

Security Device Manager: Blockieren des P2P-Datenverkehrs auf einem Cisco IOS-Router mithilfe des NBAR-Konfigurationsbeispiels

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Network Based Application Recognition \(NBAR\) - Übersicht](#)

[Konfigurieren der P2P-Datenverkehrsblockierung \(Peer-to-Peer\)](#)

[Netzwerkdiagramm](#)

[Routerkonfiguration](#)

[Konfigurieren des Routers mit SDM](#)

[Router-SDM-Konfiguration](#)

[Anwendungs-Firewall - Funktion zur Instant Message Traffic Enforcement in Cisco IOS Version 12.4\(4\)T und höher](#)

[Durchsetzung von Instant Message-Datenverkehr](#)

[Instant Messenger-Anwendungsrichtlinie](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie der Cisco IOS[®]-Router so konfiguriert wird, dass der Peer-to-Peer (P2P)-Datenverkehr vom internen Netzwerk zum Internet mithilfe der Network Based Application Recognition (NBAR) blockiert wird.

NBAR erkennt spezifische Netzwerkprotokolle und Netzwerkanwendungen, die in Ihrem Netzwerk verwendet werden. Nachdem ein Protokoll oder eine Anwendung von der NBAR erkannt wurde, können Sie mithilfe der Modular Quality of Service Command Line Interface (MQC) die mit diesen Protokollen oder Anwendungen verknüpften Pakete in Klassen gruppieren. Diese Klassen werden basierend darauf gruppiert, ob die Pakete bestimmten Kriterien entsprechen.

Für NBAR besteht das Kriterium darin, ob das Paket mit einem bestimmten, NBAR bekannten Protokoll oder einer bestimmten Anwendung übereinstimmt. Mit dem MQC kann Netzwerkverkehr mit einem Netzwerkprotokoll (z. B. Citrix) in eine Datenverkehrsklasse unterteilt werden, während Datenverkehr, der einem anderen Netzwerkprotokoll (z. B. gnutella) entspricht, in eine andere Datenverkehrsklasse platziert werden kann. Später kann der Netzwerkverkehr innerhalb jeder

Klasse mithilfe einer Datenverkehrsrichtlinie (Richtlinienzuordnung) die entsprechende QoS-Behandlung erhalten. Weitere Informationen zu NBAR finden Sie im Abschnitt [Klassifizierung von Netzwerkverkehr mit NBAR](#) im *Konfigurationshandbuch zu Quality of Service-Lösungen von Cisco IOS*.

Voraussetzungen

Anforderungen

Bevor Sie NBAR so konfigurieren, dass P2P-Datenverkehr blockiert wird, müssen Sie Cisco Express Forwarding (CEF) aktivieren.

Verwenden Sie `ip cef` im globalen Konfigurationsmodus, um CEF zu aktivieren:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Router der Serie 2801 mit Cisco IOS[®] Softwareversion 12.4(15)T
- Cisco Security Device Manager (SDM) Version 2.5

Hinweis: Informationen zur Konfiguration des Routers mithilfe von SDM finden Sie unter [Basic Router Configuration](#) (Basiskonfiguration des Routers).

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Network Based Application Recognition (NBAR) - Übersicht

Network-Based Application Recognition (NBAR) ist eine Klassifizierungs-Engine, die eine Vielzahl von Protokollen und Anwendungen erkennt und klassifiziert. Wenn NBAR ein Protokoll oder eine Anwendung erkennt und klassifiziert, kann das Netzwerk so konfiguriert werden, dass die entsprechende Quality of Service (QoS) für die Anwendung oder den Datenverkehr mit diesem Protokoll angewendet wird.

NBAR führt diese Funktionen aus:

- **Identifikation von Anwendungen und Protokollen (Layer 4 bis Layer 7)**NBAR kann Anwendungen klassifizieren, die Folgendes verwenden: Statisch zugewiesene Portnummern

Transfer Control Protocol (TCP) und User Datagram Protocol (UDP). Nicht-UDP- und Nicht-TCP-IP-Protokolle. Dynamisch zugewiesene TCP- und UDP-Portnummern, die während der Verbindungsherstellung ausgehandelt werden. Für die Klassifizierung von Anwendungen und Protokollen ist eine Stateful Inspection erforderlich. Stateful Inspection ist die Fähigkeit, Datenverbindungen zu erkennen, die durch Übergeben der Steuerungsverbindungen über den Datenverbindungsport klassifiziert werden, an dem Zuweisungen vorgenommen werden. Unterport-Klassifizierung: Klassifizierung von HTTP- (URLs, MIME- oder Hostnamen) und Citrix-Anwendungen ICA-Datenverkehr (Independent Computing Architecture) auf Basis des veröffentlichten Anwendungsnamens. Klassifizierung basierend auf Deep Packet Inspection und mehreren anwendungsspezifischen Attributen. Die RTP-Payload-Klassifizierung (Real-Time Transport Protocol) basiert auf diesem Algorithmus, bei dem das Paket anhand mehrerer Attribute im RTP-Header als RTP klassifiziert wird.

- **Protokollerkennung** Die Protokollerkennung ist eine häufig verwendete NBAR-Funktion, die Anwendungs- und Protokollstatistiken (Paketanzahl, Byteanzahl und Bitraten) pro Schnittstelle erfasst. GUI-basierte Verwaltungstools können diese Informationen grafisch anzeigen, indem SNMP-Statistiken von der NBAR PD Management Information Base (MIB) abgefragt werden. Wie bei allen Netzwerkfunktionen ist es wichtig, die Leistungs- und Skalierbarkeitsmerkmale zu kennen, bevor die Funktion in einem Produktionsnetzwerk bereitgestellt wird. Bei softwarebasierten Plattformen werden die Auswirkungen der CPU-Auslastung und die nachhaltige Datenrate bei Aktivierung dieser Funktion berücksichtigt. Um NBAR so zu konfigurieren, dass der Datenverkehr für alle Protokolle, die der NBAR auf einer bestimmten Schnittstelle bekannt sind, erkannt wird, verwenden Sie den **Befehl [ip nbar protocol discovery](#) im Schnittstellenkonfigurationsmodus oder im VLAN-Konfigurationsmodus**. Um die Datenverkehrserkennung zu deaktivieren, verwenden Sie den Befehl **`no ip nbar protocol discovery`**.

[Konfigurieren der P2P-Datenverkehrsblockierung \(Peer-to-Peer\)](#)

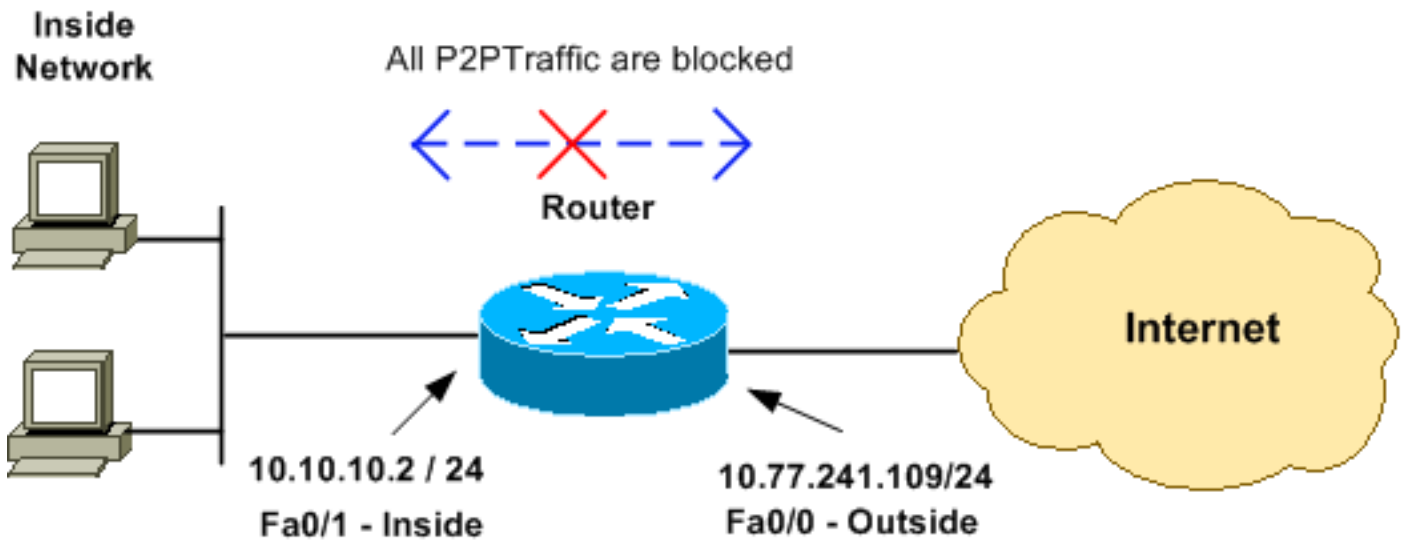
In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Ein Teil des P2P-Datenverkehrs kann aufgrund der Art seines P2P-Protokolls nicht vollständig blockiert werden. Diese P2P-Protokolle ändern dynamisch ihre Signaturen, um DPI-Engines zu umgehen, die versuchen, ihren Datenverkehr vollständig zu blockieren. Cisco empfiehlt daher, die Bandbreite zu begrenzen, anstatt sie vollständig zu blockieren. (Throttle the bandwidth for this traffic. Bieten Sie eine sehr geringe Bandbreite. Lassen Sie die Verbindung jedoch bestehen.)

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

[Netzwerkdiagramm](#)

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Routerkonfiguration

Konfiguration zur Blockierung des P2P-Datenverkehrs auf dem Cisco IOS-Router

```
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$AH0xTgk6d3hcMGn6jTGxs/
!
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
```

Konfigurieren des Routers mit SDM

Router-SDM-Konfiguration

Gehen Sie wie folgt vor, um die Blockierung von P2P-Datenverkehr auf einem Cisco IOS-Router zu konfigurieren:

Hinweis: Um NBAR so zu konfigurieren, dass der Datenverkehr für alle Protokolle erkannt wird, die NBAR auf einer bestimmten Schnittstelle bekannt sind, sollte der Befehl [ip nbar protocol discovery](#) im Schnittstellenkonfigurationsmodus oder im VLAN-Konfigurationsmodus verwendet werden, um die Datenverkehrserkennung zu aktivieren. Setzen Sie die SDM-Konfiguration fort, nachdem Sie die Protokollerkennung für die erforderliche Schnittstelle konfiguriert haben, für die die konfigurierte QoS-Richtlinie verwendet wird.

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

1. Öffnen Sie einen Browser, und geben Sie die IP-Adresse des Routers ein, der für den SDM-Zugriff konfiguriert wurde. Beispiel: https://<SDM_Router_IP_Address>Achten Sie darauf, alle Warnungen zu autorisieren, die Ihr Browser bezüglich der Authentizität des SSL-Zertifikats ausgibt. Standardmäßig sind Benutzername und Kennwort leer. Der Router zeigt dieses Fenster an, um das Herunterladen der SDM-Anwendung zu ermöglichen. In diesem Beispiel wird die Anwendung auf den lokalen Computer geladen und nicht in einem Java-Applet ausgeführt.

Cisco Router and Security Device Manager (SDM)



V 2.5

Copyright © 2002 - 2007 Cisco Systems, Inc.
All rights reserved.



Der SDM-

Download beginnt jetzt.

2. Wenn der SDM-Launcher heruntergeladen wurde, führen Sie die Schritte aus, die von den Aufforderungen angewiesen werden, um die Software zu installieren und den Cisco SDM Launcher auszuführen.
3. Geben Sie einen Benutzernamen und ein Kennwort ein (falls angegeben), und klicken Sie auf OK. In diesem Beispiel wird **cisco123** als Benutzername und **cisco123** als Kennwort

Authentication Required

Java

Enter login details to access level_15 or view_access on /10.77.241.109:

User name: cisco123

Password: ●●●●●●●●●●

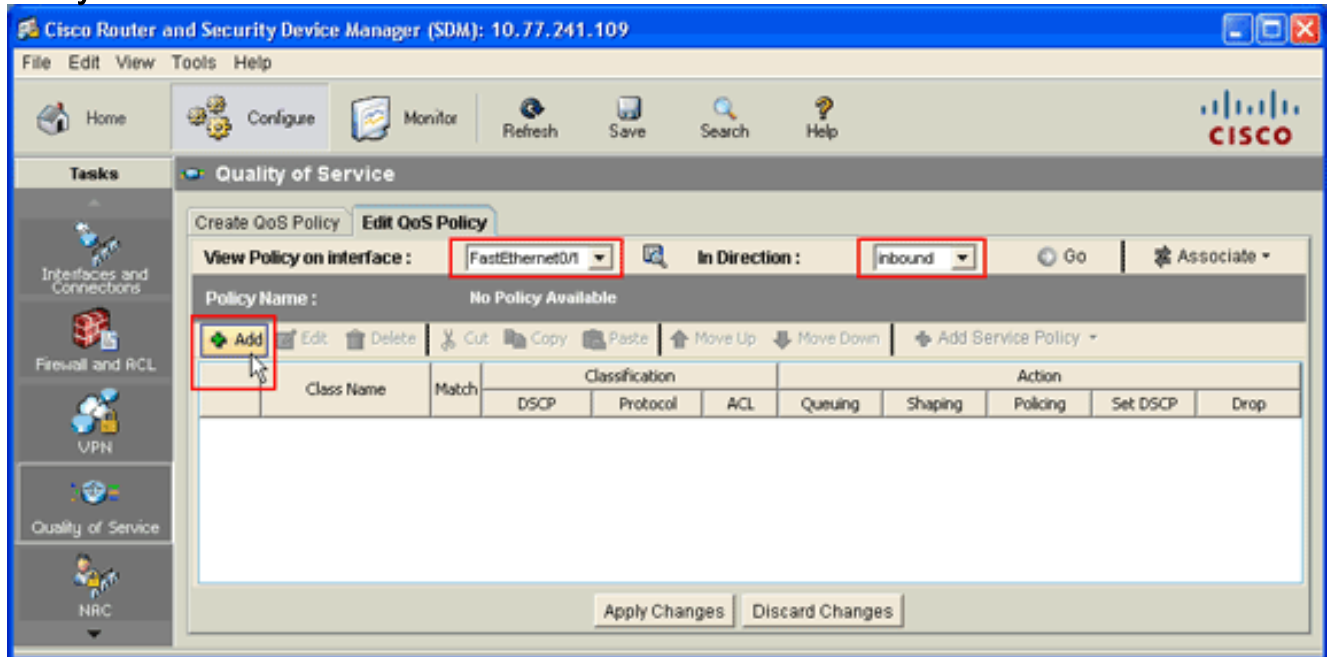
Save this password in your password list

OK Cancel

Authentication scheme: Basic

verwendet.

4. Wählen Sie **Configure > Quality of Service** aus, und klicken Sie auf der SDM-Startseite auf die Registerkarte **Edit QoS Policy**.



5. Wählen Sie in der Dropdown-Liste View Policy on Interface (Richtlinie für Schnittstelle anzeigen) den Schnittstellennamen aus, und wählen Sie dann die Richtung des Datenverkehrsflusses (ein- oder ausgehend) aus der Dropdown-Liste In Direction (Richtung) aus. In diesem Beispiel ist die Schnittstelle *FastEthernet 0/1*, und die Richtung ist *eingehend*.
6. Klicken Sie auf **Hinzufügen**, um eine neue QoS-Klasse für die Schnittstelle hinzuzufügen. Das Dialogfeld "QoS-Klasse hinzufügen" wird

Add a QoS Class

Class Name: Class Default:

Classification

Match Any All

Name	Value
DSCP	
Protocol	
Access Rule	

Edit...

Action

Drop

Set DSCP

Queuing

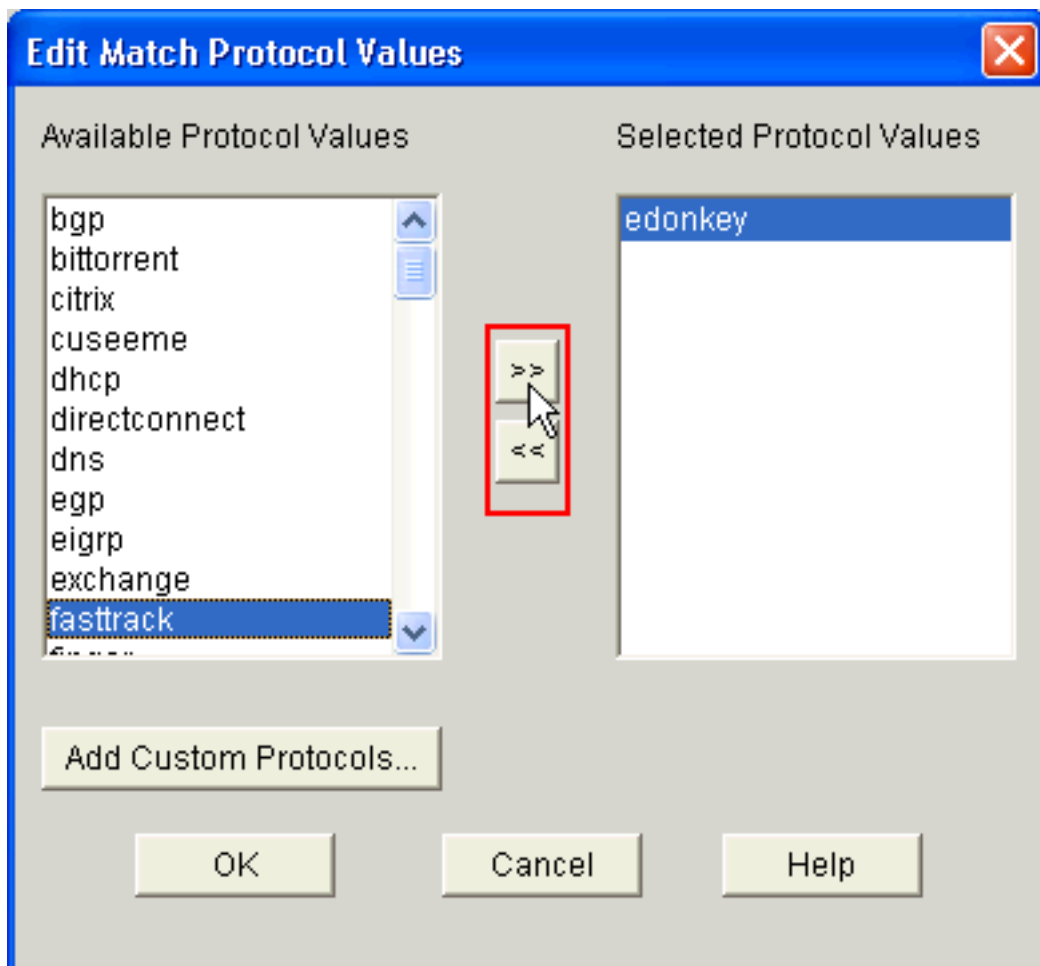
Shaping

Policing

OK Cancel Help

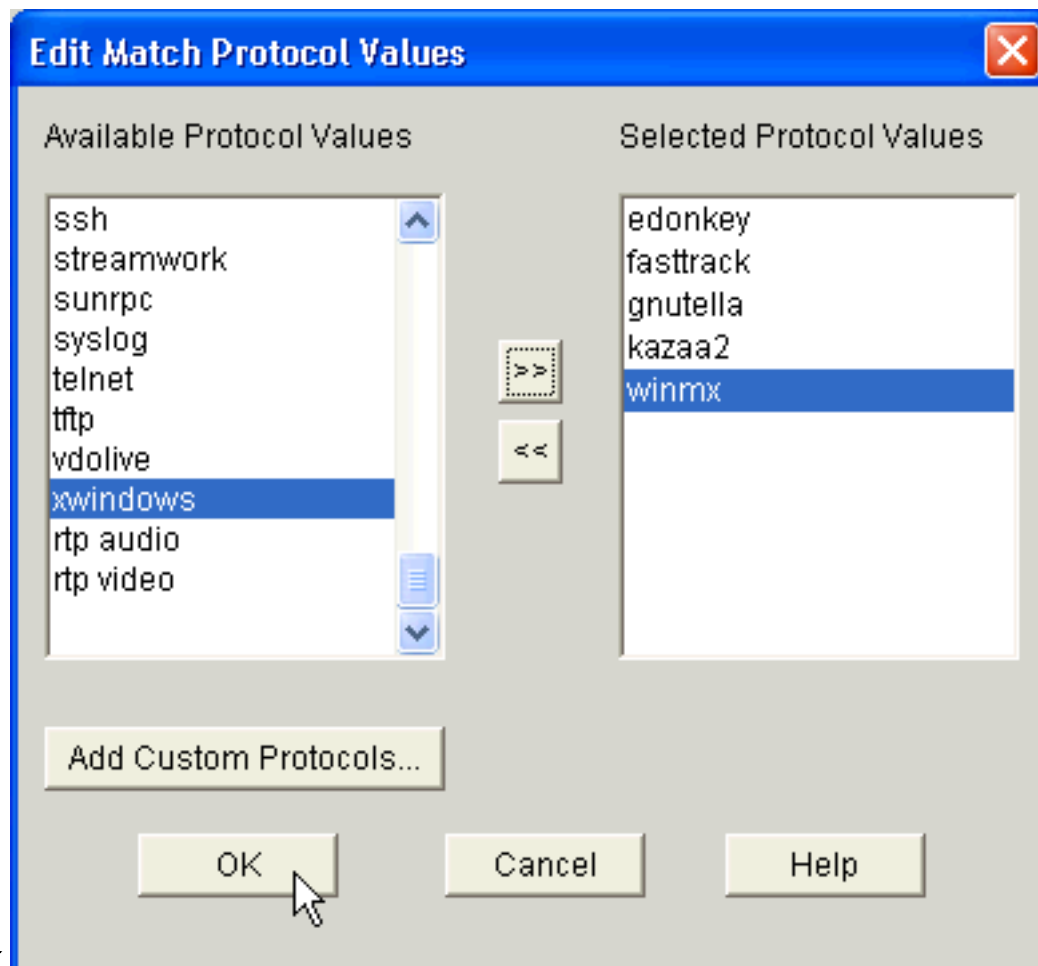
angezeigt.

7. Wenn Sie eine neue Klasse erstellen möchten, klicken Sie auf das Optionsfeld **Klassenname**, und geben Sie einen Namen für die Klasse ein. Andernfalls klicken Sie auf das Optionsfeld **Klassenstandard**, wenn Sie die Standardklasse verwenden möchten. In diesem Beispiel wird eine neue Klasse mit dem Namen *p2p* erstellt.
8. Klicken Sie im Bereich Klassifizierung entweder auf das Optionsfeld **Any (Beliebig)** oder das Optionsfeld **All (Alle)** für die Option Match (Übereinstimmung). In diesem Beispiel wird die *Any* Match-Option verwendet, die den **Befehl [class-map match-any p2p](#)** auf dem Router ausführt.
9. Wählen Sie **Protokoll** in der Klassifizierungsliste aus, und klicken Sie auf **Bearbeiten**, um den Protokollparameter zu bearbeiten. Das Dialogfeld "Protokollwerte bearbeiten" wird



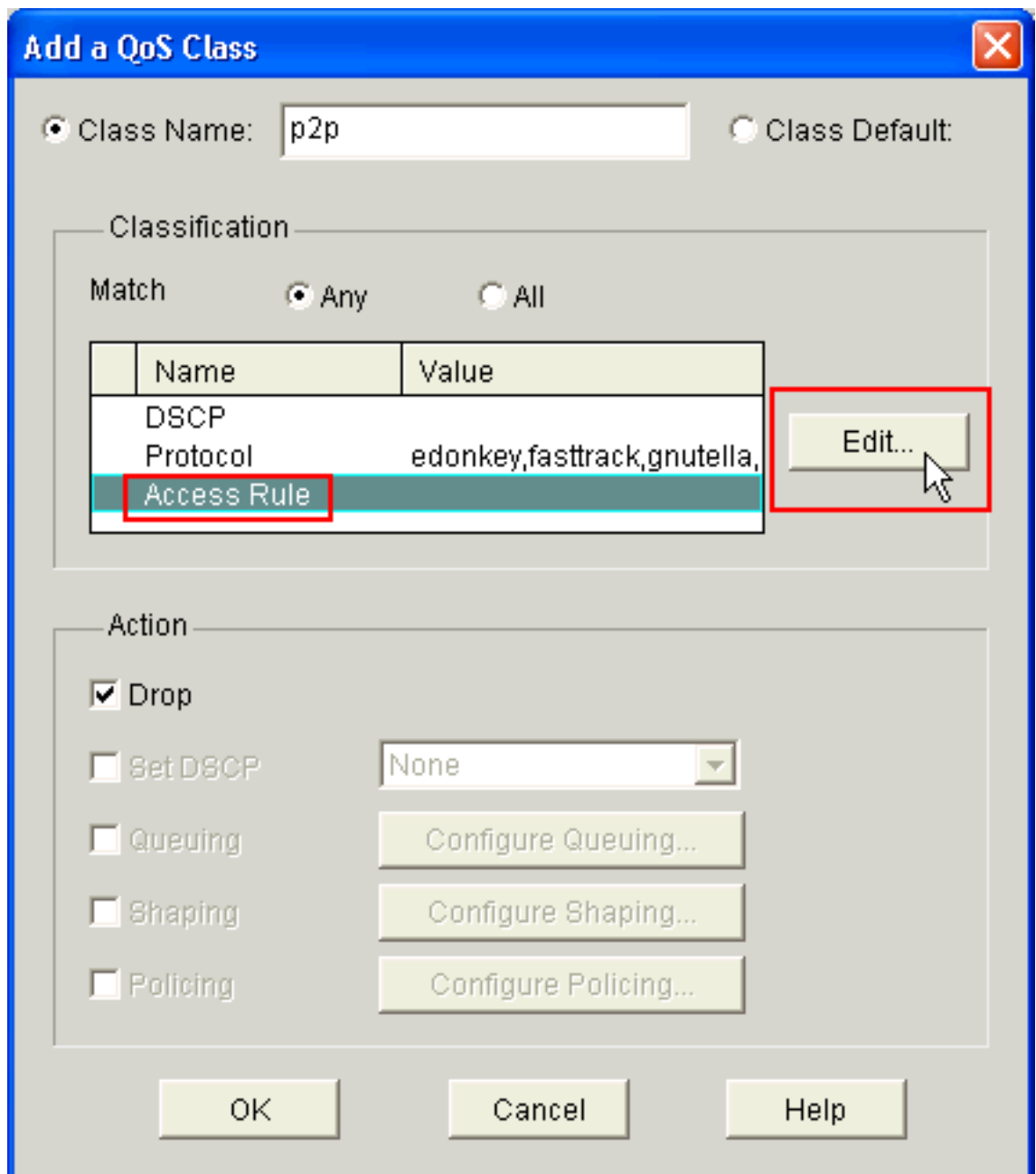
angezeigt.

- Wählen Sie in der Liste Verfügbare Protokollwerte jedes P2P-Protokoll aus, das Sie blockieren möchten, und klicken Sie auf die Schaltfläche mit dem rechten Pfeil (>>), um jedes Protokoll in die Liste Ausgewählte Protokollwerte zu verschieben. **Hinweis:** Um P2P-Datenverkehr mit NBAR zu klassifizieren, rufen Sie die [Seite Software Download \(Software-Download\)](#) auf, und laden Sie die neuesten Software- und Readme-Dateien für das P2P Protocol Description Language Module (PDLM) herunter. Zu den P2P-PDLMs, die heruntergeladen werden können, gehören WinMx, Bittorrent, Kazaa2, Gnutella, eDonkey, Fastrack und Napster. Je nach IOS benötigen Sie möglicherweise nicht die neuesten PDLM-Versionen, da einige möglicherweise in Ihr IOS integriert sind (z. B. Fastrack und Napster). Kopieren Sie nach dem Herunterladen die PDLMs in den Flash-Speicher des Routers, und laden Sie sie in IOS, indem Sie `ip nbar pdlm <flash_device>:<filename>.pdm` konfigurieren. Geben Sie den Befehl `show ip nbar pdlm` ein, um sicherzustellen, dass der Befehl erfolgreich geladen wurde. Nach dem Laden können Sie sie in den Übereinstimmungsprotokollanweisungen unter der Klassenzuordnungskonfiguration verwenden.
- Klicken Sie auf



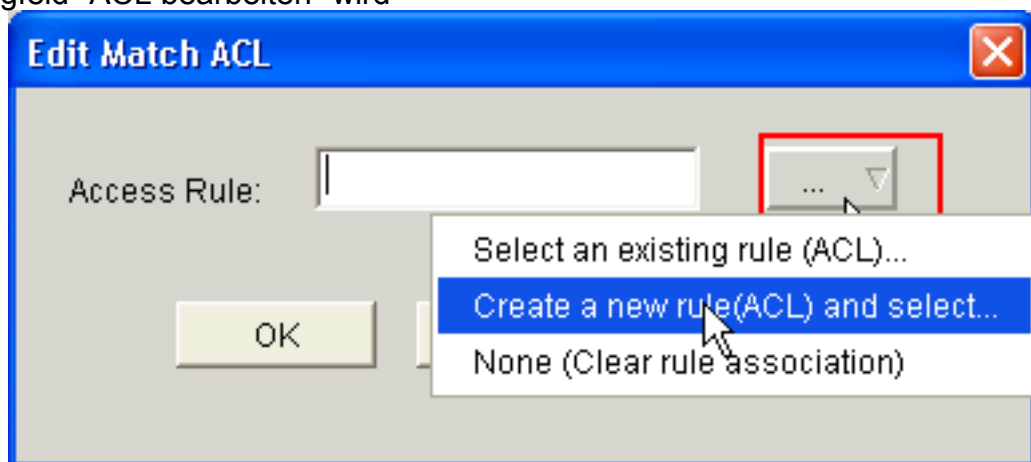
OK.

12. Wählen Sie im Dialogfeld QoS-Klasse hinzufügen aus der Liste Klassifizierung die Option **Zugriffsregeln**, und klicken Sie auf **Bearbeiten**, um eine neue Zugriffsregel zu erstellen. Sie können der **p2p**-Klassenzuordnung auch eine vorhandene Zugriffsregel



zuordnen.

Das Dialogfeld "ACL bearbeiten" wird



angezeigt.

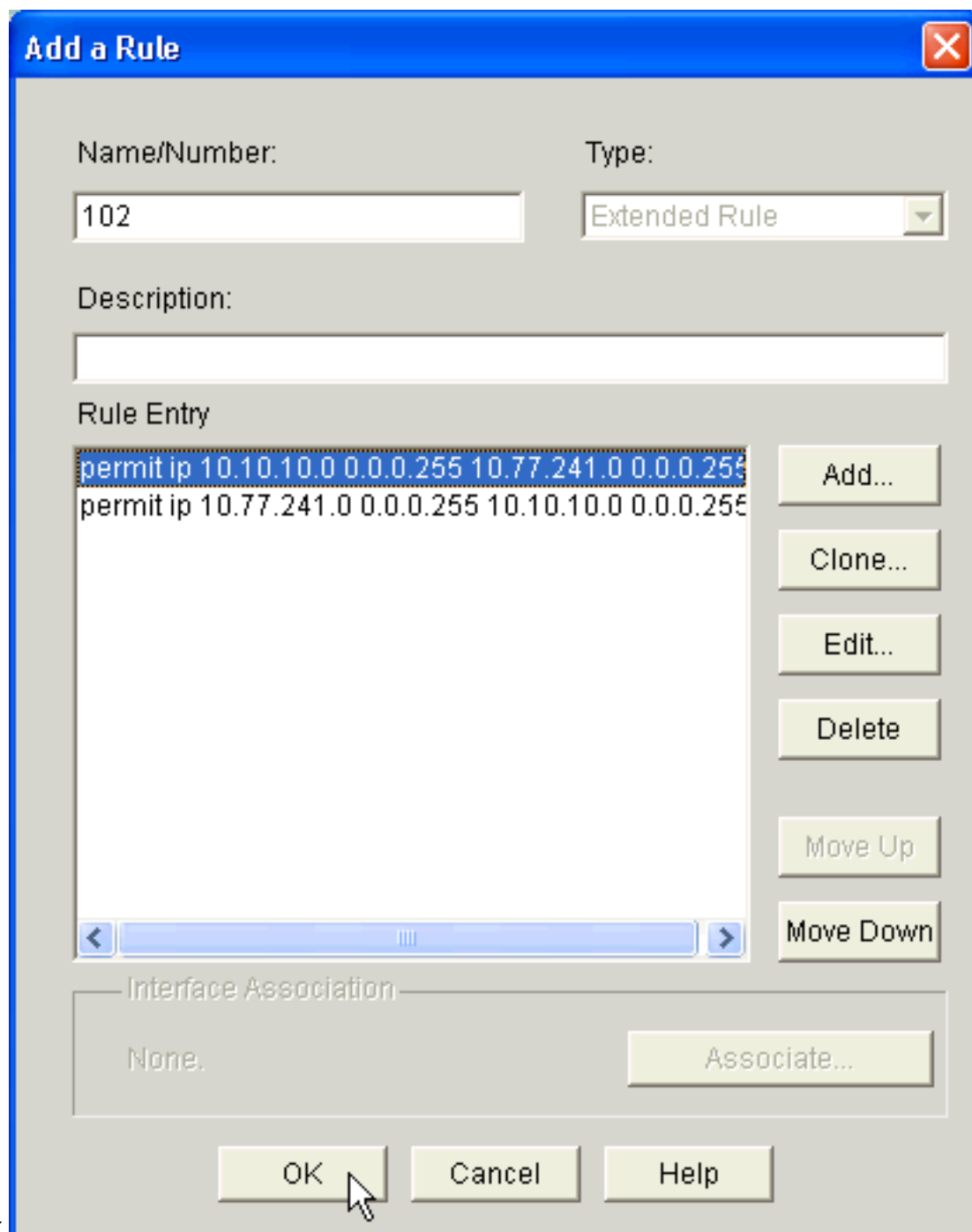
13. Klicken Sie auf die Schaltfläche Zugriffsregel (...), und wählen Sie die entsprechende Option aus. In diesem Beispiel wird eine neue ACL erstellt. Das Dialogfeld Regel hinzufügen wird

The image shows a dialog box titled "Add a Rule". It has a blue title bar with a close button. The main area is light gray. At the top left, there is a label "Name/Number:" followed by a text input field containing "102". To the right, there is a label "Type:" followed by a dropdown menu. The dropdown menu is open, showing "Extended Rule" selected (highlighted in blue) and "Standard Rule" below it. Below these fields is a "Description:" label followed by an empty text area. In the center is a large empty text area labeled "Rule Entry". To the right of this area is a vertical stack of buttons: "Add..." (with a mouse cursor pointing to it), "Clone...", "Edit...", "Delete", "Move Up", and "Move Down". At the bottom of the dialog is an "Interface Association" section with a label "None." and an "Associate..." button. At the very bottom are three buttons: "OK", "Cancel", and "Help".

angezeigt.

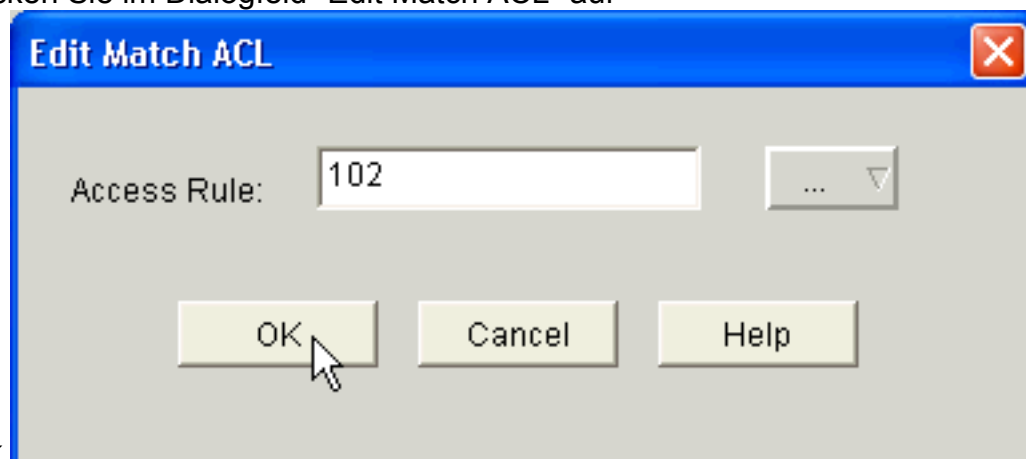
14. Geben Sie im Dialogfeld Regel hinzufügen im Feld Name/Nummer der ACL den Namen oder die Nummer der zu erstellenden ACL ein.
15. Wählen Sie in der Dropdown-Liste Type (Typ) den zu erstellenden ACL-Typ (entweder *Extended Rule (Erweiterte Regel)* oder *Standard Rule (Standardregel)*).
16. Klicken Sie auf **Hinzufügen**, um der ACL 102 Details hinzuzufügen. Das Dialogfeld Erweiterte Regeleintrag hinzufügen wird angezeigt.

17. Wählen Sie im Dialogfeld Add an Extended Rule Entry (Erweiterte Regeleingabe hinzufügen) aus der Dropdown-Liste Select an action (Aktion auswählen *Zulassen* oder *Verweigern*) eine Aktion aus, die angibt, ob die ACL-Regel den Datenverkehr zwischen dem Quell- und Zielnetzwerk zulassen oder verweigern soll. Diese Regel gilt für den ausgehenden Datenverkehr vom internen Netzwerk zum externen Netzwerk.
18. Geben Sie Informationen für das Quell- bzw. Zielnetzwerk in den Bereichen Quellhost/Netzwerk bzw. Zielhost/Netzwerk ein.
19. Klicken Sie im Bereich "Protokoll und Dienst" auf das entsprechende Optionsfeld. In diesem Beispiel wird IP verwendet.
20. Wenn Sie die übereinstimmenden Pakete mit dieser ACL-Regel protokollieren möchten, aktivieren Sie das Kontrollkästchen **Log Matches with this entry (Protokollzuordnungen zu diesem Eintrag)**.
21. Klicken Sie auf **OK**.
22. Klicken Sie im Dialogfeld Regel hinzufügen auf



OK.

23. Klicken Sie im Dialogfeld "Edit Match ACL" auf



OK.

24. Aktivieren Sie im Dialogfeld QoS-Klasse hinzufügen das Kontrollkästchen **Drop**, um den Router zu zwingen, P2P-Datenverkehr zu

Add a QoS Class

Class Name:
 Class Default:

Classification

Match Any All

Name	Value
DSCP	
Protocol	edonkey,fastrack,gnutella,
Access Rule	102

Action

Drop

Set DSCP

Queuing


Shaping

Policing

blockieren.

25. Klicken Sie auf **OK**. Die folgende Warnmeldung wird standardmäßig angezeigt, da der Schnittstelle keine QoS-Richtlinie zugeordnet ist.

Warning


 Selected interface has no QoS policy associated. SDM will auto-generate the policy and attach the configured class-map to it.

SDM generiert automatisch die QoS-Richtlinie und fügt die konfigurierte Klassenzuordnung der Richtlinie hinzu. Die CLI (Command Line Interface) entspricht diesem SDM-Konfigurationsschritt:

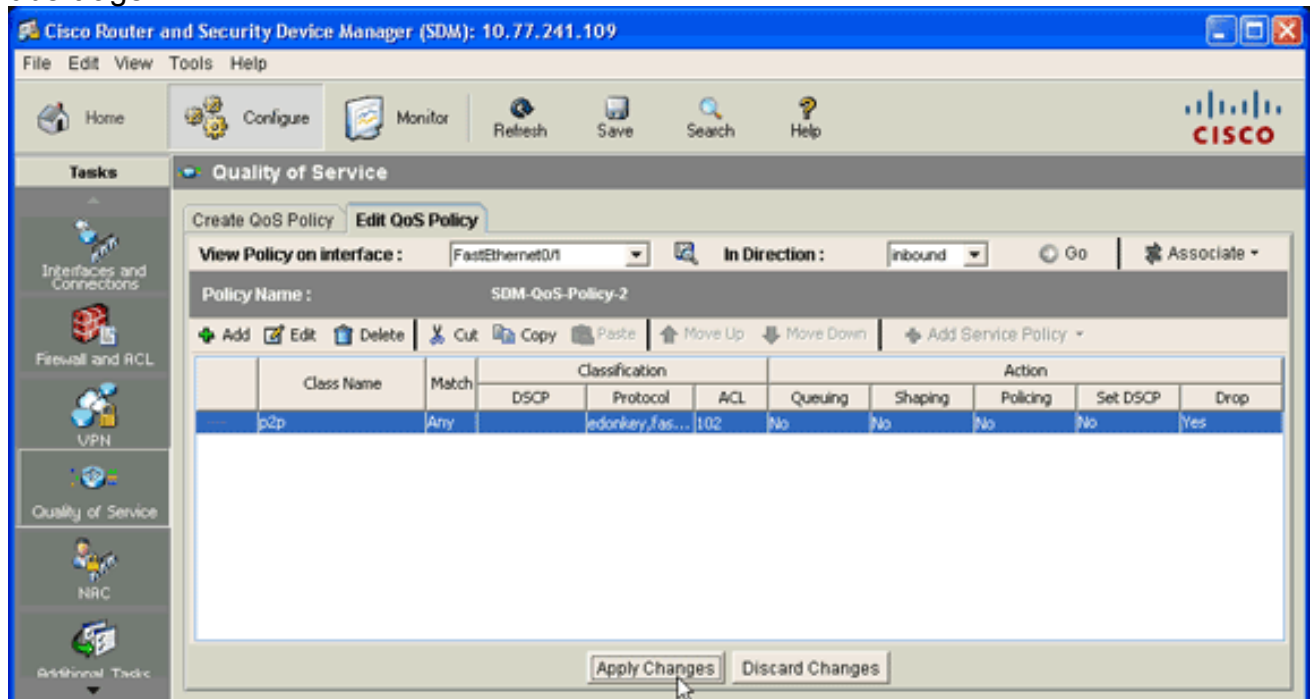
```

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. Klicken Sie auf der Registerkarte "Edit QoS Policy" (QoS-Richtlinie bearbeiten) auf **Apply Changes (Änderungen übernehmen)**, um die Konfiguration an den Router zu übertragen.



Anwendungs-Firewall - Funktion zur Instant Message Traffic Enforcement in Cisco IOS Version 12.4(4)T und höher

Durchsetzung von Instant Message-Datenverkehr

Die Funktion Application Firewall - Instant Message Traffic Enforcement (Anwendungs-Firewall - Instant Message Traffic-Durchsetzung) ermöglicht es Benutzern, eine Richtlinie zu definieren und durchzusetzen, die festlegt, welche Instant Messenger-Vkehrstypen in das Netzwerk zugelassen sind. Sie können mehrere Messengers (insbesondere AOL, YAHOO und MSN) gleichzeitig steuern, wenn diese in der **Anwendungsrichtlinie** unter **Application im** konfiguriert werden. Daher können auch die folgenden zusätzlichen Funktionen erzwungen werden:

- Konfiguration der Firewall-Inspektionsregeln
- Deep Packet Inspection der Payload (auf der Suche nach Services wie Text Chat)

Hinweis: Die Funktion zur Durchsetzung des Nachrichtenverkehrs durch die Anwendungs-Firewall-Instant wird in Cisco IOS-Versionen 12.4(4)T und höher unterstützt.

Instant Messenger-Anwendungsrichtlinie

Die Anwendungs-Firewall verwendet eine Anwendungsrichtlinie, die aus einer Sammlung statischer Signaturen besteht, um Sicherheitsverletzungen zu erkennen. Eine statische Signatur ist eine Auflistung von Parametern, die Protokollbedingungen angeben, die erfüllt werden müssen, bevor eine Aktion ausgeführt wird. Diese Protokollbedingungen und Reaktionen werden vom Endbenutzer über die CLI definiert, um eine Anwendungsrichtlinie zu bilden.

Die Cisco IOS-Anwendungs-Firewall wurde erweitert, um die Unterstützung systemeigener Instant Messenger-Anwendungsrichtlinien zu gewährleisten. So kann die Cisco IOS-Firewall jetzt Benutzerverbindungen zu Instant Messenger-Servern für AOL Instant Messenger (AIM), Yahoo! erkennen und verbieten. Messenger und MSN Messenger Instant Messaging-Dienste. Diese Funktion steuert alle Verbindungen für unterstützte Dienste, einschließlich Text-, Sprach-, Video- und Dateiübertragungsfunktionen. Die drei Anträge können individuell abgelehnt oder genehmigt werden. Jeder Service kann individuell gesteuert werden, sodass ein Text-Chat-Service zugelassen wird und Sprach-, Datei-, Video- und andere Dienste eingeschränkt werden. Diese Funktion ergänzt die vorhandenen Funktionen zur Anwendungsinspektion, um Instant Messenger (IM)-Anwendungsdatenverkehr zu kontrollieren, der als HTTP (Web)-Datenverkehr getarnt ist. Weitere Informationen finden Sie unter [Anwendungs-Firewall - Durchsetzung von Instant Message-Datenverkehr](#).

Hinweis: Wenn eine IM-Anwendung blockiert wird, wird die Verbindung zurückgesetzt und eine Syslog-Meldung generiert.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des Befehls show anzuzeigen**.

- [show ip nbar pdlm](#) - Um das von NBAR verwendete PDLM anzuzeigen, verwenden Sie den Befehl **show ip nbar pdlm** im privilegierten EXEC-Modus:

```
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](#) - Um Informationen über die Version der NBAR-Software in Ihrer Cisco IOS-Version oder die Version eines NBAR PDLM auf Ihrem Cisco IOS-Router anzuzeigen, verwenden Sie den Befehl **show ip nbar version** im privilegierten EXEC-Modus:

```
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](#) - Um die Paketstatistiken aller Klassen anzuzeigen, die für alle Dienstrichtlinien entweder auf der angegebenen Schnittstelle oder Subschnittstelle oder auf einer bestimmten permanenten Virtual Circuit (PVC) auf der Schnittstelle konfiguriert sind, verwenden Sie den Befehl **show policy-map interface** im privilegierten EXEC-Modus:

```

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

```

- **show running-config policy-map** - Um alle Richtlinienzuordnungskonfigurationen sowie die Standardzuordnungskonfiguration anzuzeigen, verwenden Sie den Befehl **show running-config policy-map**:

```

R1#show running-config policy-map
Building configuration...

```

```

Current configuration : 57 bytes

```

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

- **show running-config class-map** - Verwenden Sie den Befehl **show running-config class-map**, um Informationen über die Klassenzuordnungskonfiguration anzuzeigen:

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des Befehls show** anzuzeigen.

Hinweis: Beachten Sie [vor der](#) Verwendung von **Debug**-Befehlen die [Informationen](#) zu [Debug-Befehlen](#).

- **show access-list** - Um die Zugriffslistenkonfiguration anzuzeigen, die auf dem Cisco IOS-Router ausgeführt wird, verwenden Sie den Befehl **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
```

Zugehörige Informationen

- [Cisco IOS Security Configuration Guide, Release 12.4-Support](#)
- [Network Based Application Recognition \(NBAR\)](#)
- [Cisco Express Forwarding \(CEF\)](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)