UDP négociés pendant

l'établissement de la connexion. L'inspection avec état est exigée pour la classification des applications et des protocoles. L'inspection avec état est la capacité de découvrir les connexions de données qui seront classifiées en passant les connexions de contrôle au-dessus du port de connexion de données où des affectations sont faites.Classification de port secondaire : Classification de HTTP (URLs, pantomime ou noms d'hôte) et d'indépendant d'applications de Citrix calculant le trafic de l'architecture (AIC) basé sur le nom d'application édité.Classification basée sur l'inspection profonde de paquet et les plusieurs attributs spécifiques à l'application. La classification de charge utile de Protocole RTP (Real-Time Transport Protocol) est basée sur cet algorithme dans lequel le paquet est classifié comme RTP basé sur de plusieurs attributs dans l'en-tête de RTP.

- **Détection de Protocol**La détection de Protocol est une caractéristique utilisée généralement NBAR qui recueille des statistiques d'application et de protocole (comptes de paquet, nombres d'octets, et débits binaires) par interface. Les outils de gestion basés par GUI peuvent graphiquement afficher ces informations, en votant des statistiques SNMP du Management Information Base palladium NBAR (MIB). Comme avec n'importe quelle configuration de réseau, il est important de comprendre les caractéristiques de performance et évolutivité avant de déployer la caractéristique dans un réseau de production. Sur les Plateformes articulées autour d'un logiciel, les mesures qui sont considérées sont incidence d'utilisation du processeur et le débit de données viable tandis que cette caractéristique est activée. Afin de configurer NBAR pour découvrir le trafic pour tous les protocoles qui sont connus à NBAR sur une interface spécifique, utilisez la commande d'**ip nbar protocol-discovery** dans le mode de configuration d'interface ou le mode de configuration VLAN. Afin de désactiver la détection du trafic, n'utilisez l'**aucune** commande d'**ip nbar protocol-discovery**.

Configurez le blocage peer-to-peer du trafic (de P2P)

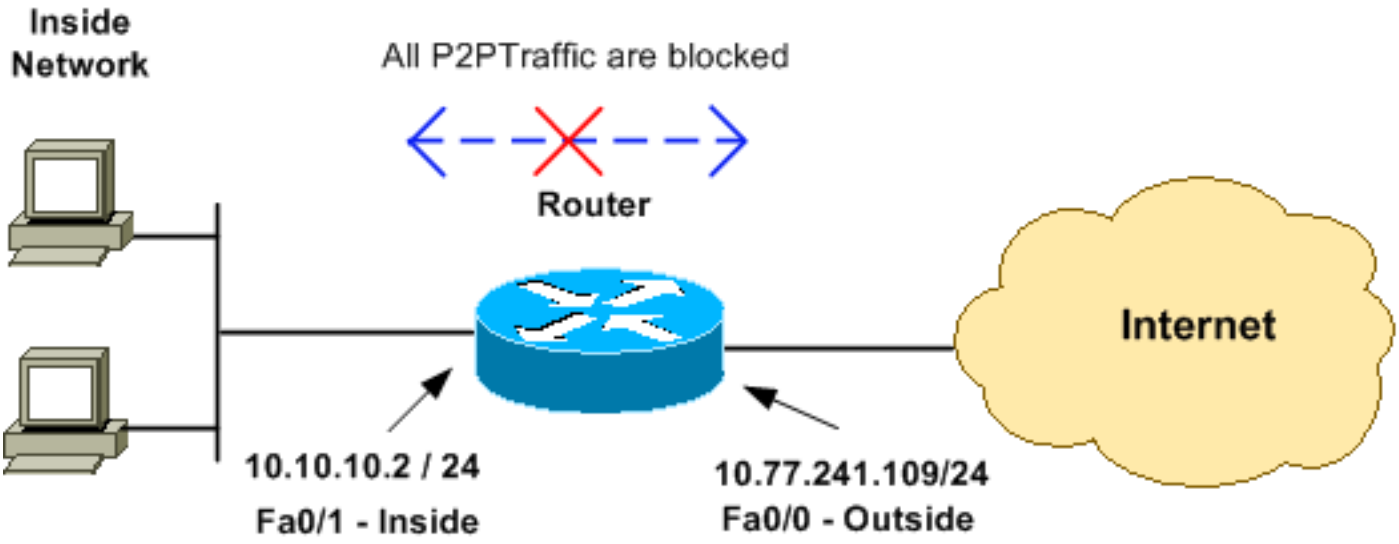
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Du trafic P2P ne peut pas être dû complètement bloqué à la nature de son protocole de P2P. Ces protocoles de P2P changent dynamiquement leurs signatures pour sauter toutes les engines DPI qui essayent de bloquer complètement leur trafic. Par conséquent, Cisco recommande que vous limitiez la bande passante au lieu de les bloquer complètement. (Étranglez la bande passante pour ce trafic. Donnez très moins de bande passante ; cependant, permettez la connexion d'intervenir.)

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configuration du routeur

Configuration pour bloquer le trafic P2P sur le routeur 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
```

Configurez le routeur avec SDM

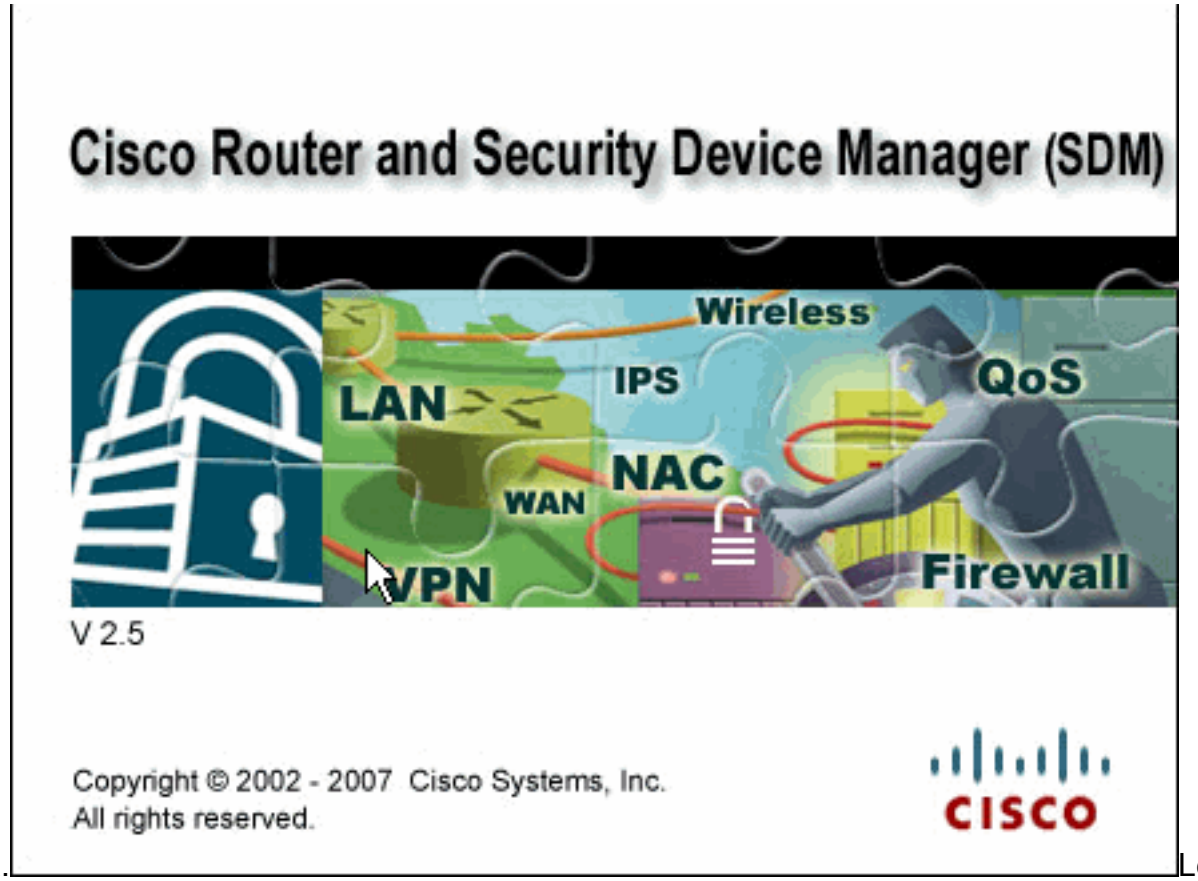
Configuration SDM du routeur

Terminez-vous ces étapes afin de configurer le blocage du trafic P2P sur un routeur Cisco IOS :

Remarque: Afin de configurer NBAR pour découvrir le trafic pour tous les protocoles qui sont connus à NBAR sur une interface spécifique, la commande d'ip nbar protocol-discovery devrait être utilisée dans le mode de configuration d'interface ou le mode de configuration VLAN pour activer la détection du trafic. Procédez à la configuration SDM après avoir configuré la détection de protocole sur l'interface requise où la stratégie QoS configurée est utilisée.

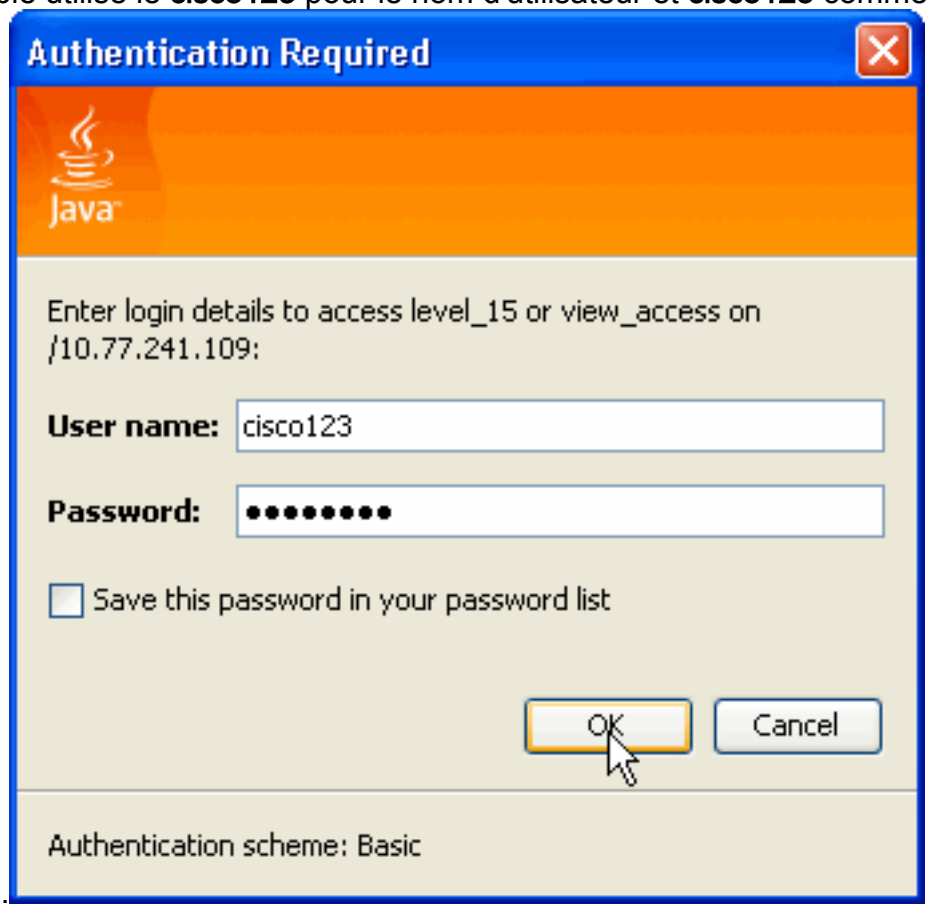
```
Hostname#config t
              Hostname(config)#interface fastEthernet 0/1
              Hostname(config-if)#ip nbar protocol-discovery
              Hostname(config-if)#end
```

1. Ouvrez un navigateur, et écrivez l'adresse IP du routeur qui a été configuré pour l'accès SDM. Par exemple, **<SDM_Router_IP_Address de https:// >**Veillez à autoriser tous les avertissements que votre navigateur vous donne lié à l'authenticité de certificat ssl. Le nom d'utilisateur et le mot de passe par défaut sont deux blanc.Le routeur affiche cette fenêtre pour permettre le téléchargement de l'application SDM. Cet exemple charge l'application sur l'ordinateur local et ne fonctionne pas dans une applet



Java.Le téléchargement de SDM commence alors.

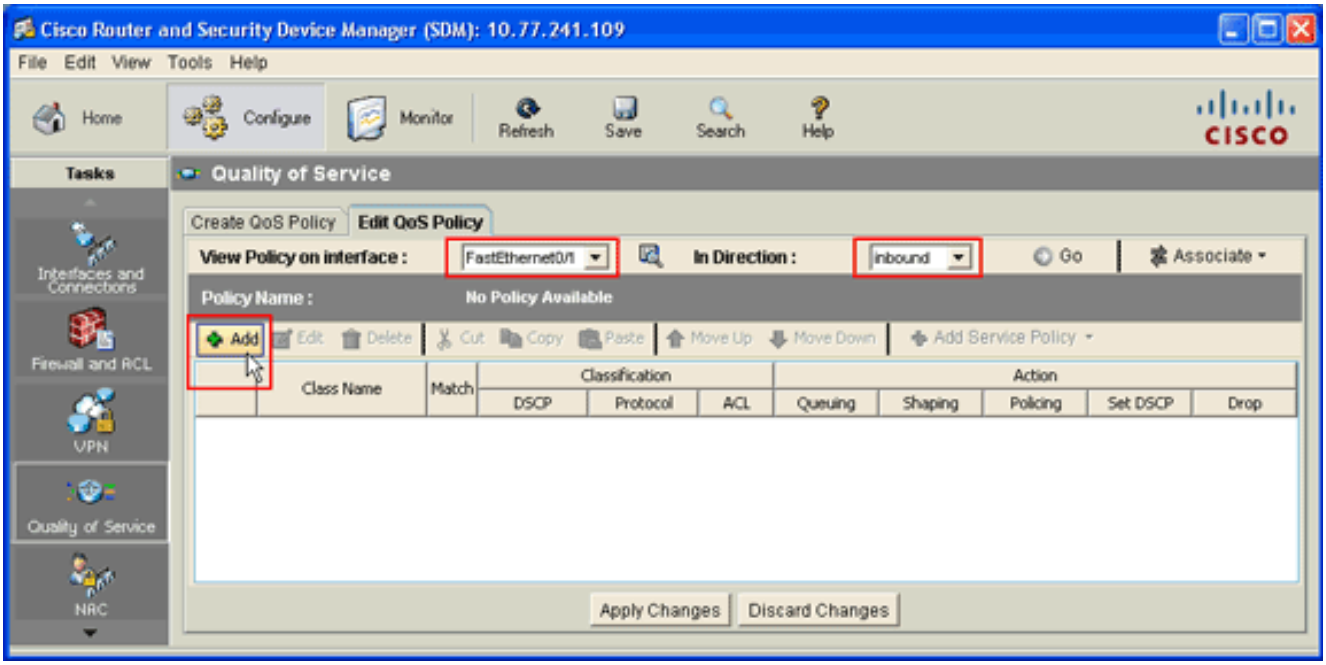
2. Une fois le lanceur de SDM téléchargé, exécutez les étapes stipulées par les invites afin d'installer le logiciel et d'exécuter le lanceur de Cisco SDM.
3. Entrez un nom d'utilisateur et un mot de passe, si vous spécifiiez un, et cliquez sur OK.Cet exemple utilise le **cisco123** pour le nom d'utilisateur et **cisco123** comme mot de



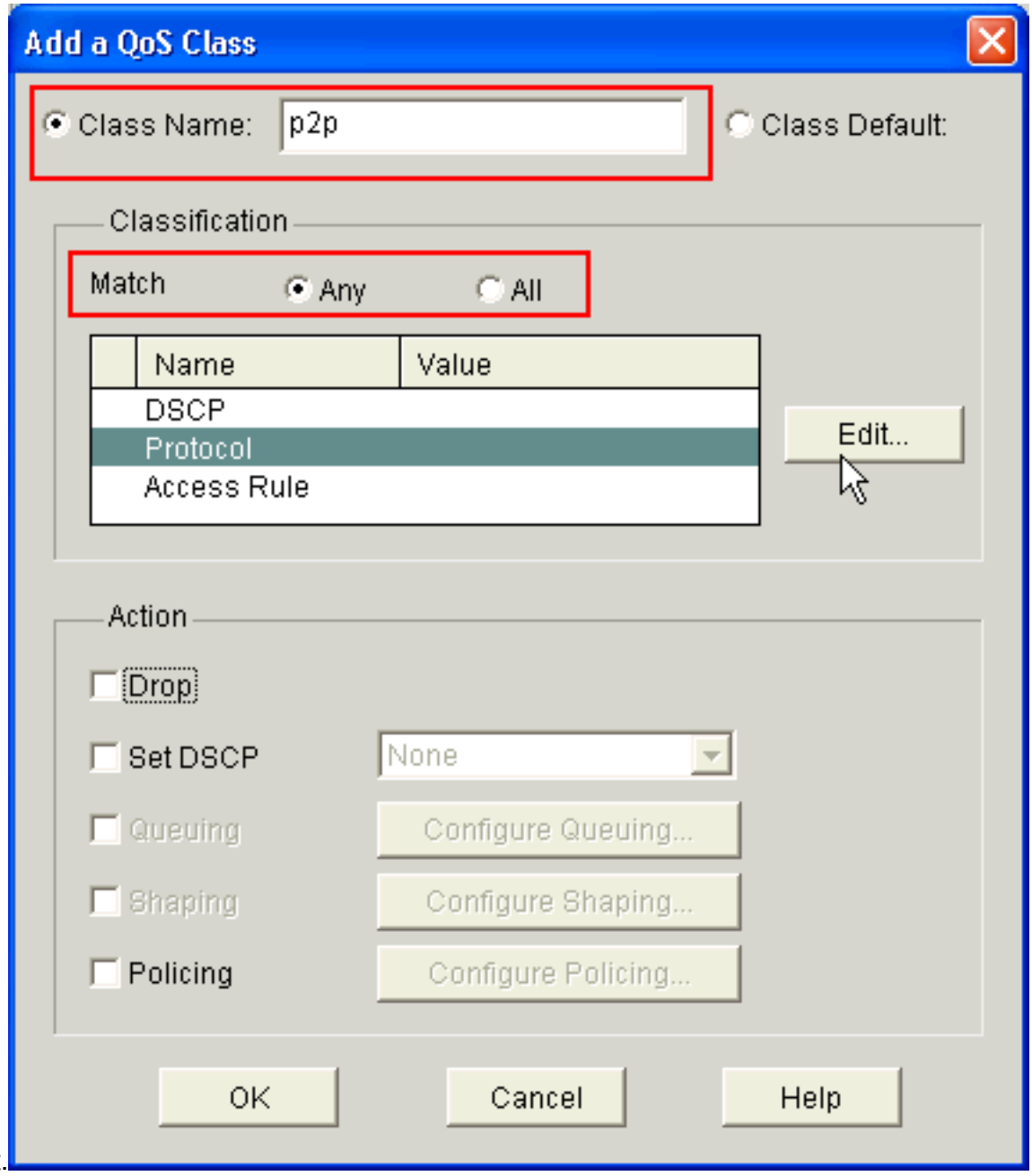
passe.

4. Choisissez **configurent > qualité de service**, et cliquent sur l'onglet de **stratégie QoS d'éditer**

sur la page d'accueil
SDM.

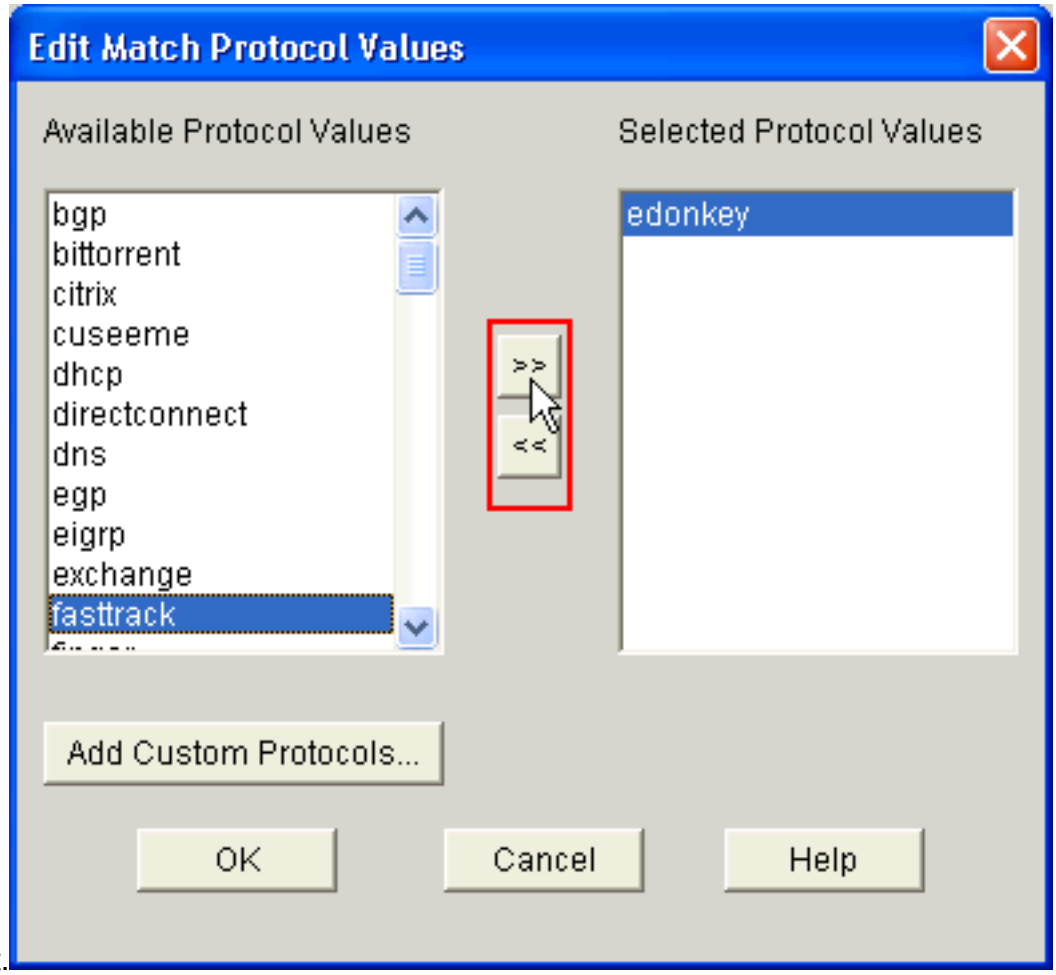


5. De la stratégie de vue sur la liste déroulante d'interface, choisissez le nom d'interface, et puis choisissez la direction de la circulation (d'arrivée ou sortant) du dans la liste déroulante de direction.Dans cet exemple, l'interface est *FastEthernet 0/1*, et la direction est *d'arrivée*.
6. Cliquez sur Add afin d'ajouter une nouvelle classe de QoS pour l'interface.L'ajouter une boîte de dialogue de classe de QoS



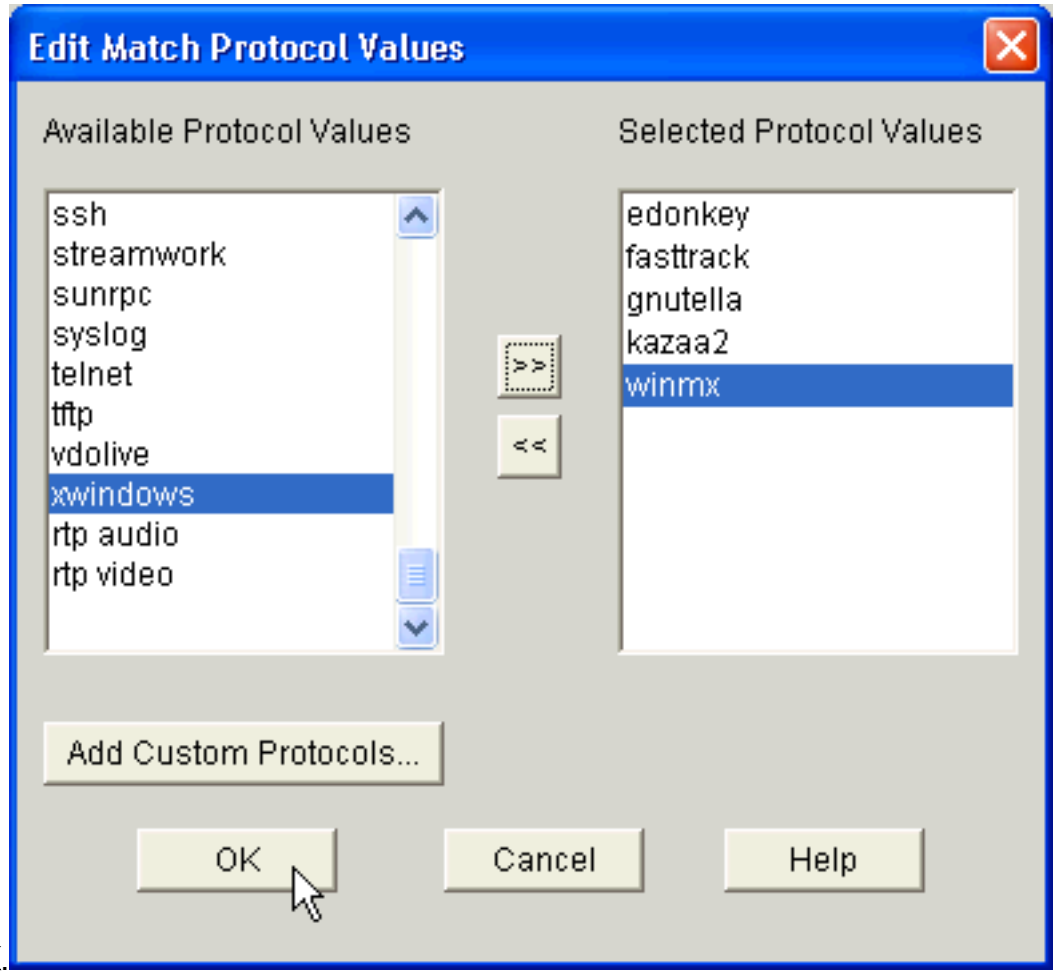
apparaît.

7. Si vous voulez créer une nouvelle classe, cliquer sur la case d'option de **nom de classe**, et écrire un nom pour votre classe. Autrement, cliquez sur la case d'option de **par défaut de classe** si vous voulez utiliser la classe par défaut.Cet exemple crée une nouvelle classe nommée *p2p*.
8. Dans la région de classification, cliquez sur la **n'importe quelle** case d'option ou la **toute la** case d'option pour l'option de correspondance.Ce les exemples utilise la *n'importe quelle* option de correspondance, qui exécute la commande de [p2p de match any de class-map](#) sur le routeur.
9. **Protocol** choisi dans la liste de Classifcation, et cliquent sur Edit afin d'éditer le paramètre du protocole.La boîte de dialogue de valeurs de match protocol d'éditer

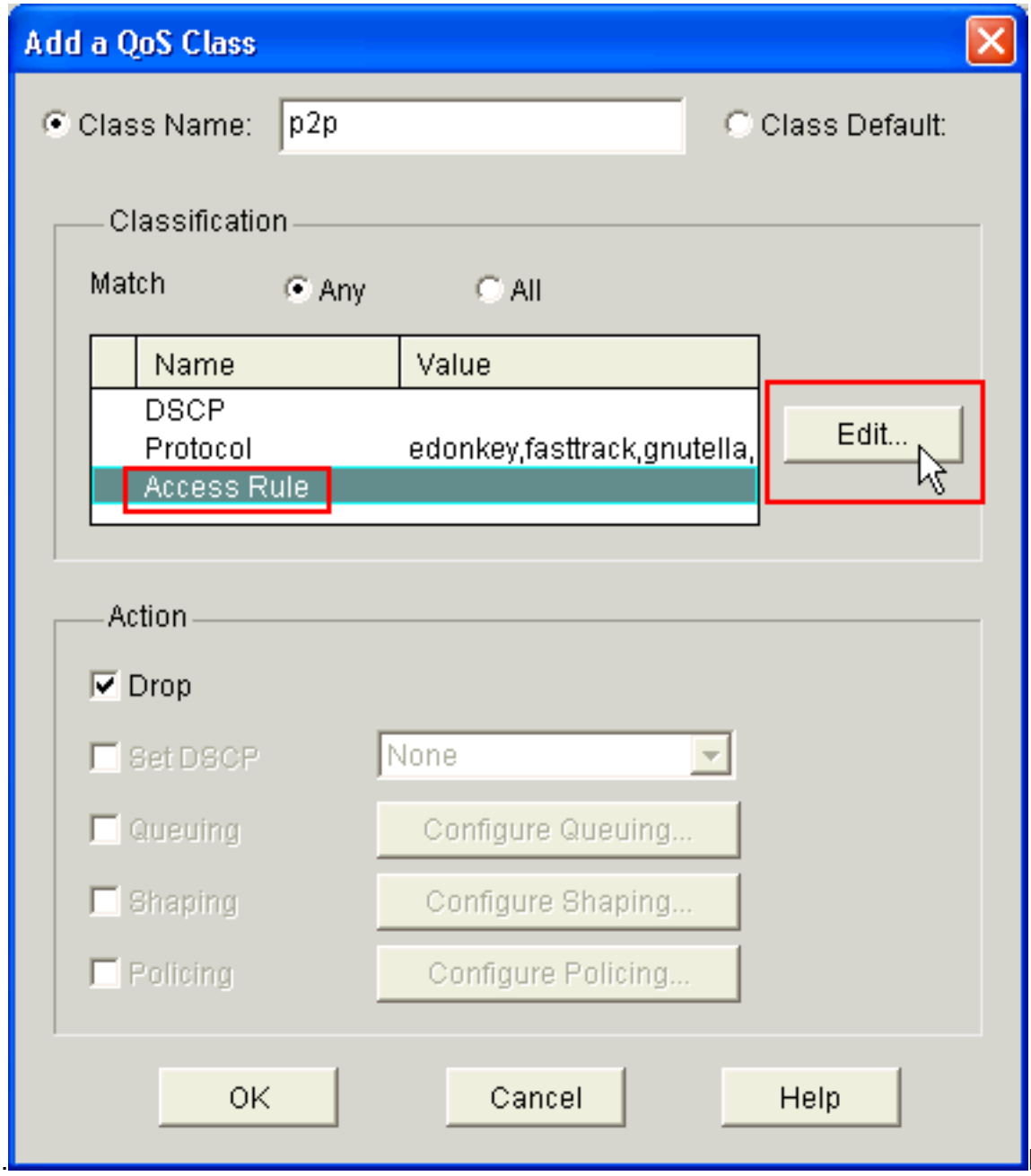


apparaît.

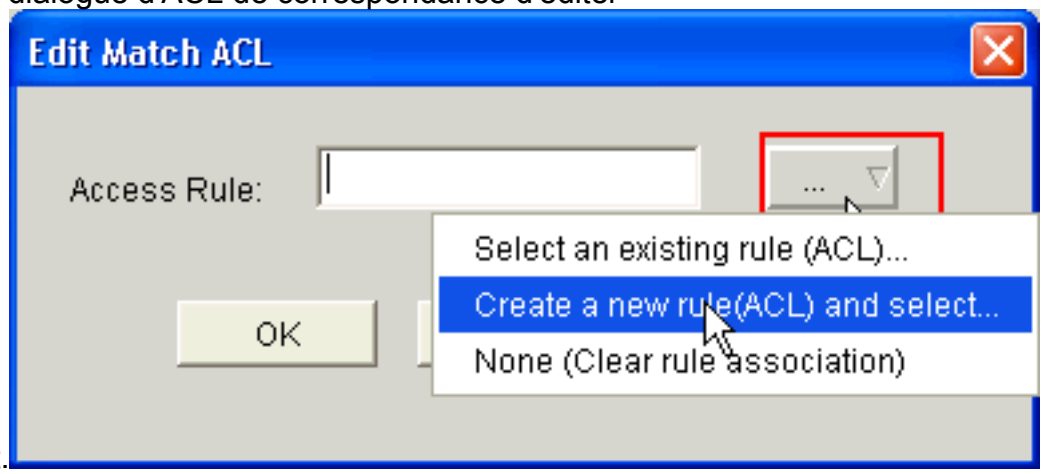
10. De la liste de valeurs disponible de Protocol, sélectionnez chaque protocole de P2P que vous voulez bloquer, et cliquez sur le bouton de flèche à droite (**>>**) pour déplacer chaque protocole à la liste de valeurs sélectionnée de Protocol.**Remarque:** Afin de classifier le trafic P2P avec NBAR, allez à la page de téléchargement du logiciel, et téléchargez le plus défunts logiciel et fichiers readmes du module de langage de description de Protocol de P2P (PDLM). Le P2P PDLMs disponible pour le téléchargement incluent WinMx, Bittorrent, Kazaa2, Gnutella, eDonkey, promotion accélérée, et Napster. Selon votre IOS, vous ne pourriez pas avoir besoin des dernières versions PDLM puisque certains pourraient être intégrés dans votre IOS (par exemple, promotion accélérée et Napster). Une fois que téléchargé, copiez le PDLMs sur l'éclair du routeur, et chargez-les dans l'IOS en configurant le **<flash_device d'ip nbar pdlm > : <filename >.pdlm**. Émettez la commande de **show ip nbar pdlm** afin de s'assurer qu'elle a été chargée avec succès. Une fois que chargé, vous pouvez les utiliser dans les déclarations de match protocol sous votre configuration de class map.



11. Cliquez sur **OK**.
12. Dans l'ajouter une boîte de dialogue de classe de QoS, des **règles d'accès** choisies de la liste de classification, et cliquent sur Edit afin de créer une nouvelle règle d'accès. Vous pouvez également tracer une règle d'accès existante au class map de

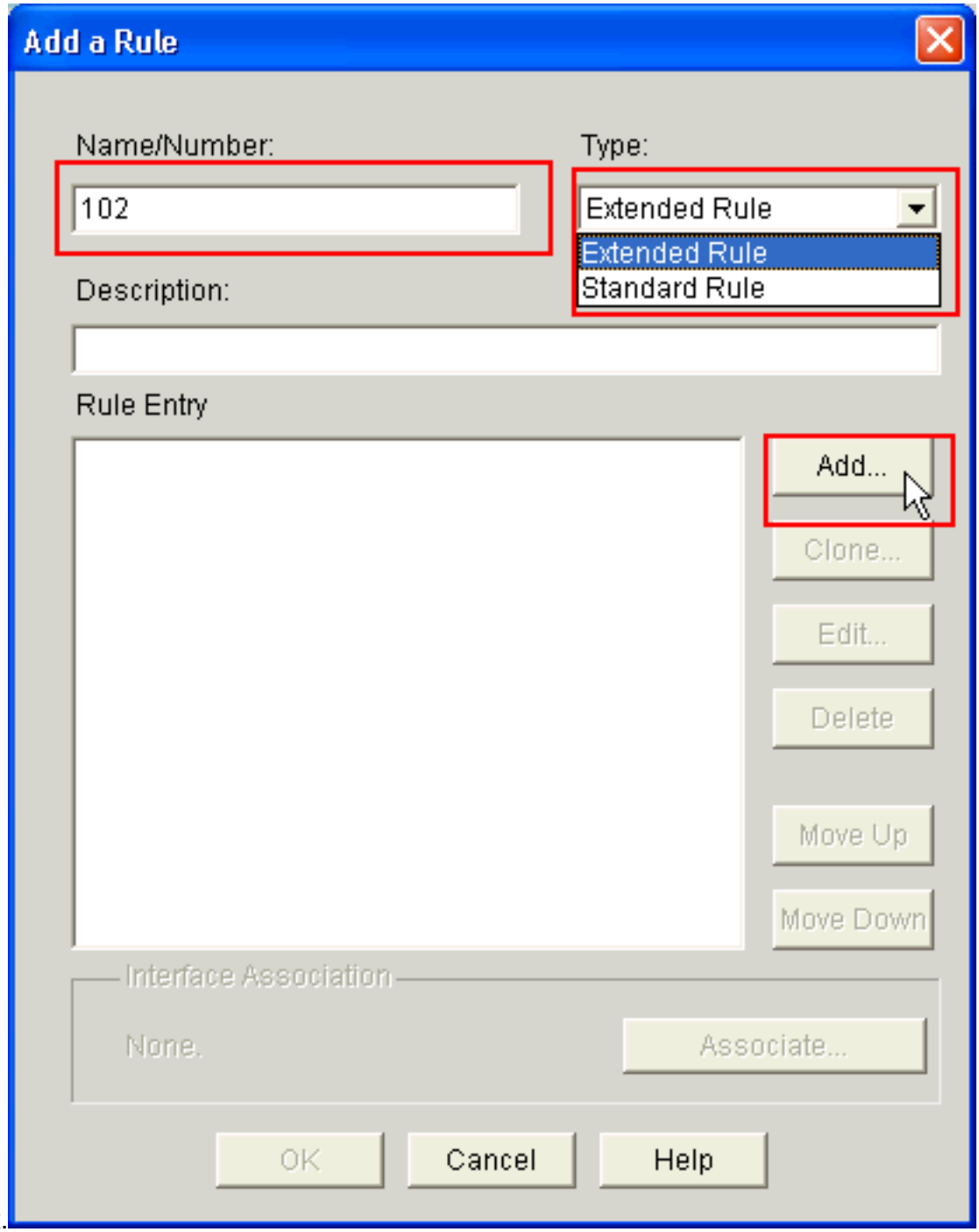


p2p.La boîte de dialogue d'ACL de correspondance d'éditer



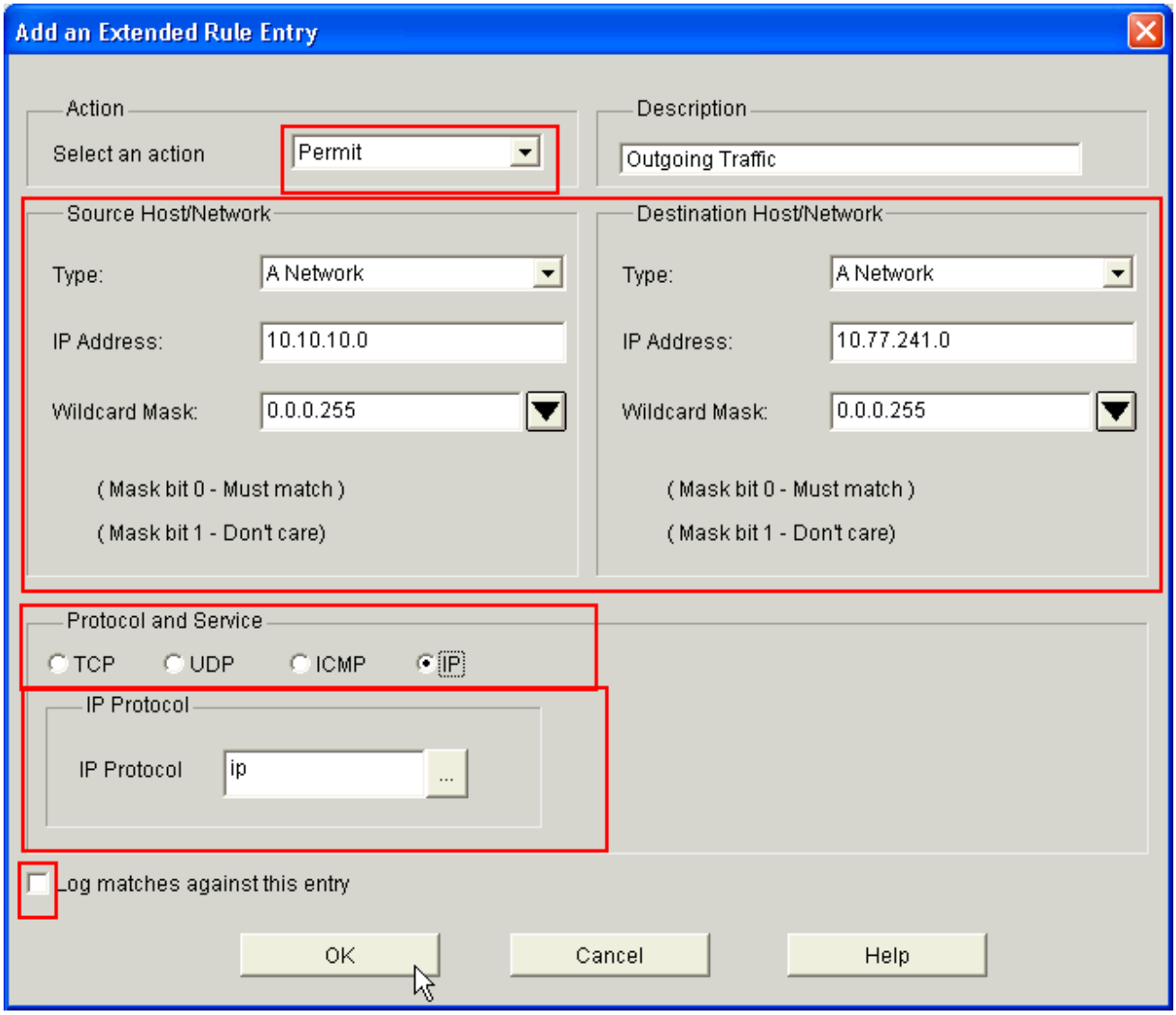
apparaît.

13. Cliquez sur le bouton de règle d'accès (**...**), et choisissez l'option appropriée. Cet exemple crée un nouvel ACL.L'ajouter une boîte de dialogue de règle

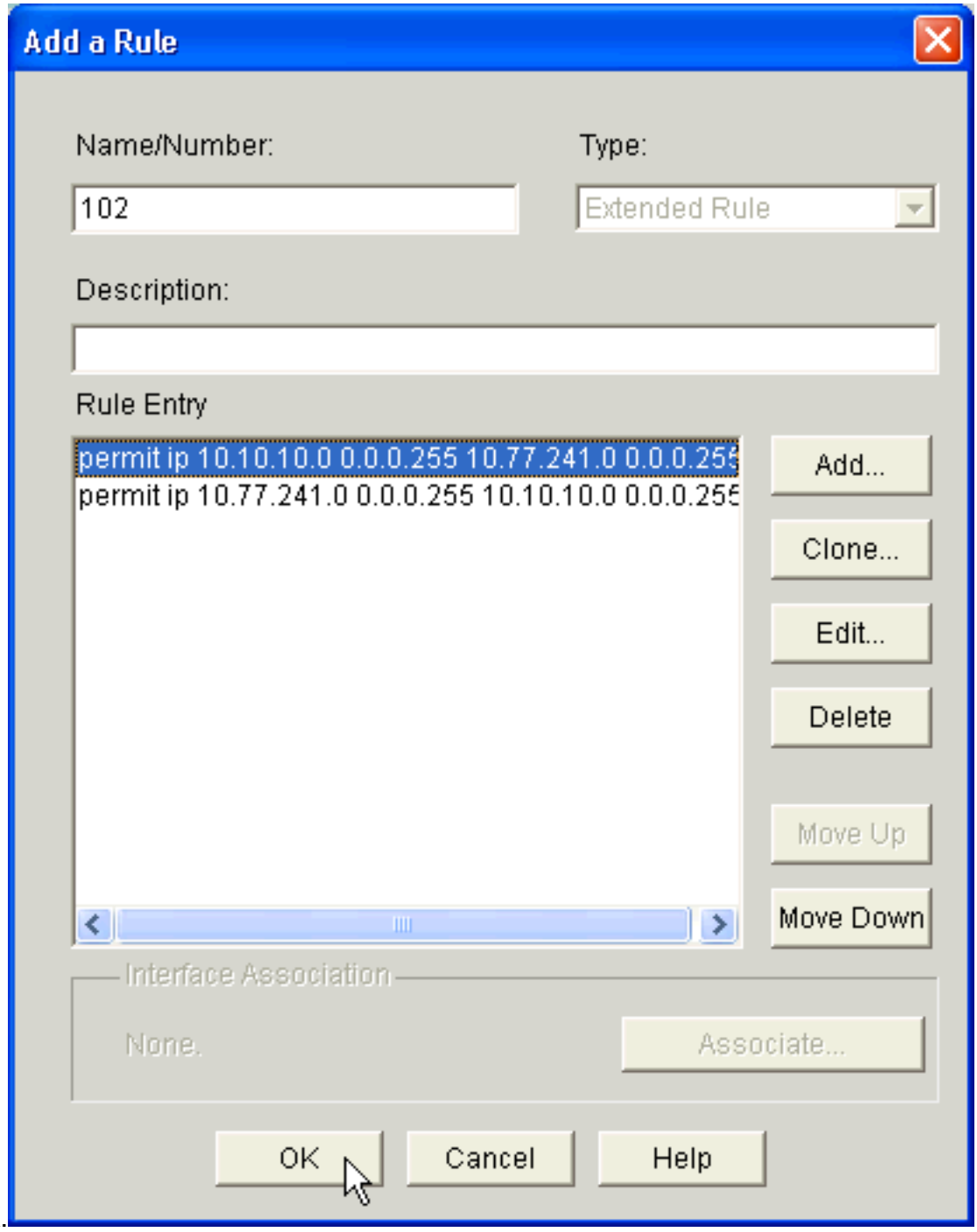


apparaît.

14. Dans l'ajouter une boîte de dialogue de règle, entrent dans le nom ou le nombre de l'ACL à créer dans le domaine de nom/numéro de l'ACL.
15. De la liste déroulante de type, choisissez le type d'ACL à créer (*règle étendue* ou *règle standard*).
16. Cliquez sur Add afin d'ajouter des détails à l'ACL *102*.L'ajouter une boîte de dialogue étendue d'entrée de règle
    apparaît.

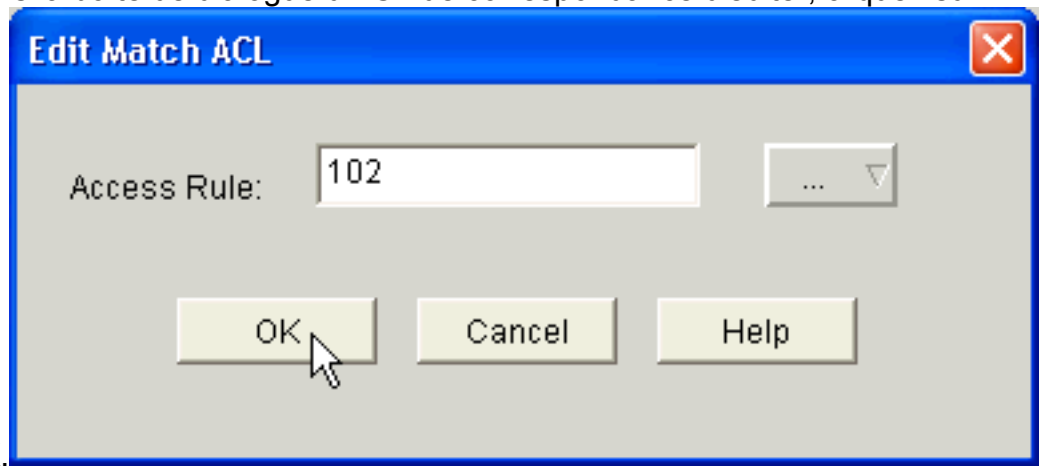


17. Dans l'ajouter une boîte de dialogue étendue d'entrée de règle, choisissent une action (ou l'*autorisation* ou *refusent*) du choisi une liste déroulante d'action qui indique si la règle d'ACL devrait permettre ou refuser le trafic entre la source et les réseaux de destination. Cette règle est pour le trafic sortant du réseau intérieur au réseau extérieur.
18. Entrez dans les informations pour la source et les réseaux de destination dans les régions de Source Host/Network et de destination host/réseau respectivement.
19. Dans Protocol et la zone de service, cliquez sur la case d'option appropriée. Cet exemple utilise l'IP.
20. Si vous voulez se connecter les paquets assortis contre cet ACL ordonnent, cochent les **correspondances de log contre cette** case d'**entrée**.
21. Cliquez sur **OK**.
22. Dans l'ajouter une boîte de dialogue de règle, cliquent sur



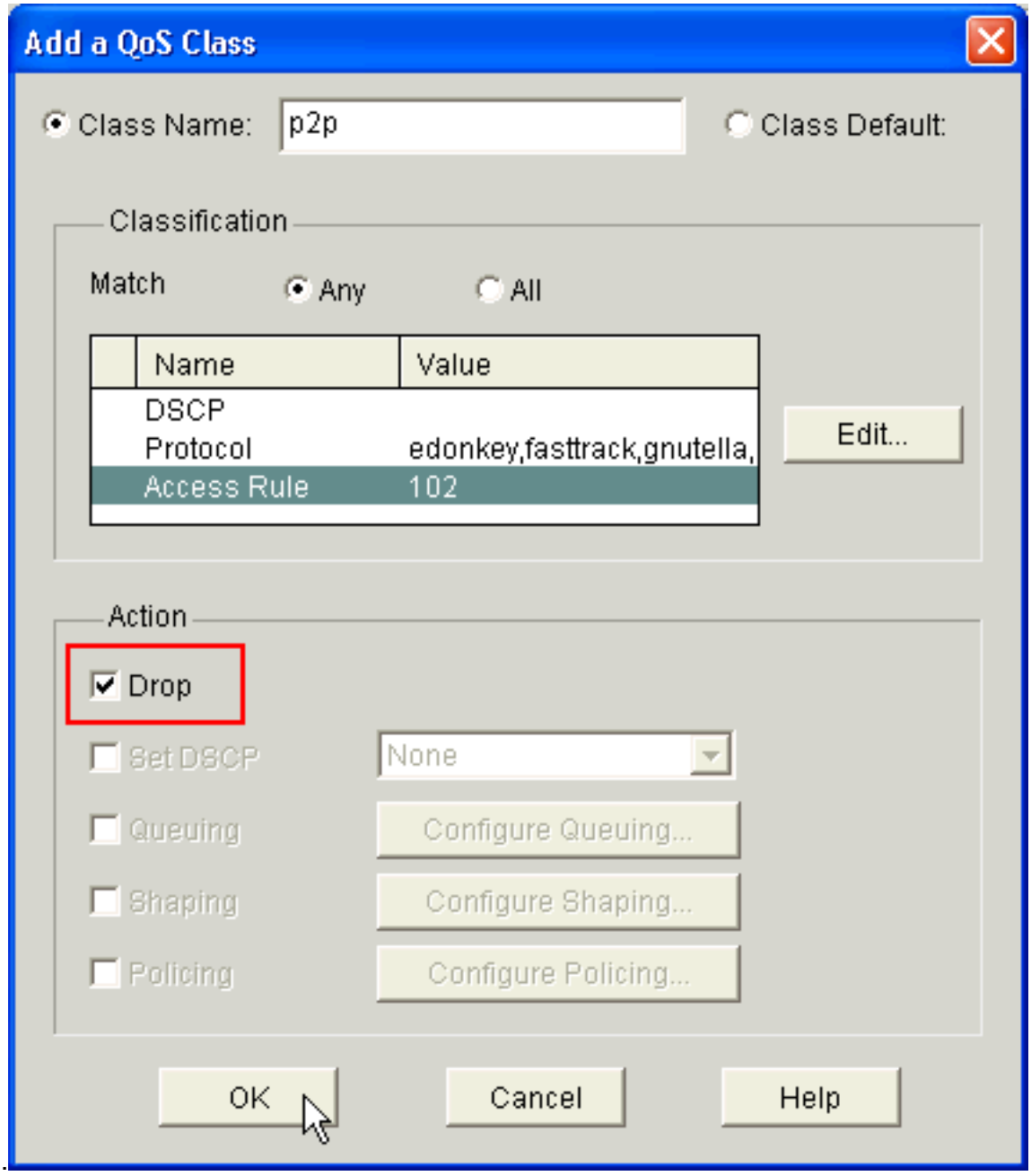
OK.

23. Dans la boîte de dialogue d'ACL de correspondance d'éditer, cliquez sur



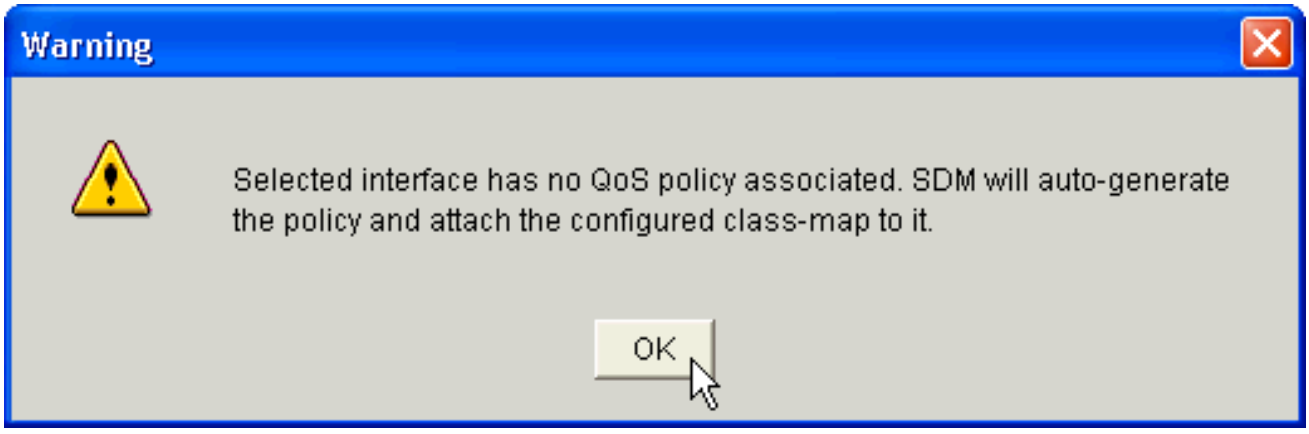
OK.

24. Dans l'ajouter une boîte de dialogue de classe de QoS, cochent la case de **baisse** afin de forcer le routeur pour bloquer le trafic



P2P.

25. Cliquez sur **OK**.Le message d'avertissement suivant est affiché par défaut car aucune stratégie QoS n'est tracée à l'interface.

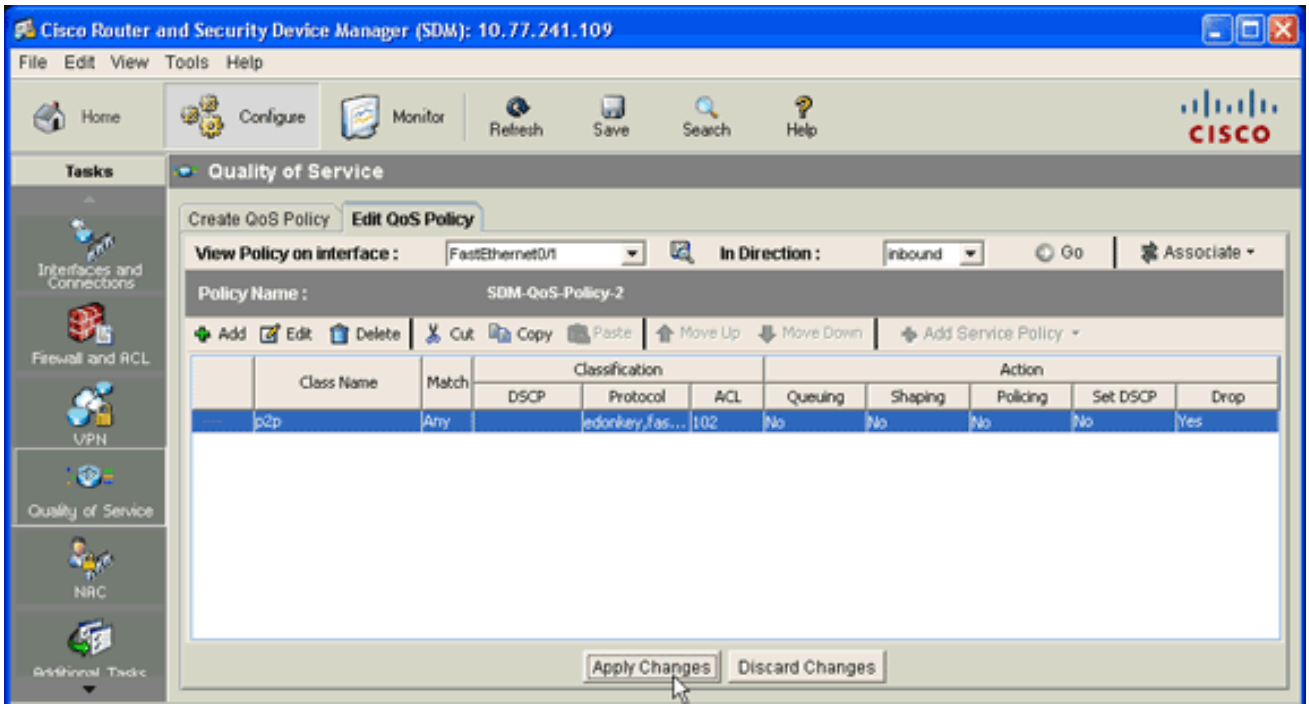


SDM automatique-génèrera la stratégie QoS et reliera le class map configuré à la stratégie. L'équivalent de l'interface de ligne de commande (CLI) de cette étape de configuration SDM est :

```
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. Sur l'onglet de stratégie QoS d'éditer, cliquez sur Apply les **modifications** afin de fournir la configuration au routeur.



Pare-feu d'application — Caractéristique instantanée d'application de trafic téléphonique dans des versions 12.4(4)T et ultérieures de Cisco IOS

Application de trafic téléphonique d'instant message

Le pare-feu d'application — La caractéristique d'application de trafic téléphonique d'instant message permet à des utilisateurs de définir et imposer une stratégie qui spécifie que des types de trafic de messagerie instantanée sont permis dans le réseau. Vous pouvez contrôler de plusieurs messengers (à savoir AOL, YAHOO, et MSN) simultanément une fois configuré dans la **stratégie d'appfw** sous l'**application im**. Par conséquent, la fonctionnalité supplémentaire suivante peut également être imposée :

- Configuration des règles d'inspection de Pare-feu
- Inspection profonde de paquet de la charge utile (recherchant des services tels que la conversation textuelle)

Remarque: La caractéristique d'application de trafic téléphonique de Pare-feu-instant d'application est prise en charge dans des versions 12.4(4)T et ultérieures de Cisco IOS.

Stratégie d'application d'Instant Messenger

Le pare-feu d'application emploie une stratégie d'application, qui se compose d'une collection de signatures statiques, pour détecter des violations de sécurité. Une signature statique est une collection de paramètres qui spécifient les conditions de protocole qui doivent être remplies avant qu'une mesure soit prise. Ces états et réactions de protocole sont définis par l'utilisateur final par

l'intermédiaire du CLI pour former une stratégie d'application.

Le pare-feu d'application de Cisco IOS a été amélioré pour prendre en charge des stratégies indigènes instantanées d'application de messenger. Ainsi, le Pare-feu Cisco IOS peut maintenant détecter et interdire des connexions utilisateur aux serveurs de messagerie instantanée pour AOL Instant Messenger (AIM), Yahoo! Services de messagerie instantanée de messenger, et de MSN Messenger. Cette fonctionnalité contrôle toutes les connexions pour des services pris en charge, y compris le texte, la Voix, le vidéo, et les capacités de transfert de fichier. On peut être individuellement refusé ou permis les trois applications. Chaque service peut être individuellement contrôlé de sorte qu'on permette le service de texte-dialogue, et la Voix, le transfert de fichiers, le vidéo, et d'autres services sont limités. Cette fonctionnalité augmente la capacité d'inspection d'application existante pour contrôler le trafic de l'application de messagerie instantanée (IM) qui a été déguisé car le trafic de HTTP (Web). Référez-vous au pare-feu d'application - Pour en savoir plus d'application de trafic téléphonique d'instant message.

Remarque: Si une application IM est bloquée, la connexion est remise à l'état initial et un message de Syslog est généré, comme approprié.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- show ip nbar pdlm — Afin d'afficher le PDLM en service par NBAR, utilisez la commande de **show ip nbar pdlm** dans le mode d'exécution privilégié :`Router#show ip nbar pdlm`

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

- show ip nbar version — Afin d'afficher des informations sur la version du logiciel NBAR dans votre Cisco IOS libérez ou la version d'un NBAR PDLM sur votre routeur Cisco IOS, utilisent la commande de **show ip nbar version** dans le mode d'exécution privilégié :`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 — Afin d'afficher les statistiques de paquet de toutes les classes qui sont configurées pour toutes les stratégies de service sur l'interface spécifiée ou la sous-interface ou sur un circuit virtuel permanent spécifique (PVC) sur l'interface, utilisez la commande de **show policy-map interface** dans le mode d'exécution privilégié :`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
```

- **policy-map de show running-config** — Afin d'afficher tous les configuration de policy-map aussi bien que stratégie par défaut tracez la configuration, utilisent la commande de **policy-map de show running-config** :`R1#show running-config policy-map`

```
Building configuration...

Current configuration : 57 bytes
```

```
!
policy-map SDM-QoS-Policy-2
 class p2p
   drop
!
end
```

- **class-map de show running-config** — Afin d'afficher les informations sur la configuration de class map, utilisez la commande de **class-map de show running-config** :`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
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **liste d'accès d'exposition** — Afin d'afficher la configuration d'accesslist qui fonctionne sur le routeur Cisco IOS, utilisez la **commande access-list d'exposition** :`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
```

Informations connexes

- Guide de configuration de Cisco IOS Security, version 12.4-Support
- Reconnaissance d'application fondée sur le réseau (NBAR)
- Cisco Express Forwarding (CEF)
- Support et documentation techniques - Cisco Systems