Security Device Manager: Blocco del traffico P2P su un router Cisco IOS con configurazione NBAR Esempio

Sommario

Introduzione

In questo documento viene descritto come configurare il router Cisco IOS® in modo da bloccare il traffico peer-to-peer (P2P) dalla rete interna verso Internet utilizzando Network Based Application Recognition (NBAR).

NBAR riconosce specifici protocolli e applicazioni di rete utilizzati nella rete. Dopo che un protocollo o un'applicazione viene riconosciuta da NBAR, è possibile utilizzare l'interfaccia della riga di comando Modular Quality of Service (MQC) per raggruppare in classi i pacchetti associati a tali protocolli o applicazioni. Queste classi sono raggruppate in base alla conformità dei pacchetti a determinati criteri.

Per NBAR, il criterio è se il pacchetto corrisponde a un protocollo o a un'applicazione specifica nota a NBAR. Utilizzando MQC, il traffico di rete con un protocollo (Citrix, ad esempio) può essere indirizzato a una classe di traffico, mentre il traffico che corrisponde a un protocollo di rete diverso (gnutella, ad esempio) può essere indirizzato a un'altra classe di traffico. Successivamente, è possibile assegnare al traffico di rete all'interno di ciascuna classe il trattamento QoS appropriato

utilizzando una policy di traffico (policy map). Per ulteriori informazioni su NBAR, consultare la sezione Classificazione del traffico di rete tramite NBAR nella *Guida alla configurazione di soluzioni Cisco IOS Quality of Service*.

Prerequisiti

Requisiti

Prima di configurare NBAR per bloccare il traffico P2P, è necessario abilitare Cisco Express Forwarding (CEF).

Per abilitare il protocollo CEF, usare il comando **ip cef** in modalità di configurazione globale:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Router Cisco 2801 con software Cisco IOS® versione 12.4(15)T
- Cisco Security Device Manager (SDM) versione 2.5

Nota: per consentire al router di essere configurato dal modello SDM, consultare il documento sulla configurazione base del router utilizzando l'SDM.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Panoramica di NBAR (Network Based Application Recognition)

Network-Based Application Recognition (NBAR) è un motore di classificazione che riconosce e classifica un'ampia gamma di protocolli e applicazioni. Quando NBAR riconosce e classifica un protocollo o un'applicazione, la rete può essere configurata in modo da applicare la qualità del servizio (QoS) appropriata per tale applicazione o traffico con tale protocollo.

NBAR esegue le seguenti funzioni:

- **Identificazione di applicazioni e protocolli (dal layer 4 al layer 7)**NBAR può classificare le applicazioni che utilizzano:Numeri di porta TCP (Transfer Control Protocol) e UDP (User Datagram Protocol) assegnati in modo statico.Protocolli IP non UDP e non TCP.Numeri di porta TCP e UDP assegnati in modo dinamico negoziati durante la connessione. L'ispezione

stateful è necessaria per la classificazione di applicazioni e protocolli. L'ispezione con conservazione dello stato consente di individuare le connessioni dati che verranno classificate passando le connessioni di controllo sulla porta di connessione dati in cui vengono effettuate le assegnazioni.Classificazione porte secondarie: Classificazione del traffico HTTP (URL, mime o nomi host) e delle applicazioni Citrix in base al nome dell'applicazione pubblicata.Classificazione basata sull'ispezione approfondita dei pacchetti e su più attributi specifici dell'applicazione. La classificazione del payload del protocollo RTP (Real-Time Transport Protocol) si basa su questo algoritmo con cui il pacchetto viene classificato come RTP in base a più attributi nell'intestazione RTP.

- **Rilevamento protocollo**L'individuazione del protocollo è una funzione NBAR di uso comune che raccoglie statistiche sulle applicazioni e sui protocolli (conteggi dei pacchetti, conteggi dei byte e velocità di trasmissione) per interfaccia. Gli strumenti di gestione basati su GUI possono visualizzare graficamente queste informazioni, eseguendo il polling delle statistiche SNMP dal MIB (NBAR PD Management Information Base). Come per qualsiasi funzione di rete, è importante comprendere le caratteristiche di prestazioni e scalabilità prima di implementare la funzione in una rete di produzione. Nelle piattaforme basate su software, le metriche considerate sono l'impatto sull'utilizzo della CPU e la velocità di trasferimento dei dati sostenibile quando questa funzione è abilitata. Per configurare NBAR in modo da rilevare il traffico di tutti i protocolli noti a NBAR su un'interfaccia specifica, usare il comando **ip nbar protocol-discovery** in modalità di configurazione interfaccia o in modalità di configurazione VLAN. Per disabilitare la funzione traffic discovery, usare il comando **no ip nbar protocol-discovery**.

Configurazione del blocco del traffico peer-to-peer (P2P)

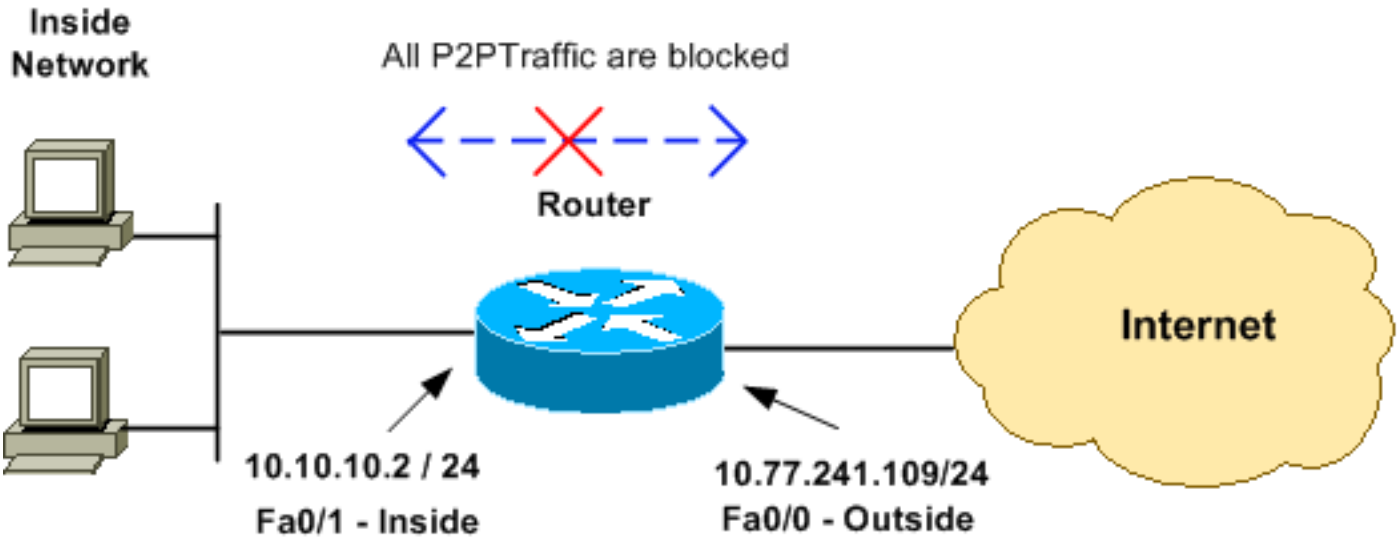
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: alcuni tipi di traffico P2P non possono essere bloccati completamente a causa della natura del protocollo P2P. Questi protocolli P2P modificano in modo dinamico le proprie firme per ignorare qualsiasi motore DPI che cerchi di bloccare completamente il traffico. Pertanto, Cisco consiglia di limitare la larghezza di banda anziché bloccarla completamente. (Limita la larghezza di banda per il traffico. Assegnare una larghezza di banda molto inferiore; la connessione deve tuttavia essere interrotta.)

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazione router

Configurazione per bloccare il traffico P2P sul router 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
```

Configurazione del router con SDM

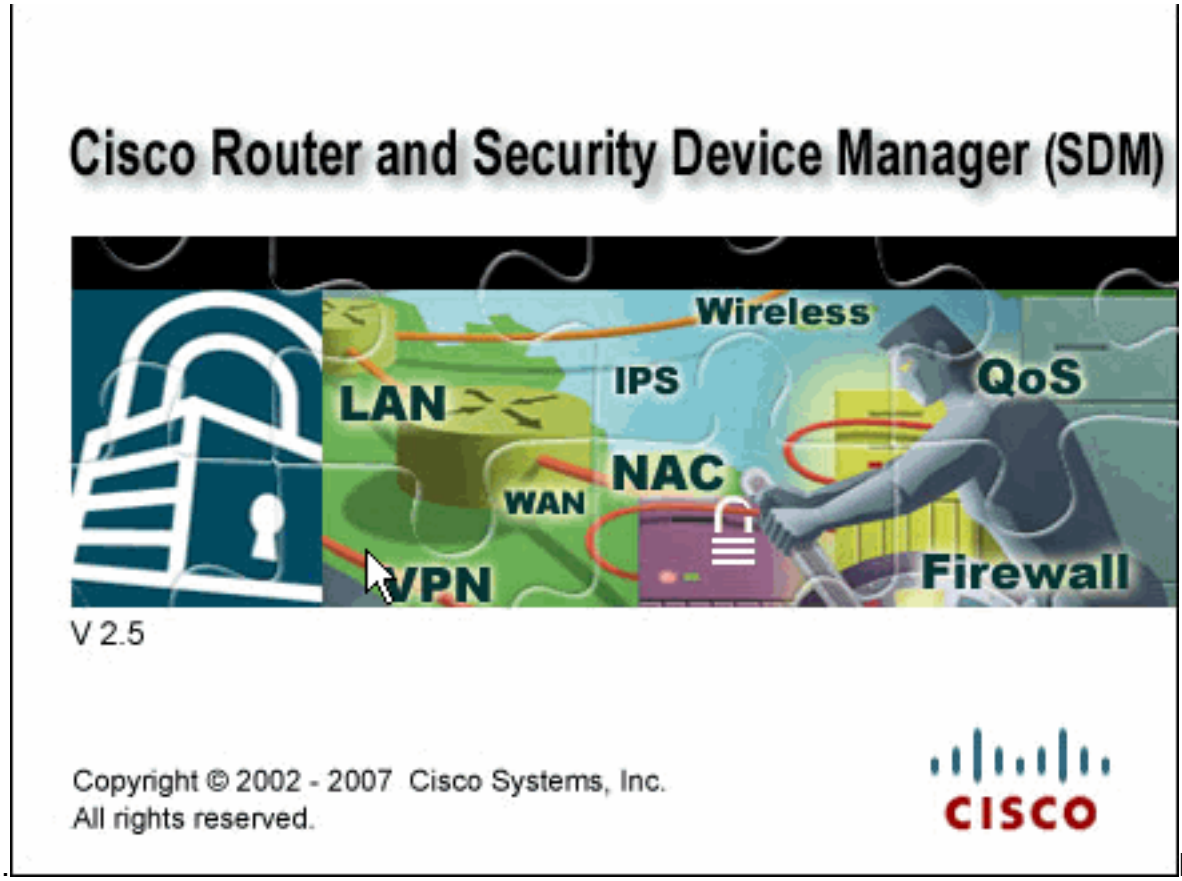
Configurazione SDM router

Completare questa procedura per configurare il blocco del traffico P2P su un router Cisco IOS:

Nota: per configurare NBAR in modo da individuare il traffico per tutti i protocolli noti a NBAR su un'interfaccia specifica, è necessario usare il comando ip nbar protocol-discovery in modalità configurazione interfaccia o in modalità configurazione VLAN per abilitare il rilevamento del traffico. Procedere con la configurazione SDM dopo aver configurato l'individuazione del protocollo sull'interfaccia richiesta in cui viene utilizzato il criterio QoS configurato.

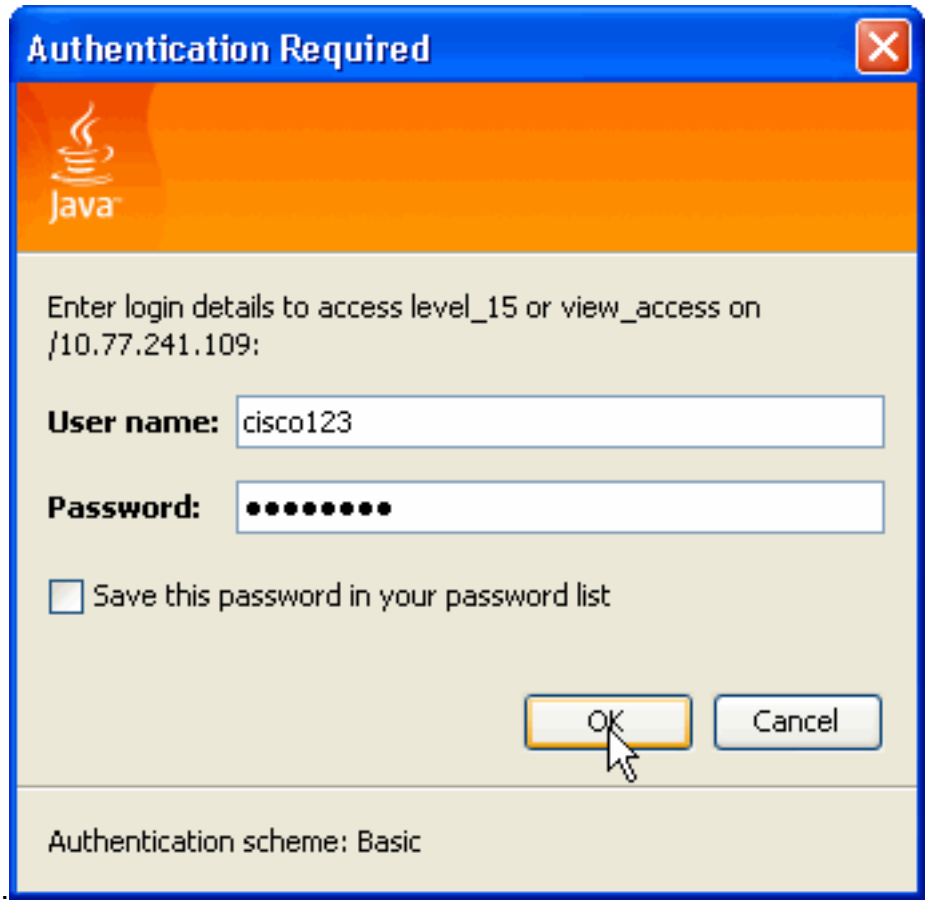
```
Hostname#config t
               Hostname(config)#interface fastEthernet 0/1
               Hostname(config-if)#ip nbar protocol-discovery
               Hostname(config-if)#end
```

1. Aprire un browser e immettere l'indirizzo IP del router configurato per l'accesso SDM. Ad esempio, **https://*<Indirizzo_IP_Router_SDM>***Accertarsi di autorizzare gli avvisi che il browser visualizza relativi all'autenticità del certificato SSL. Il nome utente e la password predefiniti sono entrambi vuoti.Il router visualizza questa finestra per consentire il download dell'applicazione SDM. In questo esempio l'applicazione viene caricata nel computer locale e non viene eseguita in un'applet



Java.Il download dell'SDM ha inizio ora.

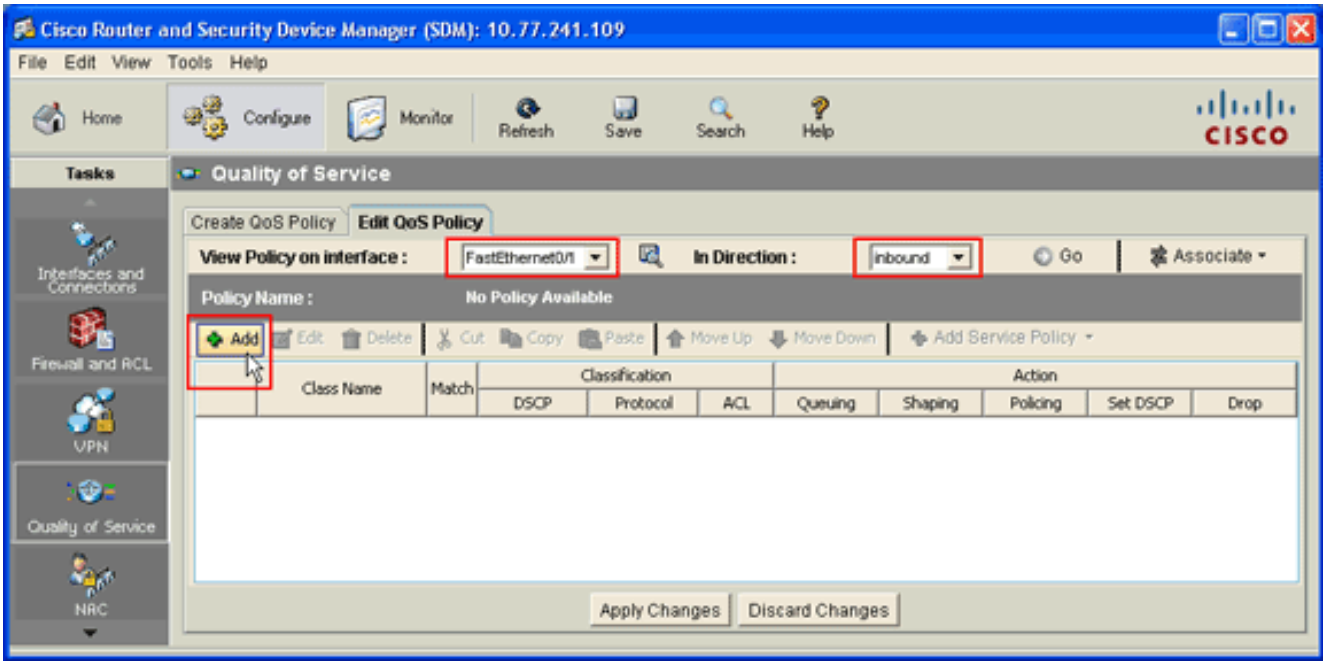
2. Una volta scaricato l'utilità di avvio SDM, completare la procedura indicata dalle istruzioni per installare il software ed eseguire l'utilità di avvio SDM di Cisco.
3. Immettere un nome utente e una password, se specificati, e fare clic su **OK**.In questo esempio viene utilizzato **cisco123** come nome utente e **cisco123** come



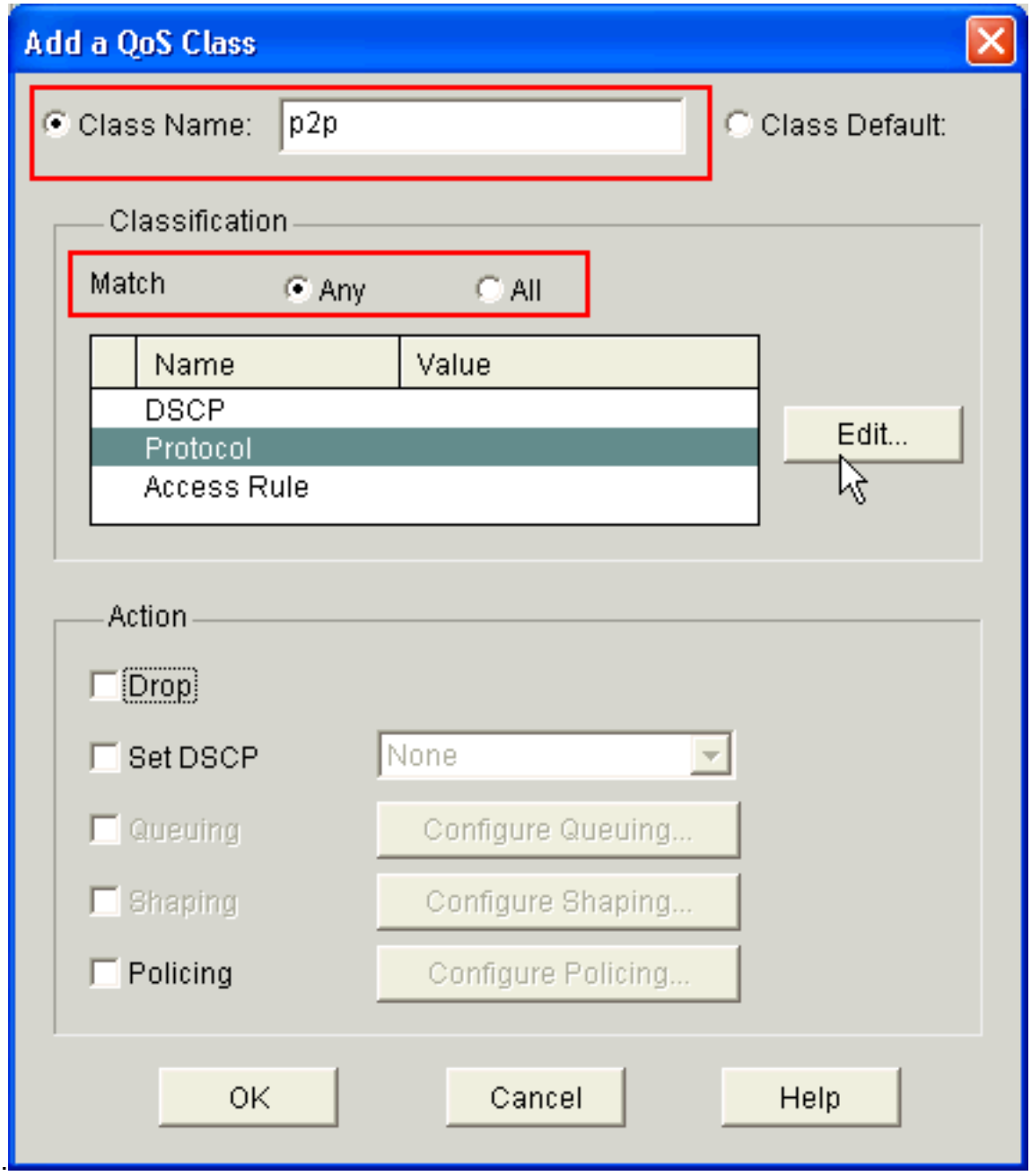
password.

4. Scegliere **Configura > Quality of Service**, quindi fare clic sulla scheda **Modifica criterio QoS**

nella home page
SDM.

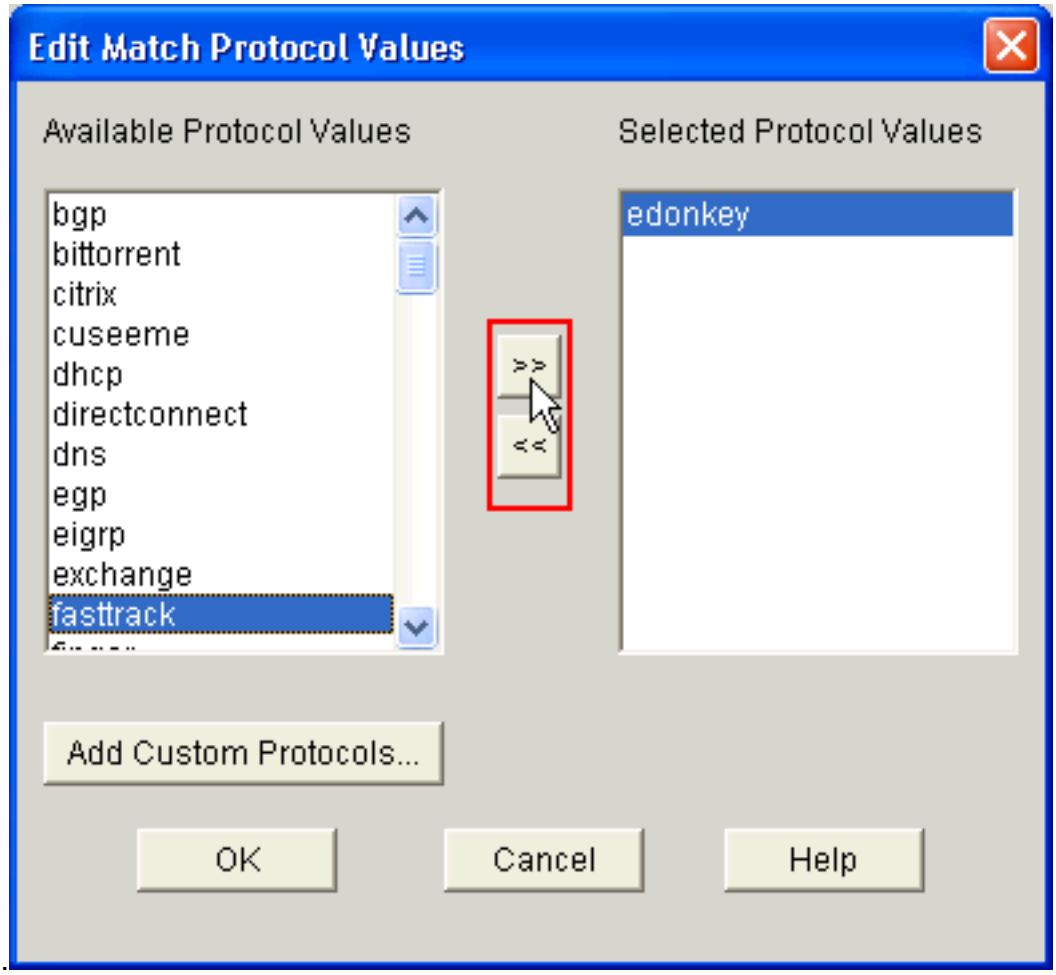


5. Dall'elenco a discesa Visualizza criterio sull'interfaccia scegliere il nome dell'interfaccia e quindi la direzione del flusso di traffico (in entrata o in uscita) dall'elenco a discesa In direzione.Nell'esempio, l'interfaccia è *Fast Ethernet 0/1*, la direzione è *inbound*.
6. Per aggiungere una nuova classe QoS per l'interfaccia, fare clic su **Add** (Aggiungi).Verrà visualizzata la finestra di dialogo Aggiungi classe



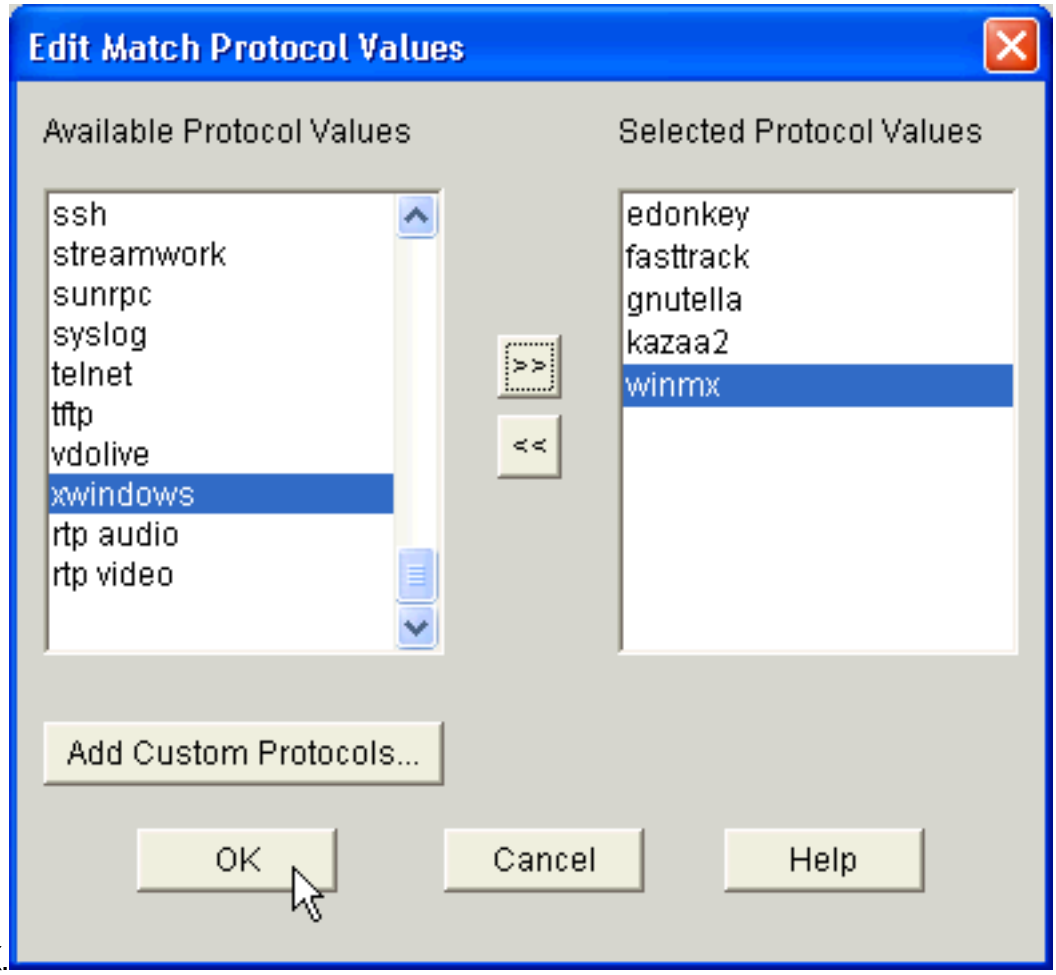
QoS.

7. Se si desidera creare una nuova classe, fare clic sul pulsante di opzione **Nome classe** e immettere un nome per la classe. In caso contrario, fare clic sul pulsante di scelta **Classe predefinita** se si desidera utilizzare la classe predefinita.In questo esempio viene creata una nuova classe denominata *p2p*.
8. Nell'area Classificazione, fare clic sul pulsante di scelta **Qualsiasi** o **Tutto** per l'opzione Corrispondenza.In questo esempio viene utilizzata l'opzione *Any* Match, che esegue il comando class-map match-any p2p sul router.
9. Selezionare **Protocol** (Protocollo) nella lista Classificazione, quindi fare clic su **Edit** (Modifica) per modificare il parametro protocol (protocollo).Verrà visualizzata la finestra di dialogo Modifica valori protocollo di

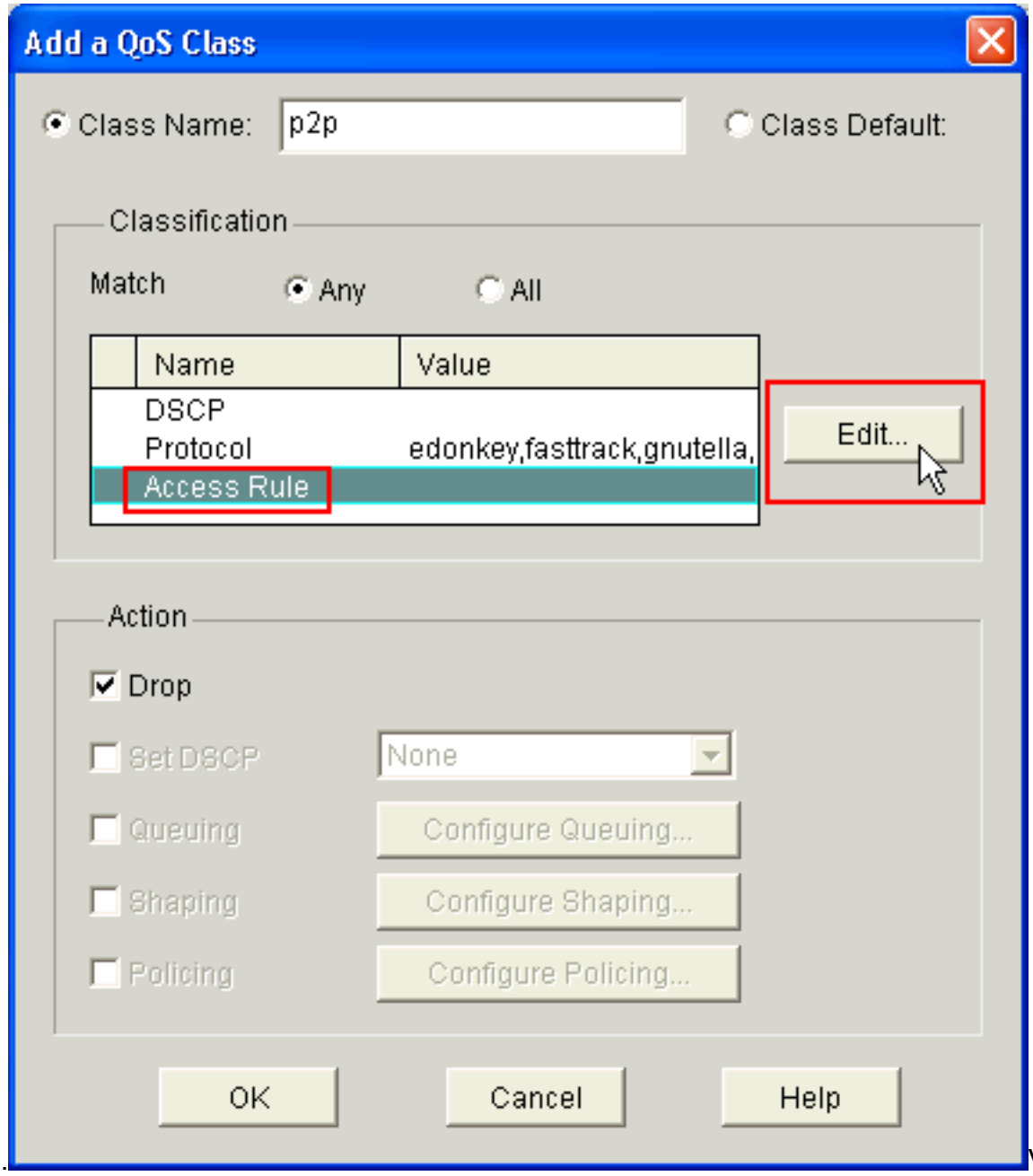


corrispondenza.

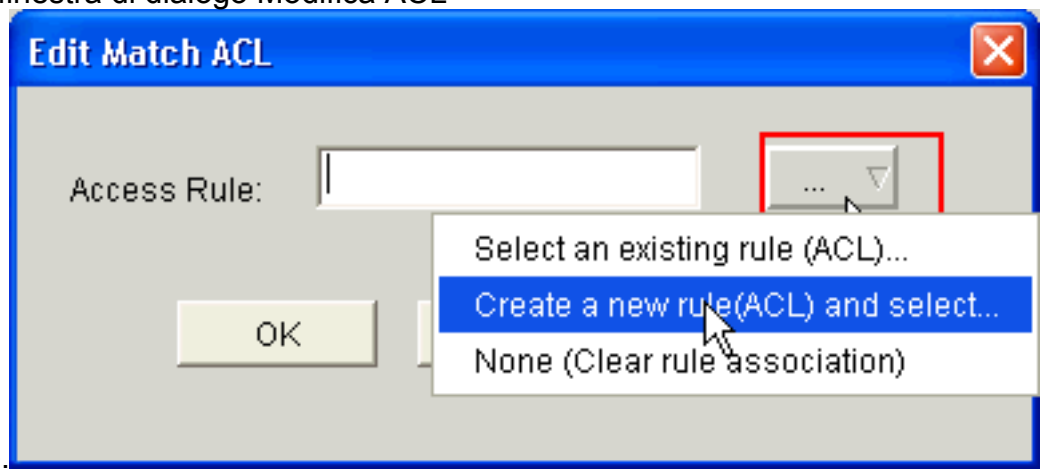
10. Dalla lista Valori protocollo disponibili, selezionare ogni protocollo P2P che si desidera bloccare e fare clic sul pulsante freccia destra (**>>**) per spostare ogni protocollo nella lista Valori protocollo selezionati.**Nota:** per classificare il traffico P2P con NBAR, andare alla pagina di download del software, e scaricare il software P2P Protocol Description Language Module (PDLM) più recente e i file Leggimi. I PDF P2P disponibili per il download includono WinMx, Bittorrent, Kazaa2, Gnutella, eDonkey, Fasttrack e Napster. A seconda del sistema operativo IOS in uso, potrebbe non essere necessario disporre delle versioni più recenti di PDLM, poiché alcune potrebbero essere integrate nel sistema operativo IOS (ad esempio, Fasttrack e Napster). Una volta scaricati, copiare i PDLM nella memoria flash del router e caricarli in IOS configurando **ip nbar pdlm <*flash_device*>:<*nomefile*>.pdlm**. Per verificare che il caricamento sia stato completato, usare il comando **show ip nbar pdlm**. Una volta caricate, è possibile utilizzarle nelle istruzioni di protocollo di corrispondenza nella configurazione della mappa di classe.



11. Fare clic su **OK**.
12. Nella finestra di dialogo Aggiungi classe QoS selezionare **Regole di accesso** dall'elenco Classificazione e fare clic su **Modifica** per creare una nuova regola di accesso. È inoltre possibile eseguire il mapping di una regola di accesso esistente alla mappa di classe

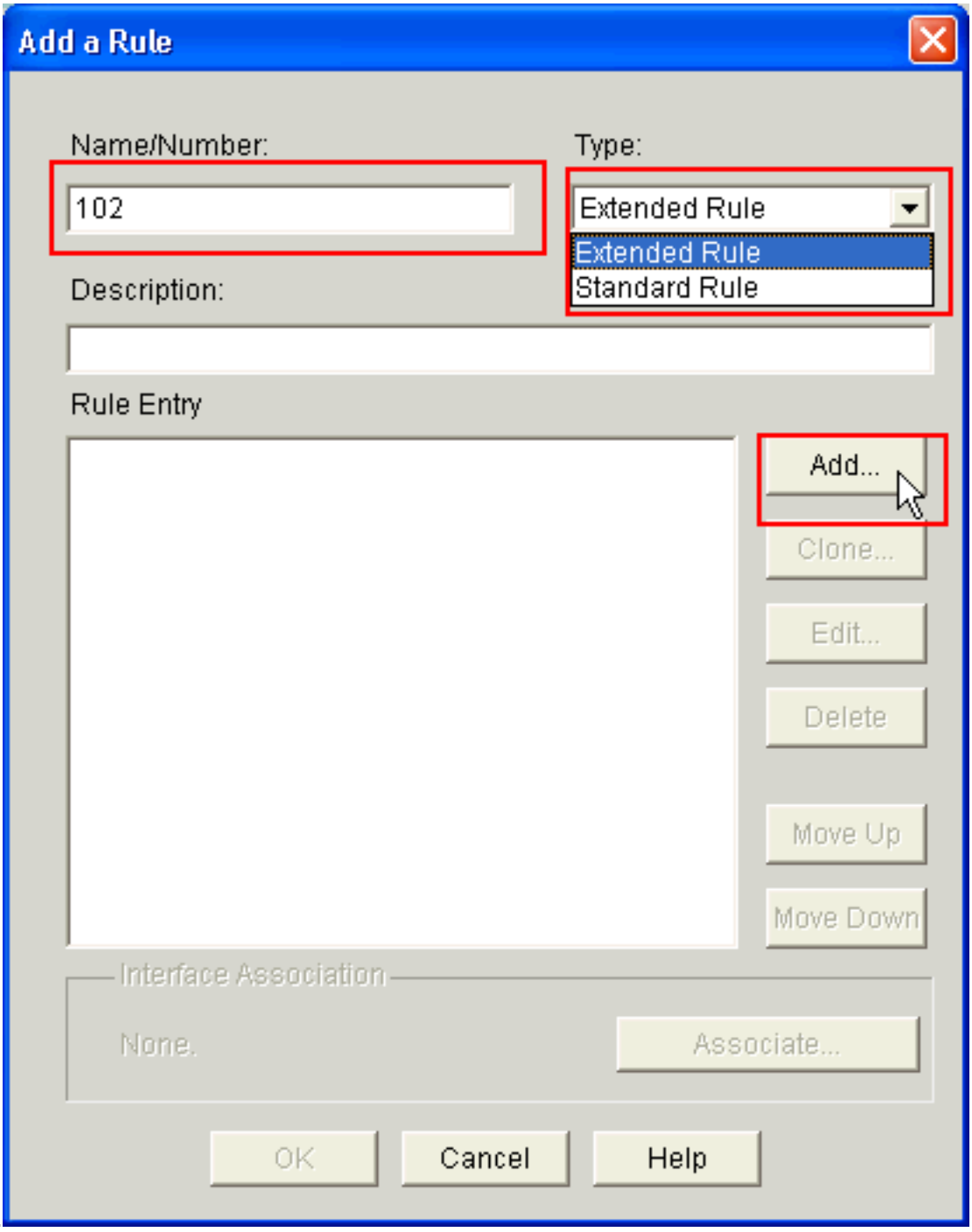


p2p.Viene visualizzata la finestra di dialogo Modifica ACL



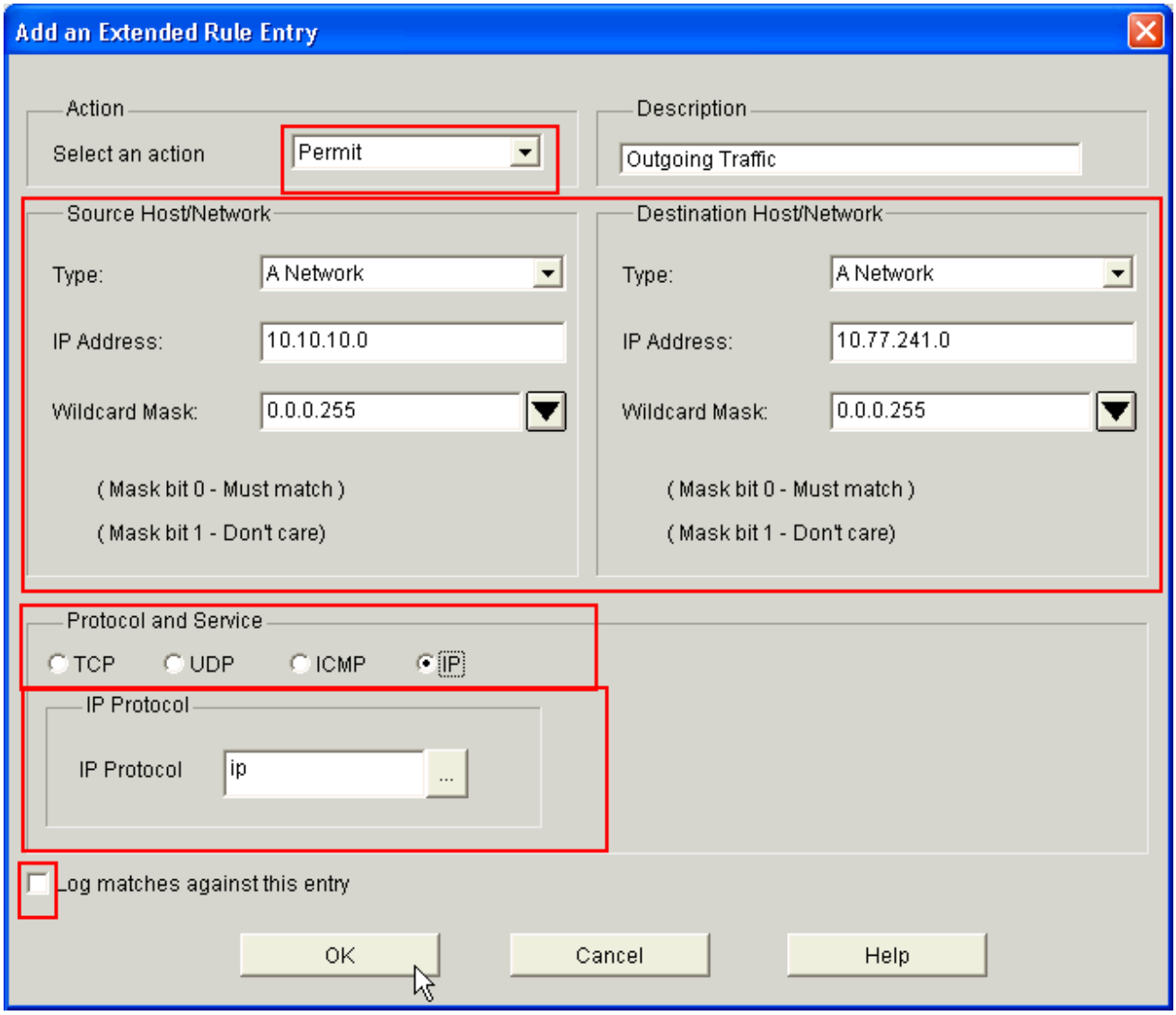
corrispondente.

13. Fare clic sul pulsante Regola di accesso (**...**) e scegliere l'opzione appropriata. In questo esempio viene creato un nuovo ACL.Verrà visualizzata la finestra di dialogo Aggiungi

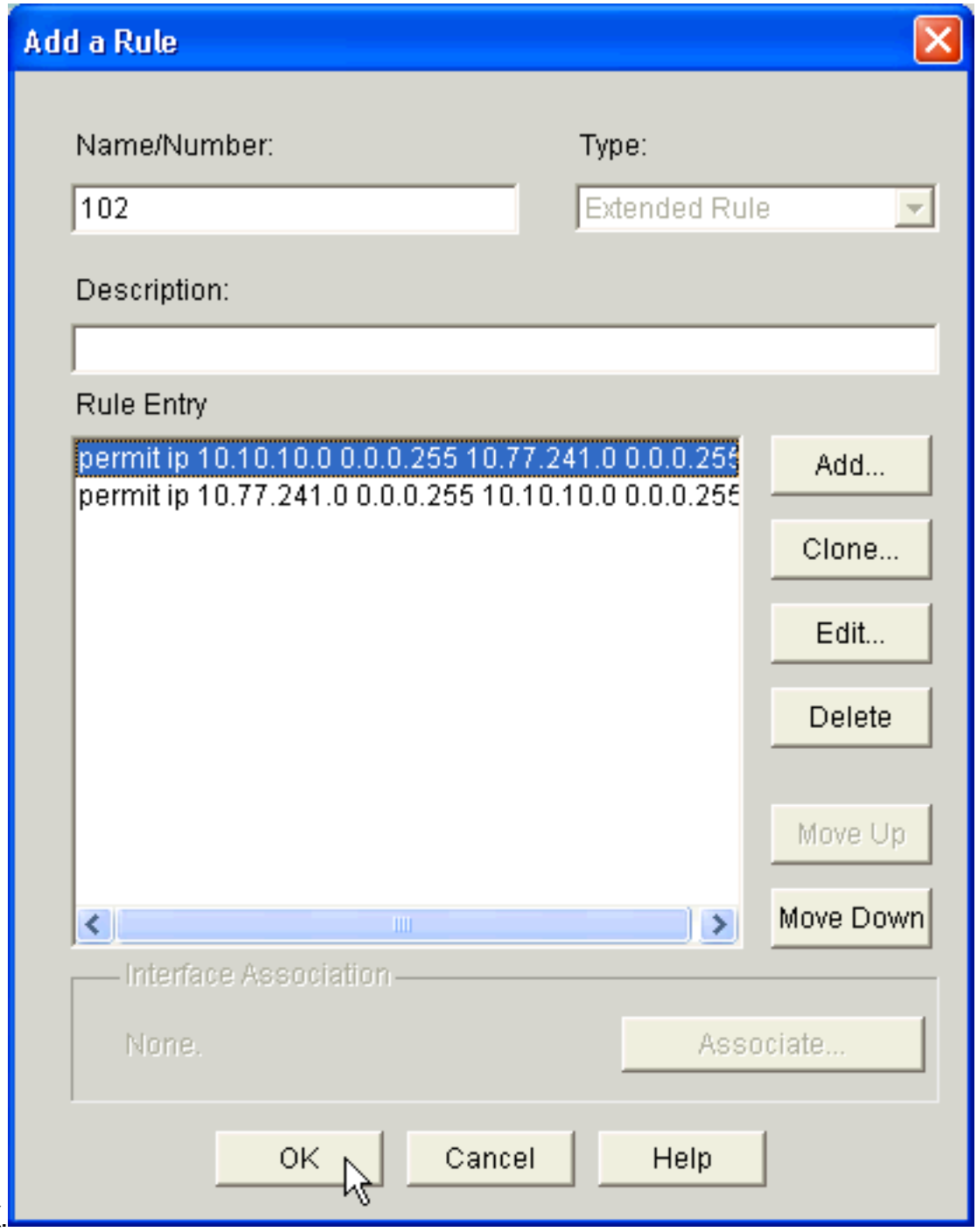


regola.

14. Nella finestra di dialogo Add a Rule, immettere il nome o il numero dell'ACL da creare nel campo Name/Number (Nome/Numero) dell'ACL.
15. Dall'elenco a discesa Tipo, scegliere il tipo di ACL da creare (*regola estesa* o *regola standard*).
16. Per aggiungere dettagli all'ACL *102*, fare clic su **Add** (Aggiungi).Verrà visualizzata la finestra di dialogo Aggiungi voce regola
    estesa.

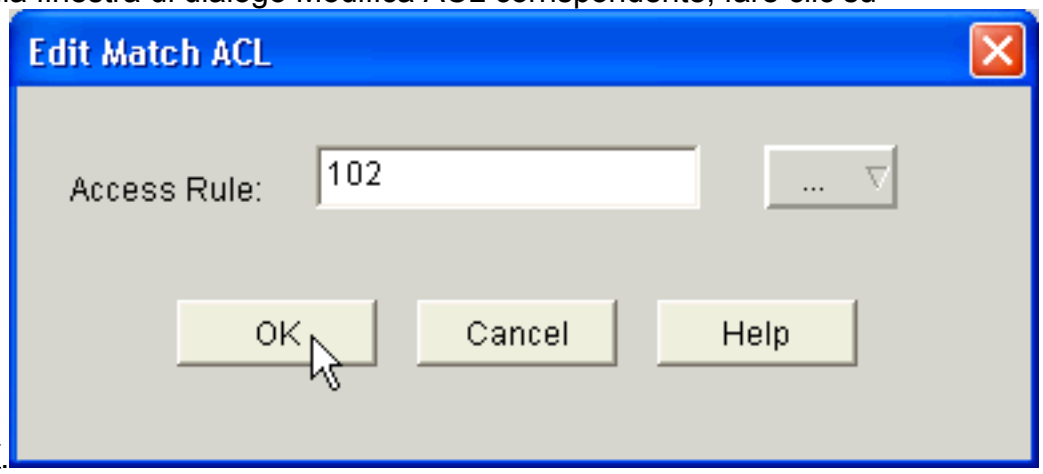


17. Nella finestra di dialogo Aggiungi voce di regola estesa, scegliere un'azione (*Autorizza* o *Nega*) dall'elenco a discesa Selezionare un'azione per indicare se la regola ACL deve autorizzare o negare il traffico tra le reti di origine e di destinazione. Regola per il traffico in uscita dalla rete interna verso la rete esterna.
18. Immettere le informazioni relative alle reti di origine e di destinazione rispettivamente nelle aree Host/rete di origine e Host/rete di destinazione.
19. Nell'area Protocollo e servizio fare clic sul pulsante di opzione appropriato. Nell'esempio viene usato il protocollo IP.
20. Per registrare i pacchetti corrispondenti in base a questa regola ACL, selezionare la casella di controllo **Registra corrispondenze in base a questa voce**.
21. Fare clic su **OK**.
22. Nella finestra di dialogo Aggiungi regola fare clic su



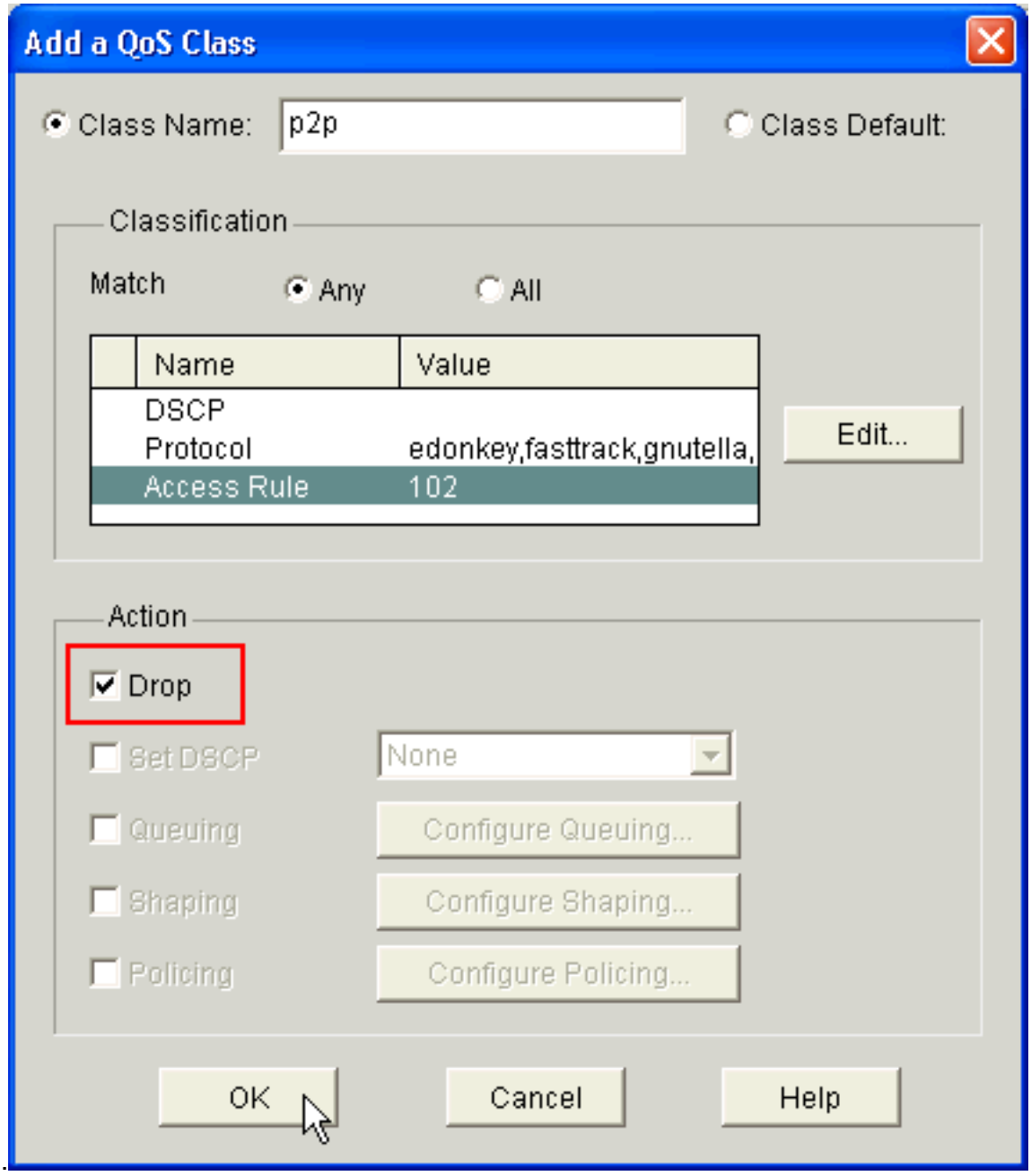
OK.

23. Nella finestra di dialogo Modifica ACL corrispondente, fare clic su



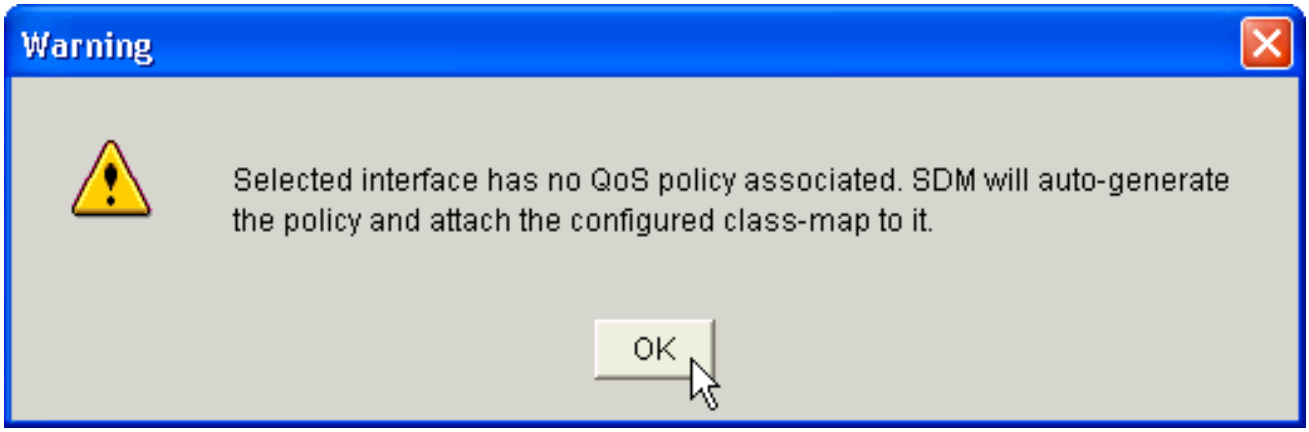
OK.

24. Nella finestra di dialogo Aggiungi classe QoS selezionare la casella di controllo **Drop** per forzare il router a bloccare il traffico



P2P.

25. Fare clic su **OK**.Il seguente messaggio di avviso viene visualizzato per impostazione predefinita quando all'interfaccia non è mappato alcun criterio QoS.

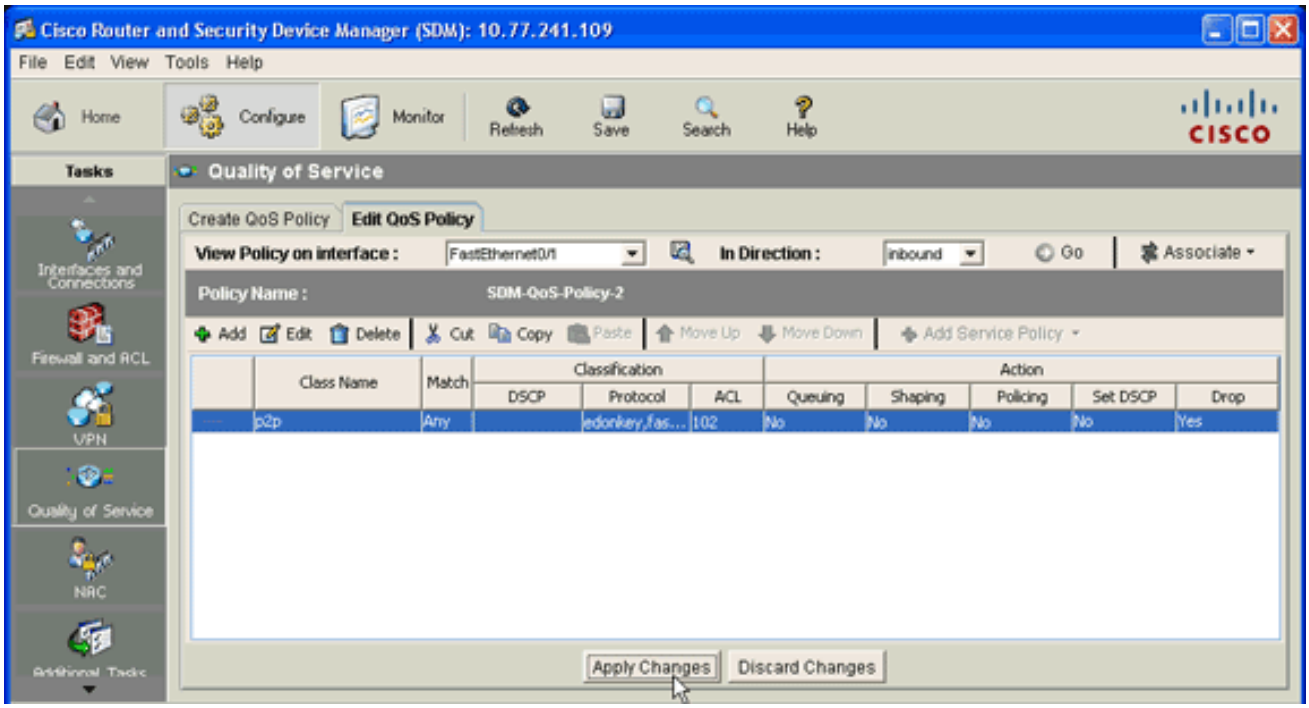


SDM genera automaticamente il criterio QoS e associa al criterio la mappa di classe configurata. L'equivalente dell'interfaccia della riga di comando (CLI) di questo passo di configurazione SDM è:

```
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. Nella scheda Modifica criterio QoS, fare clic su **Apply Changes** (Applica modifiche) per consegnare la configurazione al router.



Application Firewall: funzione di applicazione del traffico di messaggi immediati in Cisco IOS versione 12.4(4)T e successive

Applicazione del traffico di messaggi immediati

La funzione Application Firewall - Instant Message Traffic Enforcement consente agli utenti di definire e applicare un criterio che specifica quali tipi di traffico di messaggistica immediata sono consentiti nella rete. È possibile controllare più messenger (ovvero AOL, YAHOO e MSN) contemporaneamente quando configurati nel **criterio appfw** in **messaggistica immediata applicazione**. Pertanto, è possibile applicare anche le seguenti funzionalità aggiuntive:

- Configurazione delle regole di ispezione firewall
- Ispezione approfondita dei pacchetti del payload (ricerca di servizi quali chat di testo)

Nota: la funzione di imposizione del traffico di messaggi immediati con Application Firewall è supportata in Cisco IOS versione 12.4(4)T e successive.

Criteri applicazione di Instant Messenger

Il firewall dell'applicazione utilizza un criterio dell'applicazione, costituito da un insieme di firme statiche, per rilevare le violazioni della sicurezza. Una firma statica è una raccolta di parametri che specificano le condizioni del protocollo che devono essere soddisfatte prima di eseguire un'azione. Le condizioni e le reazioni del protocollo sono definite dall'utente finale tramite la CLI per formare una policy di applicazione.

Cisco IOS Application Firewall è stato migliorato per supportare i criteri delle applicazioni di

messaggistica immediata nativa. Pertanto, il firewall di Cisco IOS è ora in grado di rilevare e vietare le connessioni degli utenti ai server di messaggistica immediata per AOL Instant Messenger (AIM), Yahoo! Servizi di messaggistica immediata di Messenger e MSN Messenger. Questa funzionalità controlla tutte le connessioni per i servizi supportati, incluse le funzionalità di trasferimento di testo, voce, video e file. Le tre richieste possono essere respinte o autorizzate singolarmente. Ogni servizio può essere controllato singolarmente in modo da consentire l'utilizzo di chat di testo e limitare i servizi voce, trasferimento file, video e di altro tipo. Questa funzionalità aumenta la capacità di ispezione delle applicazioni esistenti per controllare il traffico delle applicazioni di messaggistica immediata (IM) che è stato mascherato come traffico HTTP (Web). per ulteriori informazioni, fare riferimento a Applicazione firewall - Applicazione del traffico di messaggi immediati.

Nota: se un'applicazione IM è bloccata, la connessione viene reimpostata e viene generato un messaggio syslog, come appropriato.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show ip nbar pdlm**: per visualizzare PDLM in uso da NBAR, usare il comando **show ip nbar pdlm** in modalità di esecuzione privilegiata:

```
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**: per visualizzare informazioni sulla versione del software NBAR nella versione Cisco IOS in uso o sulla versione di un PMTUD NBAR sul router Cisco IOS, usare il comando **show ip nbar version** in modalità di esecuzione privilegiata:

```
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](): per visualizzare le statistiche dei pacchetti di tutte le classi configurate per tutti i criteri dei servizi sull'interfaccia o sulla sottointerfaccia specificata o su uno specifico circuito virtuale permanente (PVC) sull'interfaccia, usare il comando **show policy-map interface** in modalità di esecuzione privilegiata:

```
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**: per visualizzare tutte le configurazioni della mappa dei criteri e la configurazione predefinita, usare il comando **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**: per visualizzare le informazioni sulla configurazione della mappa delle classi, usare il comando **show running-config class-map**:

```
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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **show access-list**: per visualizzare la configurazione dell'elenco degli accessi in esecuzione sul router Cisco IOS, usare il 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
```

Informazioni correlate

- Guida alla configurazione della sicurezza di Cisco IOS, supporto versione 12.4
- Riconoscimento applicazioni basato sulla rete (NBAR)
- Cisco Express Forwarding (CEF)
- Documentazione e supporto tecnico – Cisco Systems