# Cisco CP - Configurazione di ZFW per bloccare il traffico peer-to-peer

## Sommario

## Introduzione

Questo documento offre un approccio dettagliato per configurare un router Cisco IOS come firewall basato su zone per bloccare il traffico Peer-to-Peer (P2P) utilizzando la configurazione guidata avanzata del firewall in Cisco Configuration Professional (Cisco CP).

Il firewall di policy basato su zone (noto anche come ZFW, Zone-Policy Firewall) modifica la configurazione del firewall dal precedente modello basato su interfacce a un modello basato su zone più flessibile e di più facile comprensione. Le interfacce vengono assegnate alle zone e i criteri di ispezione vengono applicati al traffico che si sposta tra le zone. Le politiche interzona offrono notevole flessibilità e granularità. Pertanto, è possibile applicare criteri di ispezione diversi a più gruppi host connessi alla stessa interfaccia del router. Le zone definiscono i bordi di protezione della rete. Una zona definisce un limite in cui il traffico è soggetto a restrizioni dei criteri mentre attraversa un'altra area della rete. Il criterio predefinito di ZFW tra le zone è deny all. Se non viene configurato alcun criterio in modo esplicito, tutto il traffico in movimento tra le zone verrà bloccato.

Le applicazioni P2P sono tra le applicazioni più utilizzate su Internet. Le reti P2P possono fungere da canale per le minacce dannose come i worm, offrendo un percorso semplice intorno ai firewall e causando preoccupazioni sulla privacy e la sicurezza. Il software Cisco IOS versione 12.4(9)T ha introdotto il supporto ZFW per le applicazioni P2P. L'ispezione P2P offre policy di layer 4 e layer 7 per il traffico delle applicazioni. Ciò significa che ZFW può fornire un'ispezione stateful di base per autorizzare o negare il traffico, così come un controllo granulare di layer 7 su attività specifiche nei vari protocolli, in modo che alcune attività dell'applicazione siano consentite mentre altre vengono negate.

Cisco CP offre un approccio semplice e dettagliato per configurare il router IOS come firewall basato su zone tramite la configurazione guidata avanzata del firewall.

# Prerequisiti

## Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- La versione software del router IOS deve essere 12.4(9)T o successiva.
- Per i modelli di router IOS che supportano Cisco CP, consultare le note di rilascio di Cisco CP.

## Configurazione del router per eseguire Cisco CP

**Nota:** per eseguire Cisco CP su un router Cisco, eseguire la configurazione seguente:

```
Router(config)# ip http server
Router(config)# ip http secure-server
Router(config)# ip http authentication local
Router(config)# username <username> privilege 15 password 0 <password>
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

## Componenti usati

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

- Router Cisco 1841 IOS con software IOS versione 12.4(15)T
- Cisco Configuration Professional (Cisco CP) release 2.1

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

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

# Premesse

Nell'esempio di questo documento, il router è configurato come firewall basato su zona per bloccare il traffico P2P. Il router ZFW ha due interfacce, un'interfaccia interna (trusted) in-zone e un'interfaccia esterna (untrusted) in Out-zone. Il router ZFW blocca le applicazioni P2P come edonkey, fasttrack, gnutella e kazaa2 con azioni di logging per il traffico che passa da In-zone a Out-zone.

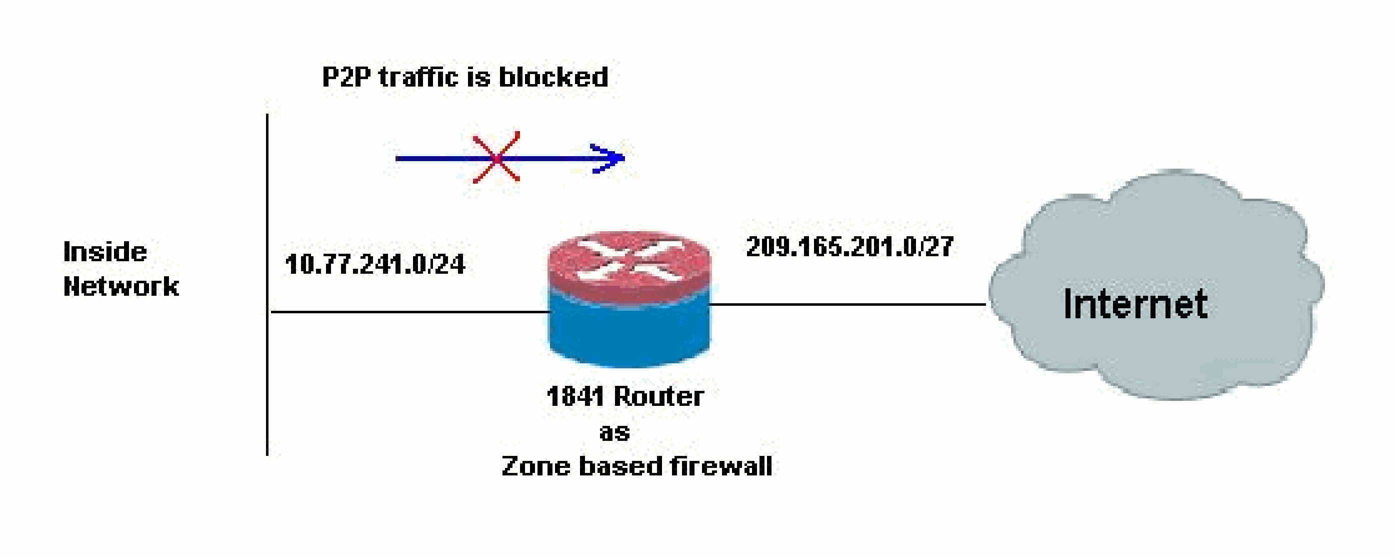
# Configurazione

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

**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:

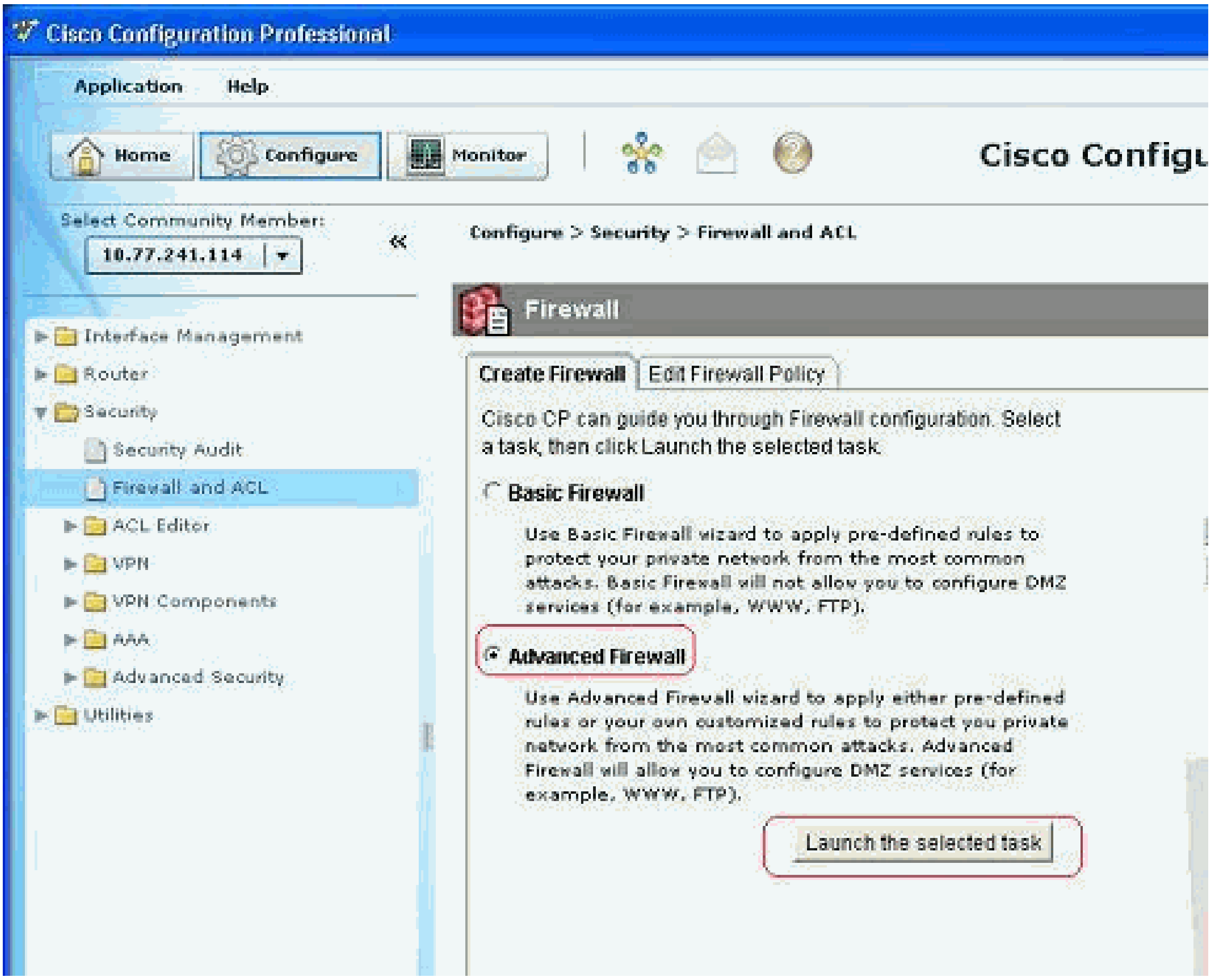


# Configurazione tramite Cisco Configuration Professional

In questa sezione viene descritto come usare la procedura guidata per configurare il router IOS come firewall basato su zone.

Attenersi alla seguente procedura:

1. Selezionare **Configure > Security > Firewall and ACL** (Configura > Sicurezza > Firewall e ACL). Quindi, scegliere il pulsante di opzione **Advanced Firewall**. Fare clic su **Avvia l'attività selezionata**.



Cisco CP can guide you through Firewall configuration. Select a task, then click Launch the selected task.

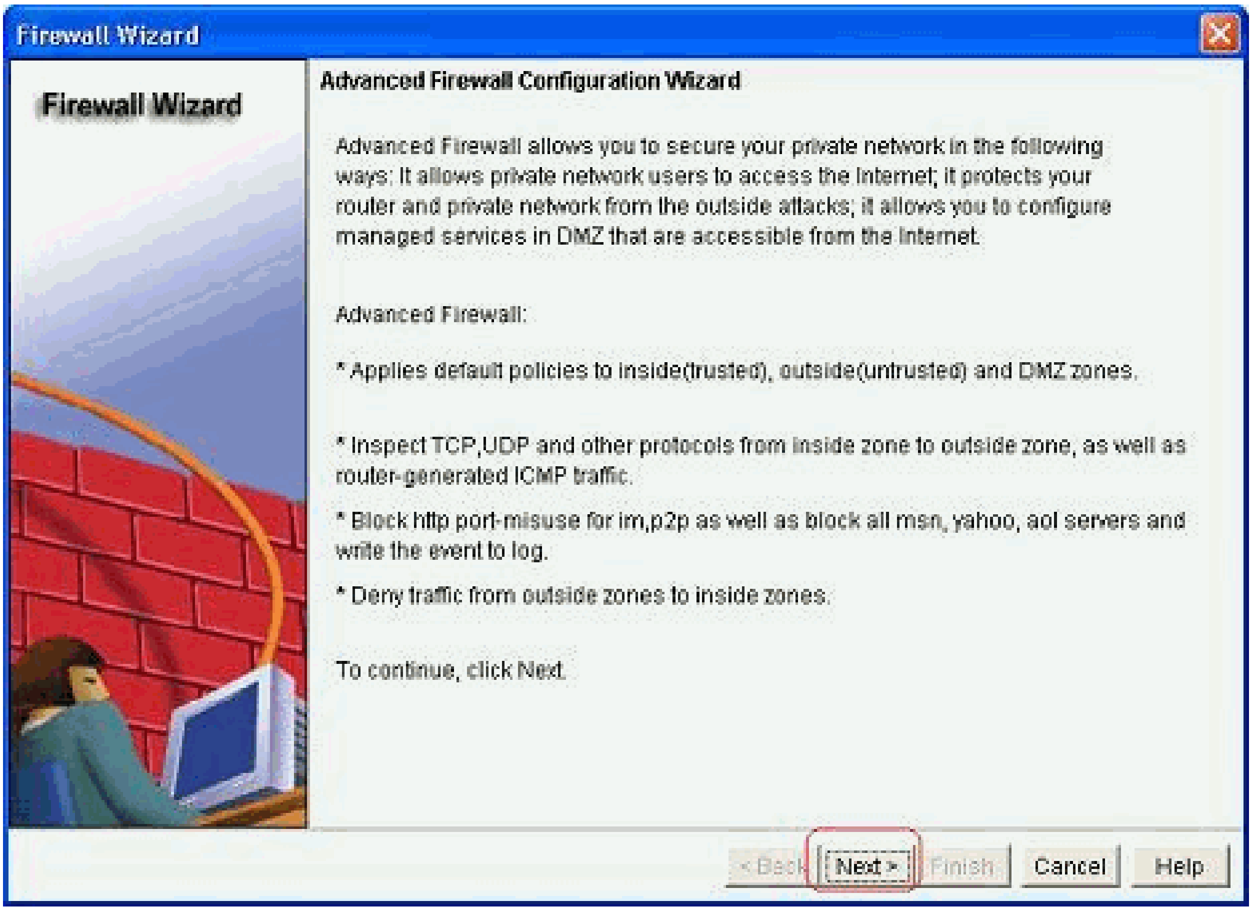
○ Basic Firewall

Use Basic Firewall wizard to apply pre-defined rules to protect your private network from the most common attacks. Basic Firewall will not allow you to configure DMZ services (for example, WWW, FTP).

● Advanced Firewall

Use Advanced Firewall wizard to apply either pre-defined rules or your own customized rules to protect you private network from the most common attacks. Advanced Firewall will allow you to configure DMZ services (for example, WWW, FTP).

2. In questa schermata successiva viene visualizzata una breve introduzione alla Creazione guidata Firewall. Fare clic su **Avanti** per avviare la configurazione del firewall.



Advanced Firewall Configuration Wizard

Advanced Firewall allows you to secure your private network in the following ways: It allows private network users to access the Internet; it protects your router and private network from the outside attacks; it allows you to configure managed services in DMZ that are accessible from the Internet.

Advanced Firewall:

* Applies default policies to inside(trusted), outside(untrusted) and DMZ zones.

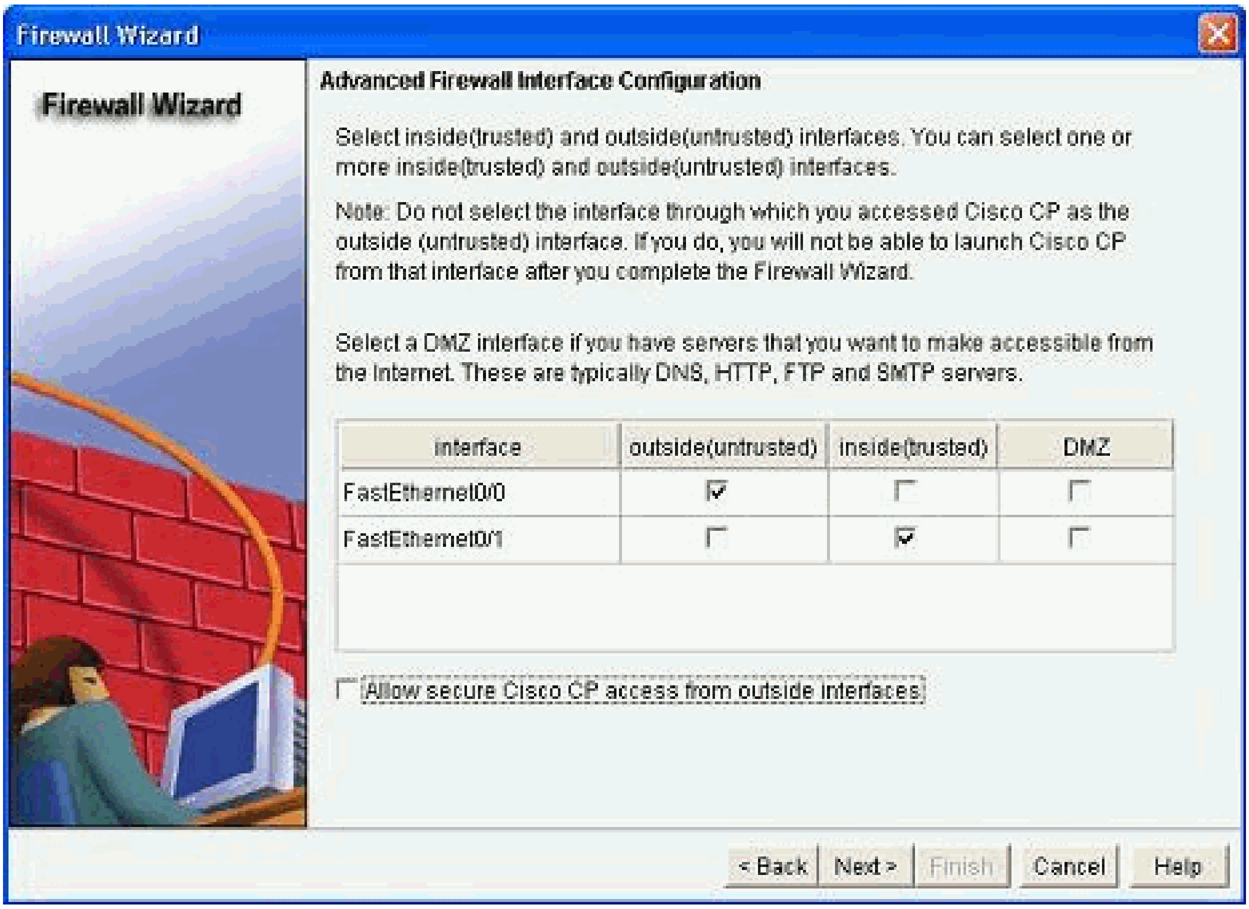
* Inspect TCP,UDP and other protocols from inside zone to outside zone, as well as router-generated ICMP traffic.

* Block http port-misuse for im,p2p as well as block all msn, yahoo, aol servers and write the event to log.

* Deny traffic from outside zones to inside zones.

To continue, click Next.

3. Selezionare le interfacce del router che devono far parte delle zone e fare clic su **Avanti**.



Advanced Firewall Interface Configuration

Select inside(trusted) and outside(untrusted) interfaces. You can select one or more inside(trusted) and outside(untrusted) interfaces.

Note: Do not select the interface through which you accessed Cisco CP as the outside (untrusted) interface. If you do, you will not be able to launch Cisco CP from that interface after you complete the Firewall Wizard.

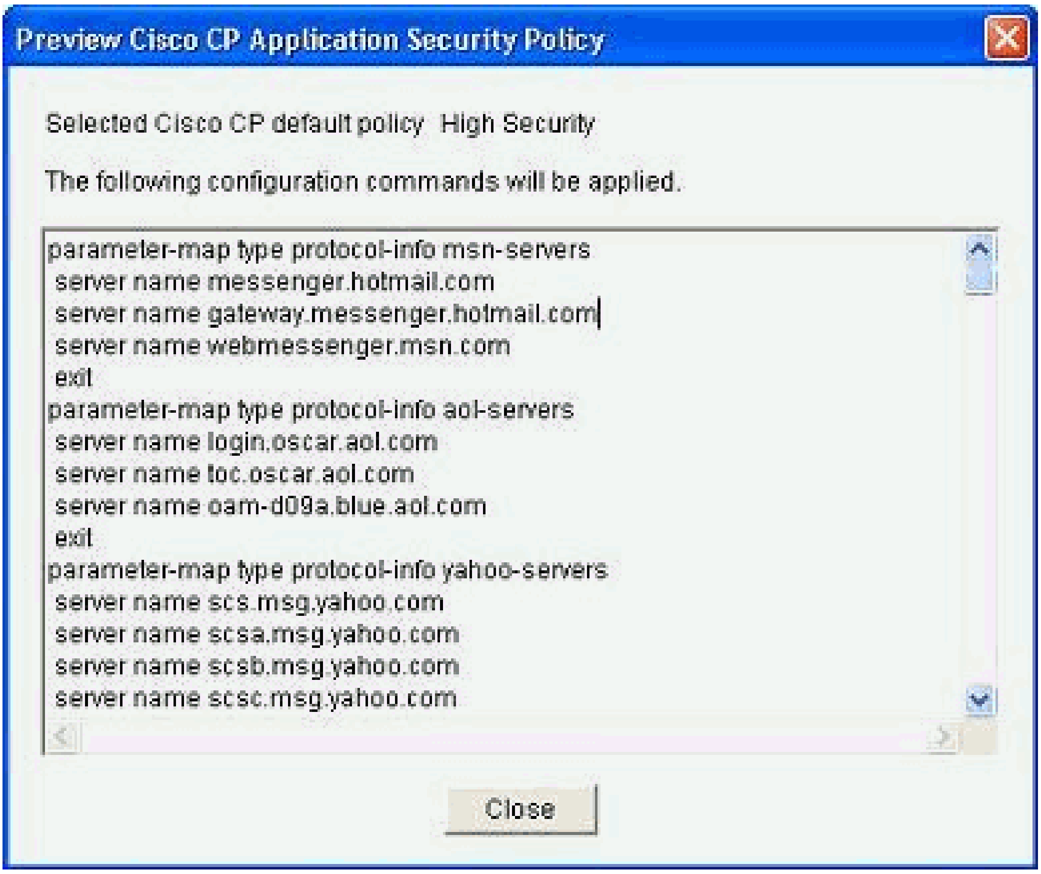
Select a DMZ interface if you have servers that you want to make accessible from the Internet. These are typically DNS, HTTP, FTP and SMTP servers.

| interface | outside(untrusted) | inside(trusted) | DMZ |
|---|---|---|---|
| FastEthernet0/0 | ☑ | □ | □ |
| FastEthernet0/1 | □ | ☑ | □ |

□ Allow secure Cisco CP access from outside interfaces

4. Nella finestra successiva vengono visualizzati il criterio predefinito con protezione elevata insieme all'insieme di comandi. Fare clic su **Close** (Chiudi) per

continuare.



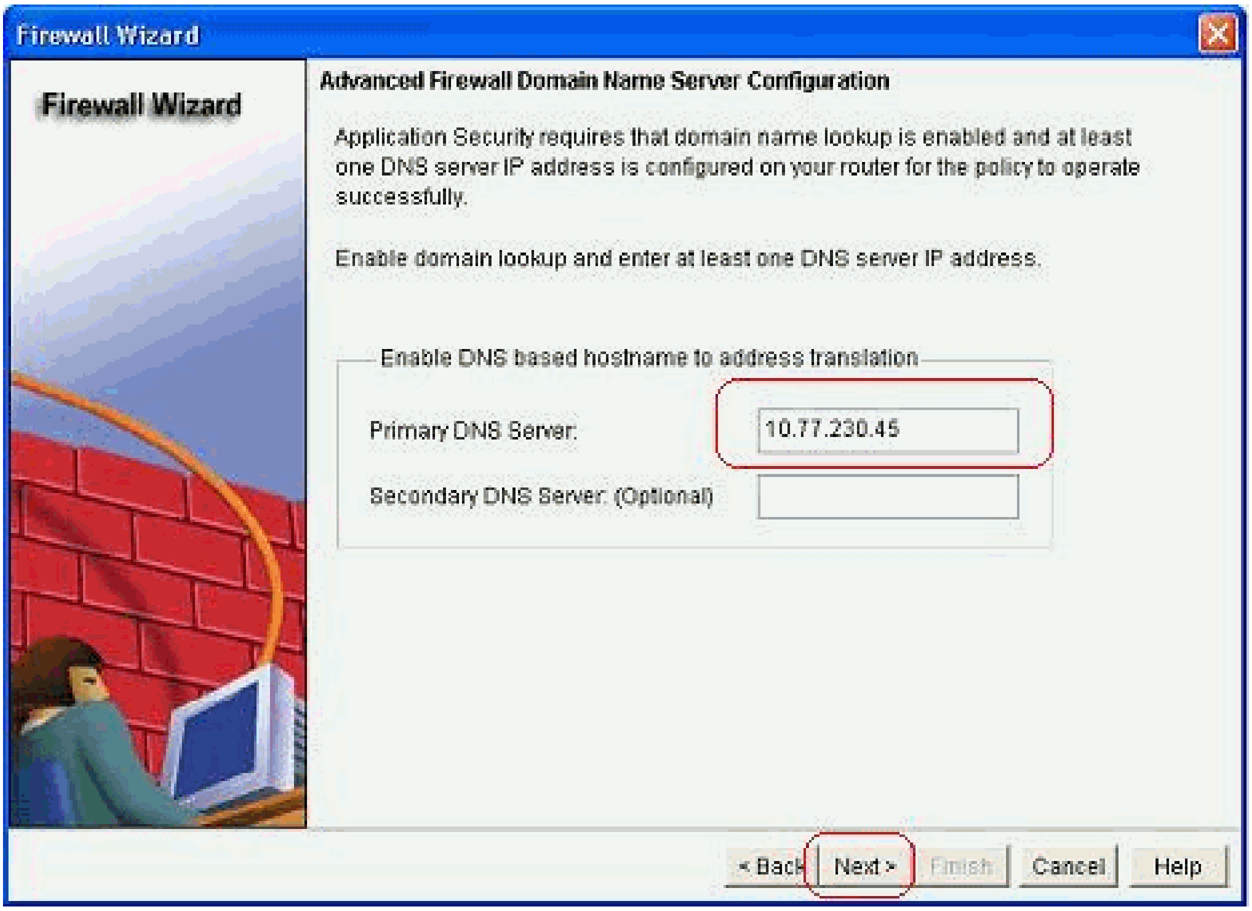
Preview Cisco CP Application Security Policy

Selected Cisco CP default policy  High Security

The following configuration commands will be applied.

```
parameter-map type protocol-info msn-servers
 server name messenger.hotmail.com
 server name gateway.messenger.hotmail.com
 server name webmessenger.msn.com
 exit
parameter-map type protocol-info aol-servers
 server name login.oscar.aol.com
 server name toc.oscar.aol.com
 server name oam-d09a.blue.aol.com
 exit
parameter-map type protocol-info yahoo-servers
 server name scs.msg.yahoo.com
 server name scsa.msg.yahoo.com
 server name scsb.msg.yahoo.com
 server name scsc.msg.yahoo.com
```

5. Immettere i dettagli del server DNS e fare clic su **Avanti**.



Firewall Wizard

Advanced Firewall Domain Name Server Configuration

Application Security requires that domain name lookup is enabled and at least one DNS server IP address is configured on your router for the policy to operate successfully.

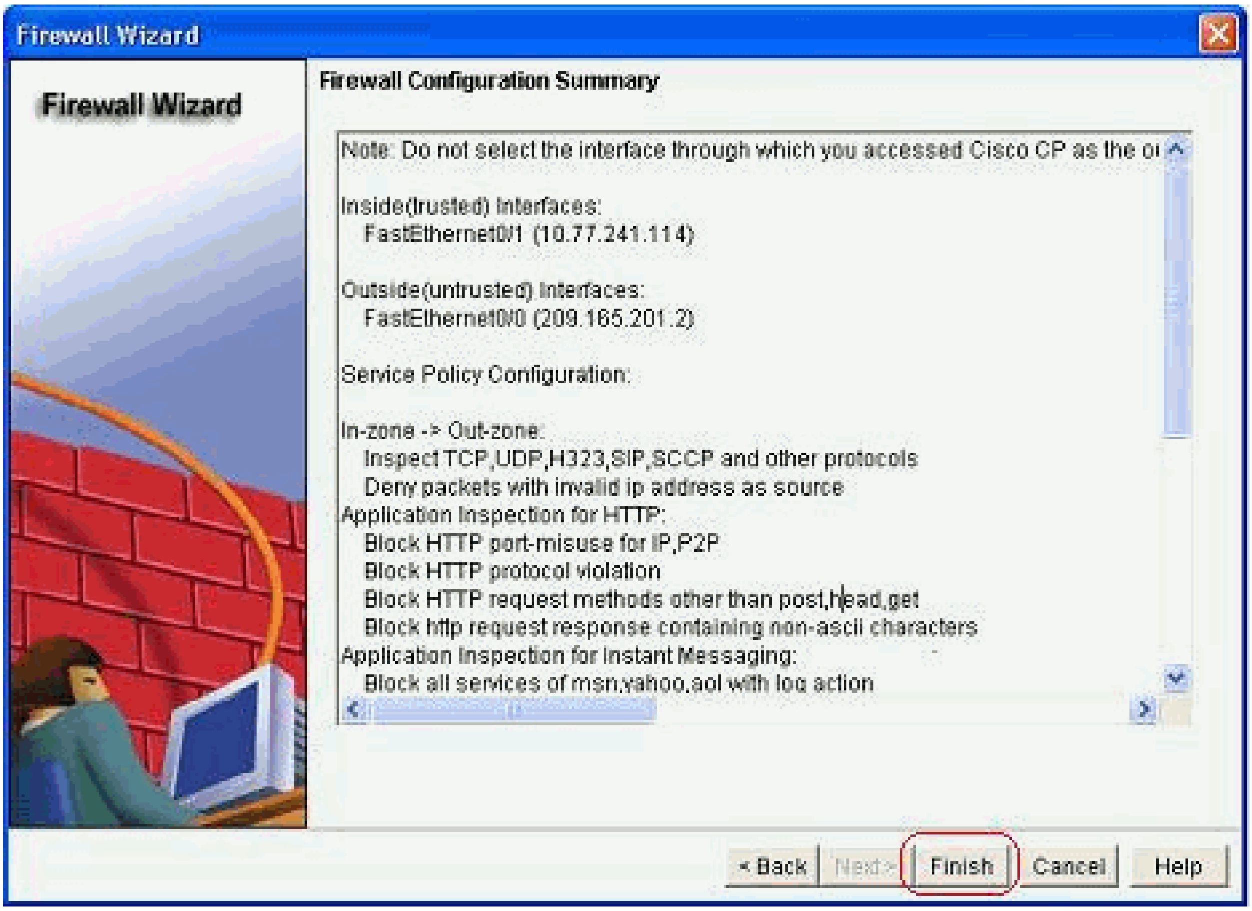
Enable domain lookup and enter at least one DNS server IP address.

Enable DNS based hostname to address translation

Primary DNS Server: 10.77.230.45

Secondary DNS Server: (Optional)

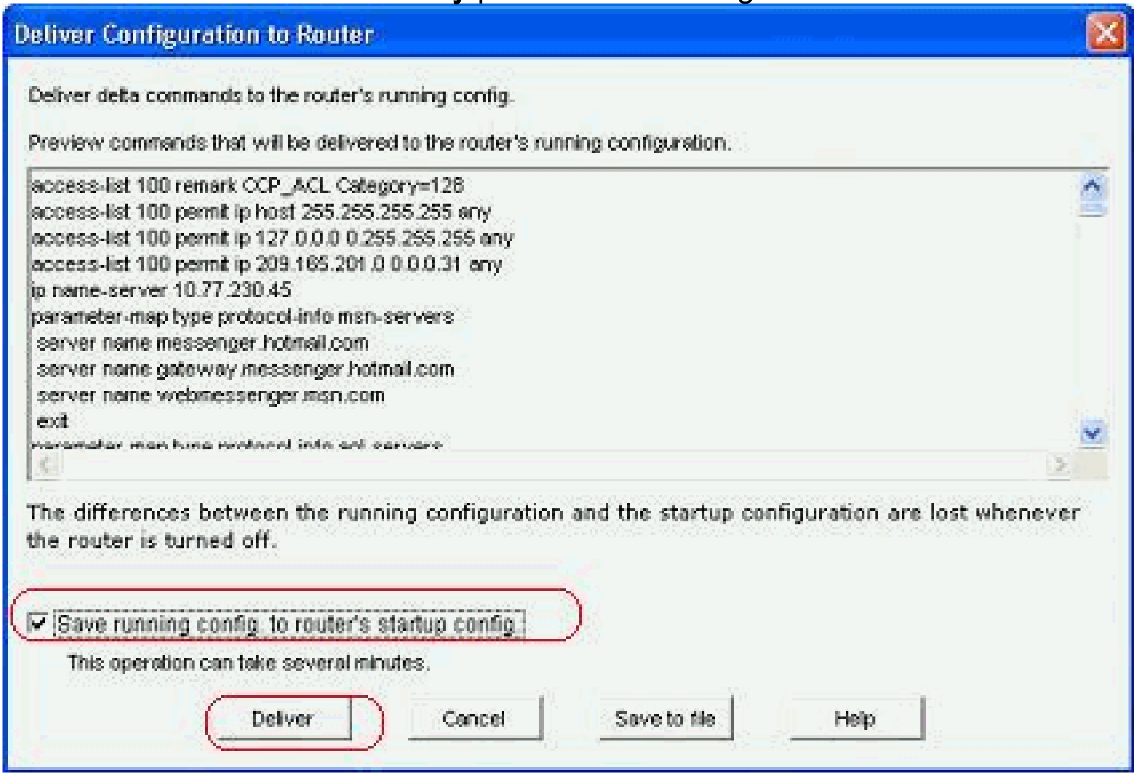
6. Cisco CP fornisce un riepilogo della configurazione come quello mostrato di seguito. Fare clic su **Fine** per completare la configurazione.



```
Note: Do not select the interface through which you accessed Cisco CP as the o

Inside(trusted) Interfaces:
   FastEthernet0/1 (10.77.241.114)

Outside(untrusted) Interfaces:
   FastEthernet0/0 (209.165.201.2)

Service Policy Configuration:

In-zone -> Out-zone:
   Inspect TCP,UDP,H323,SIP,SCCP and other protocols
   Deny packets with invalid ip address as source
Application Inspection for HTTP:
   Block HTTP port-misuse for IP,P2P
   Block HTTP protocol violation
   Block HTTP request methods other than post,head,get
   Block http request response containing non-ascii characters
Application Inspection for Instant Messaging:
   Block all services of msn,yahoo,aol with log action
```

In questa tabella viene fornito il riepilogo dettagliato della configurazione. Questa è la configurazione predefinita in base ai criteri di sicurezza elevata di Cisco CP.

7. Selezionare la casella di controllo **Salva la configurazione in esecuzione nella configurazione di avvio del router.** Fare clic su **Delivery** per inviare la configurazione al



Deliver delta commands to the router's running config.

Preview commands that will be delivered to the router's running configuration.

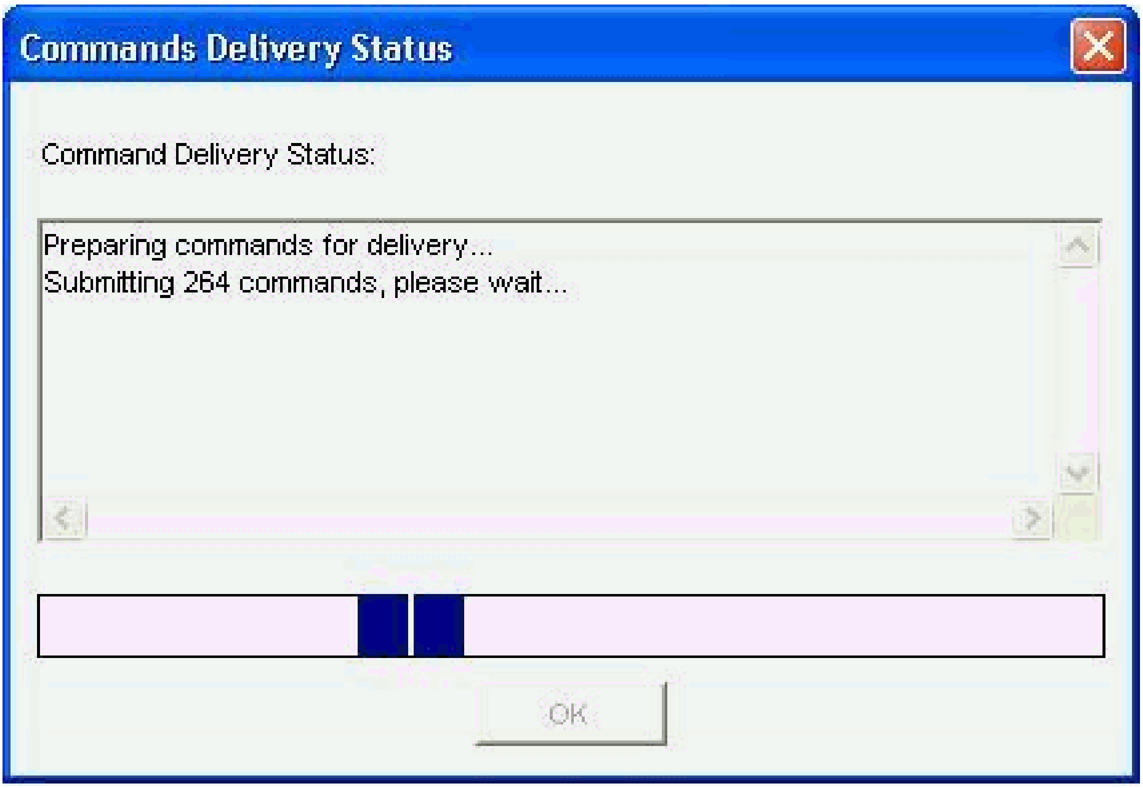
```
access-list 100 remark CCP_ACL Category=128
access-list 100 permit ip host 255.255.255.255 any
access-list 100 permit ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip 209.165.201.0 0.0.0.31 any
ip name-server 10.77.230.45
parameter-map type protocol-info msn-servers
 server name messenger.hotmail.com
 server name gateway.messenger.hotmail.com
 server name webmessenger.msn.com
 exit
parameter-map type protocol-info aol-servers
```

The differences between the running configuration and the startup configuration are lost whenever the router is turned off.

☑ Save running config. to router's startup config.

This operation can take several minutes.

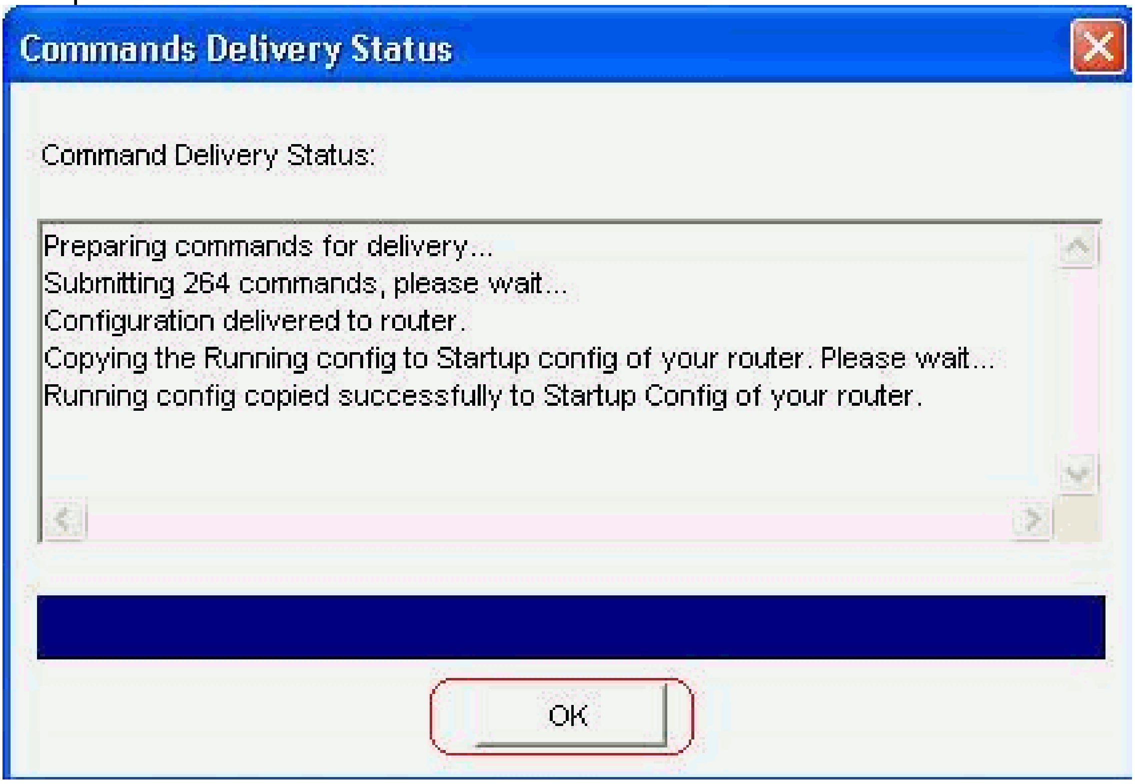
router. L'intera configurazione viene consegnata al router. L'elaborazione richiede del



```
Preparing commands for delivery...
Submitting 264 commands, please wait...
```

tempo.

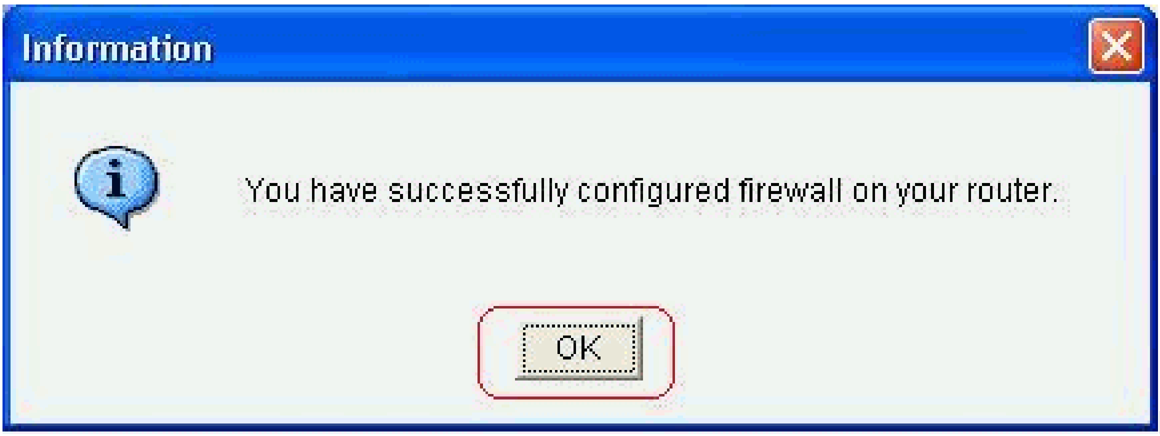
8. Fare clic su **OK** per



```
Preparing commands for delivery...
Submitting 264 commands, please wait...
Configuration delivered to router.
Copying the Running config to Startup config of your router. Please wait...
Running config copied successfully to Startup Config of your router.
```

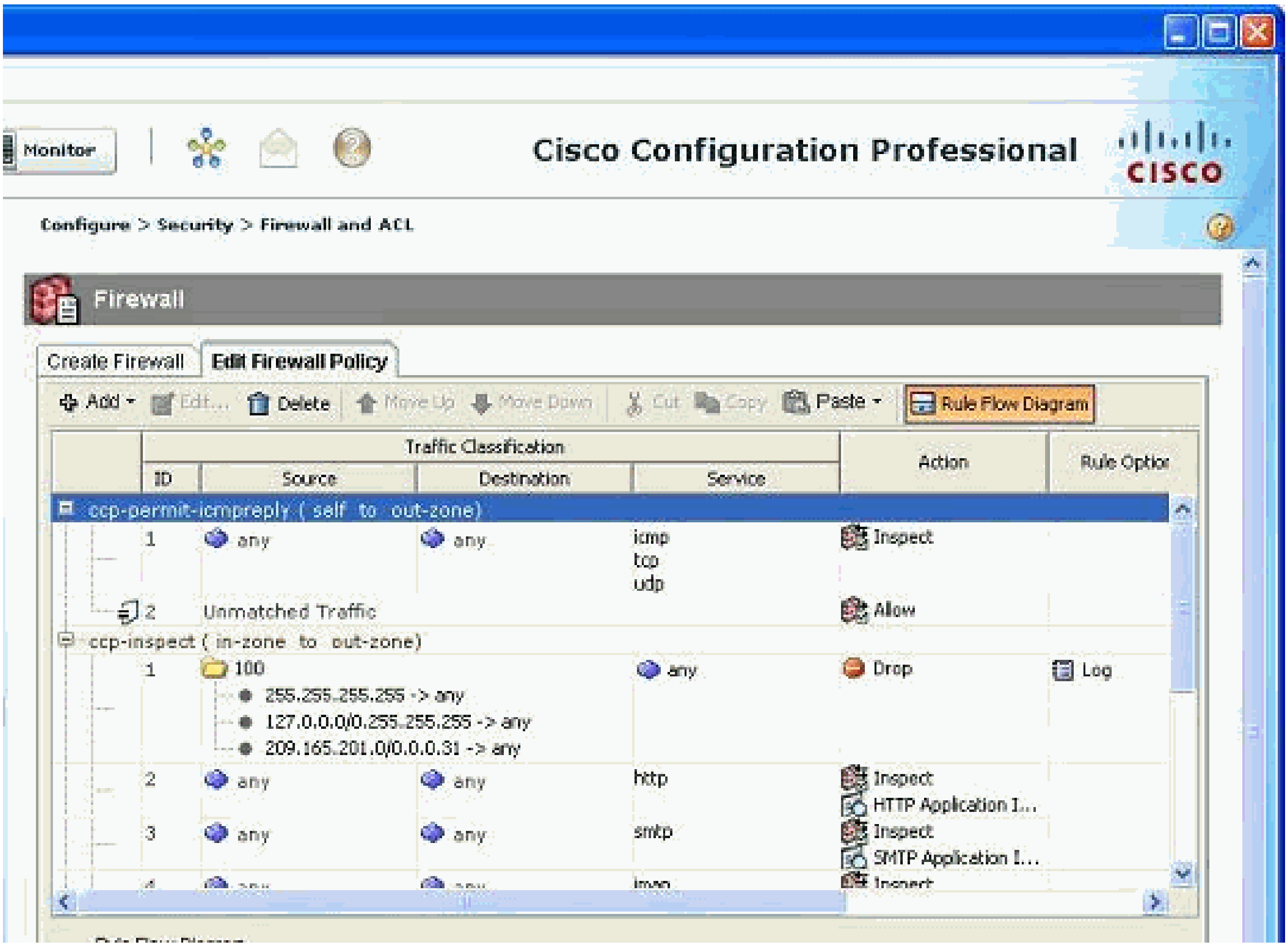
continuare.

9. Fare nuovamente clic su



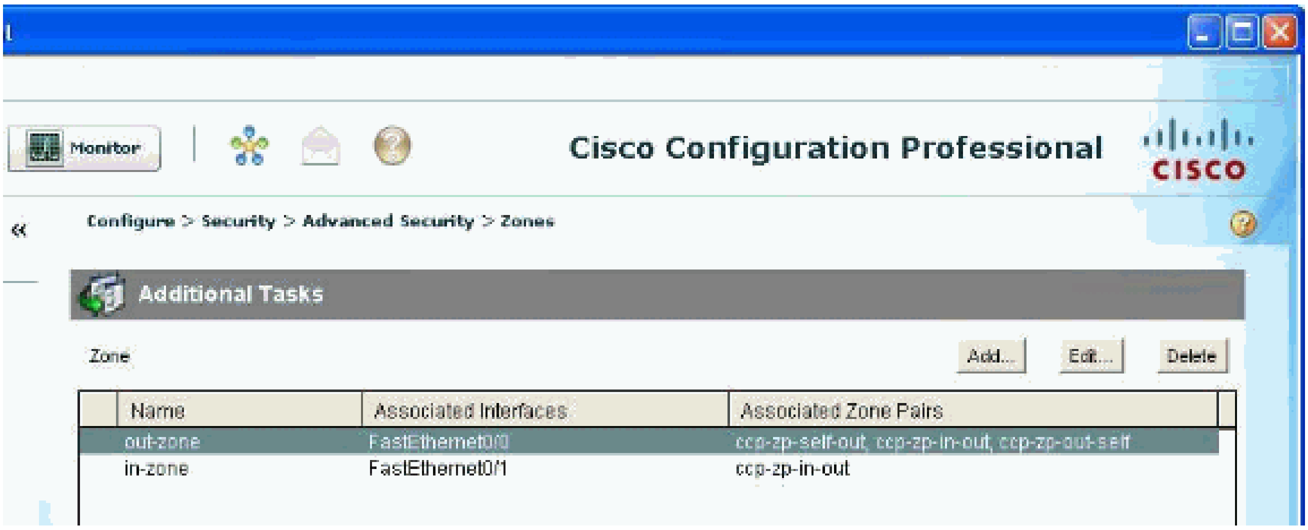
You have successfully configured firewall on your router.

OK. La configurazione è ora attiva e viene visualizzata come regole nella scheda Criteri firewall.



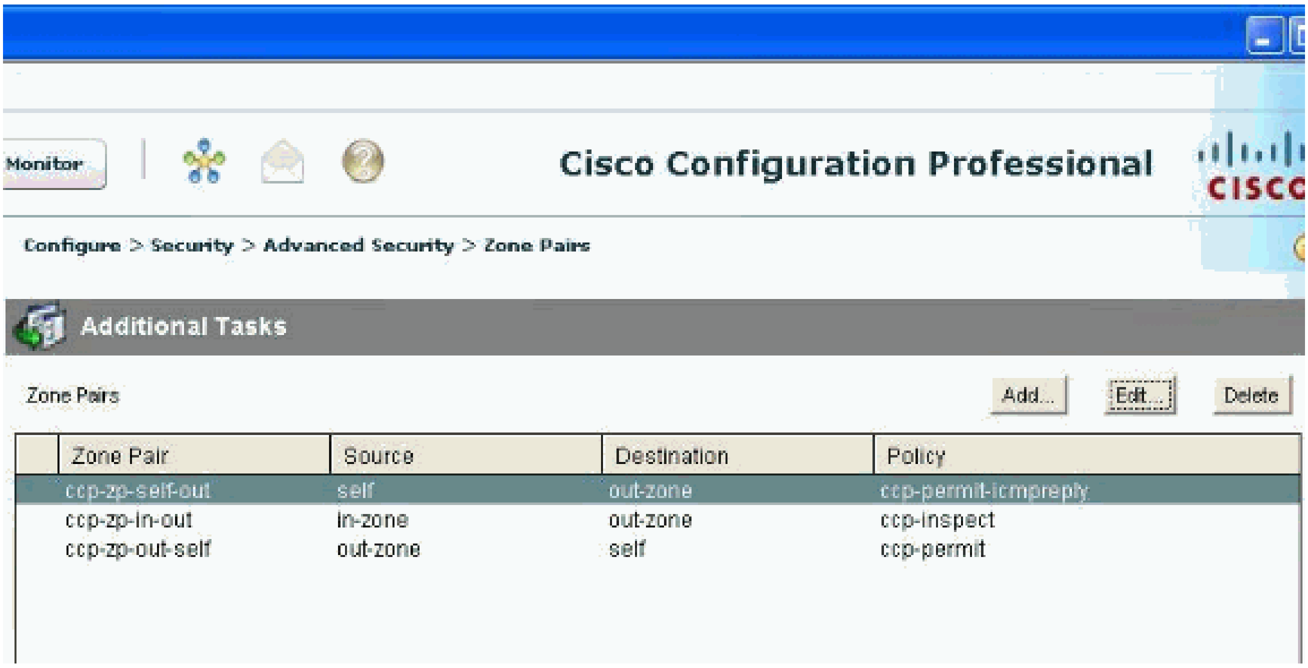
| ID | Source | Destination | Service | Action | Rule Option |
|---|---|---|---|---|---|
| ccp-permit-icmpreply ( self to out-zone) | | | | | |
| 1 | any | any | icmp<br>tcp<br>udp | Inspect | |
| 2 | Unmatched Traffic | | | Allow | |
| ccp-inspect ( in-zone to out-zone) | | | | | |
| 1 | 100<br>255.255.255.255 -> any<br>127.0.0.0/0.255.255.255 -> any<br>209.165.201.0/0.0.0.31 -> any | | any | Drop | Log |
| 2 | any | any | http | Inspect<br>HTTP Application I... | |
| 3 | any | any | smtp | Inspect<br>SMTP Application I... | |
| 4 | any | any | imap | Inspect | |

10. Le zone e le coppie di zone associate possono essere visualizzate se si sceglie **Configura > Sicurezza > Sicurezza avanzata > Zone**. È inoltre possibile aggiungere nuove zone facendo clic su **Aggiungi** oppure modificare le zone esistenti facendo clic su **Modifica**.


Monitor
Cisco Configuration Professional
cisco
Configure > Security > Advanced Security > Zones
Additional Tasks
Zone
Add...
Edit...
Delete

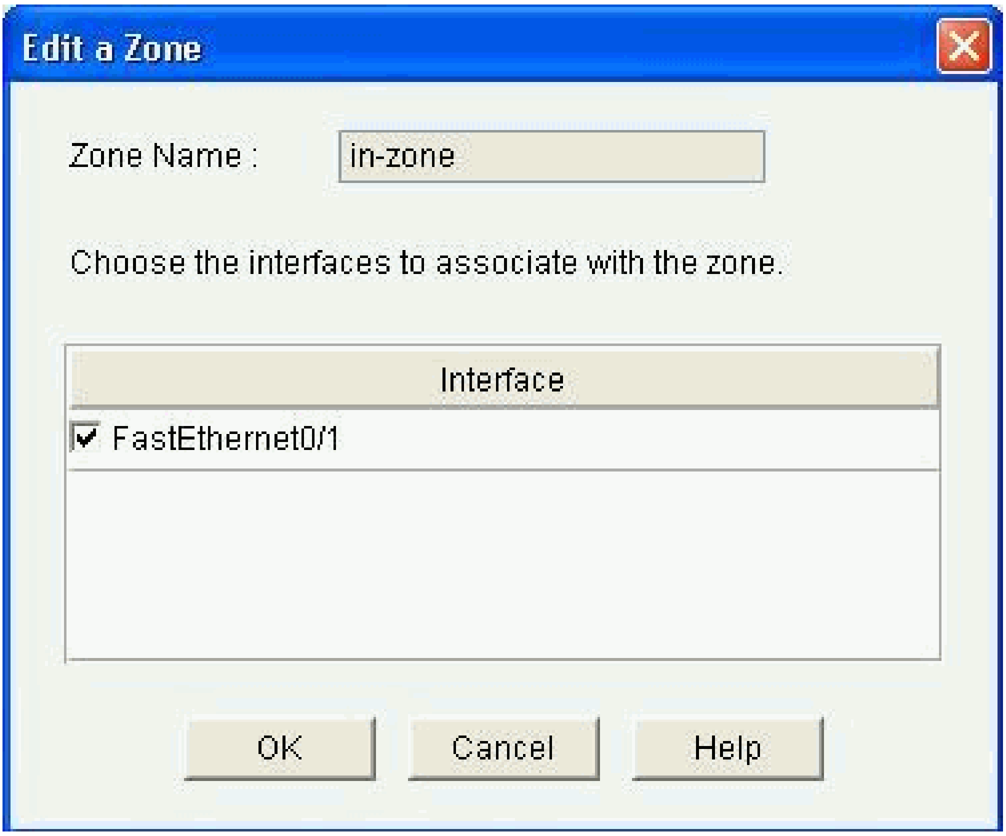
| Name | Associated Interfaces | Associated Zone Pairs |
|---|---|---|
| out-zone | FastEthernet0/0 | ccp-zp-self-out, ccp-zp-in-out, ccp-zp-out-self |
| in-zone | FastEthernet0/1 | ccp-zp-in-out |

11. Selezionare **Configura > Protezione > Protezione avanzata > Coppie di zone** per visualizzare i dettagli delle coppie di zone.


Monitor
Cisco Configuration Professional
cisco
Configure > Security > Advanced Security > Zone Pairs
Additional Tasks
Zone Pairs
Add...
Edit...
Delete

| Zone Pair | Source | Destination | Policy |
|---|---|---|---|
| ccp-zp-self-out | self | out-zone | ccp-permit-icmpreply |
| ccp-zp-in-out | in-zone | out-zone | ccp-inspect |
| ccp-zp-out-self | out-zone | self | ccp-permit |

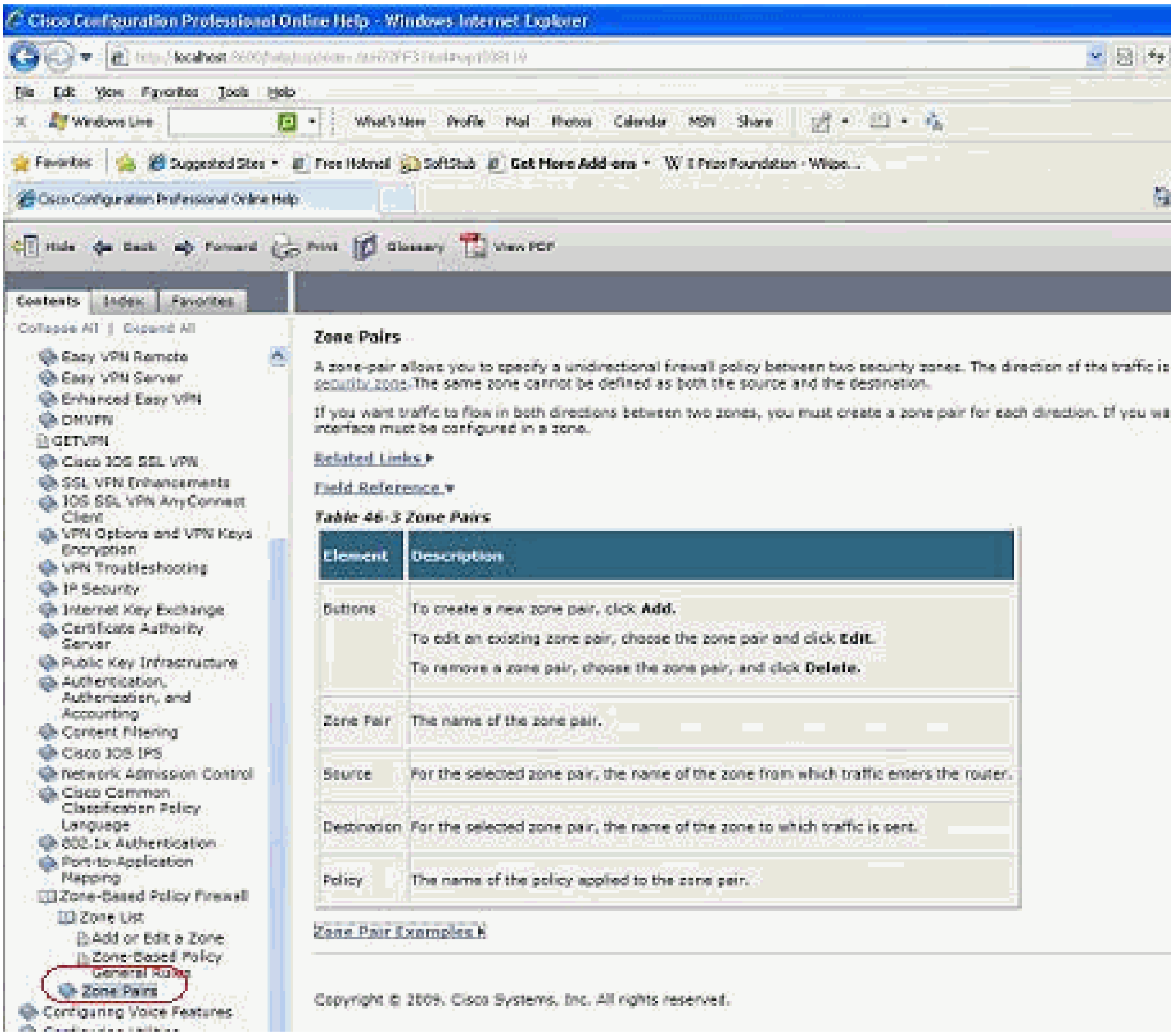
Le pagine Web incorporate nel Cisco CP offrono assistenza immediata per modificare/aggiungere/eliminare coppie di zone/zone e altre informazioni correlate.



Zone Name : in-zone

Choose the interfaces to associate with the zone.

☑ FastEthernet0/1


Cisco Configuration Professional Online Help - Windows Internet Explorer
File Edit View Favorites Tools Help
Hide Back Forward Print Glossary View PDF
Contents Index Favorites
Collapse All | Expand All
Easy VPN Remote
Easy VPN Server
Enhanced Easy VPN
DMVPN
GETVPN
Cisco IOS SSL VPN
SSL VPN Enhancements
IOS SSL VPN AnyConnect Client
VPN Options and VPN Keys Encryption
VPN Troubleshooting
IP Security
Internet Key Exchange
Certificate Authority Server
Public Key Infrastructure
Authentication, Authorization, and Accounting
Content Filtering
Cisco IOS IPS
Network Admission Control
Cisco Common Classification Policy Language
802.1x Authentication
Port-to-Application Mapping
Zone-Based Policy Firewall
Zone List
Add or Edit a Zone
Zone-Based Policy General Rules
Zone Pairs
Configuring Voice Features

**Zone Pairs**

A zone-pair allows you to specify a unidirectional firewall policy between two security zones. The direction of the traffic is
security zone. The same zone cannot be defined as both the source and the destination.

If you want traffic to flow in both directions between two zones, you must create a zone pair for each direction. If you wa
interface must be configured in a zone.

Related Links ▸

Field Reference ▾

*Table 46-3 Zone Pairs*

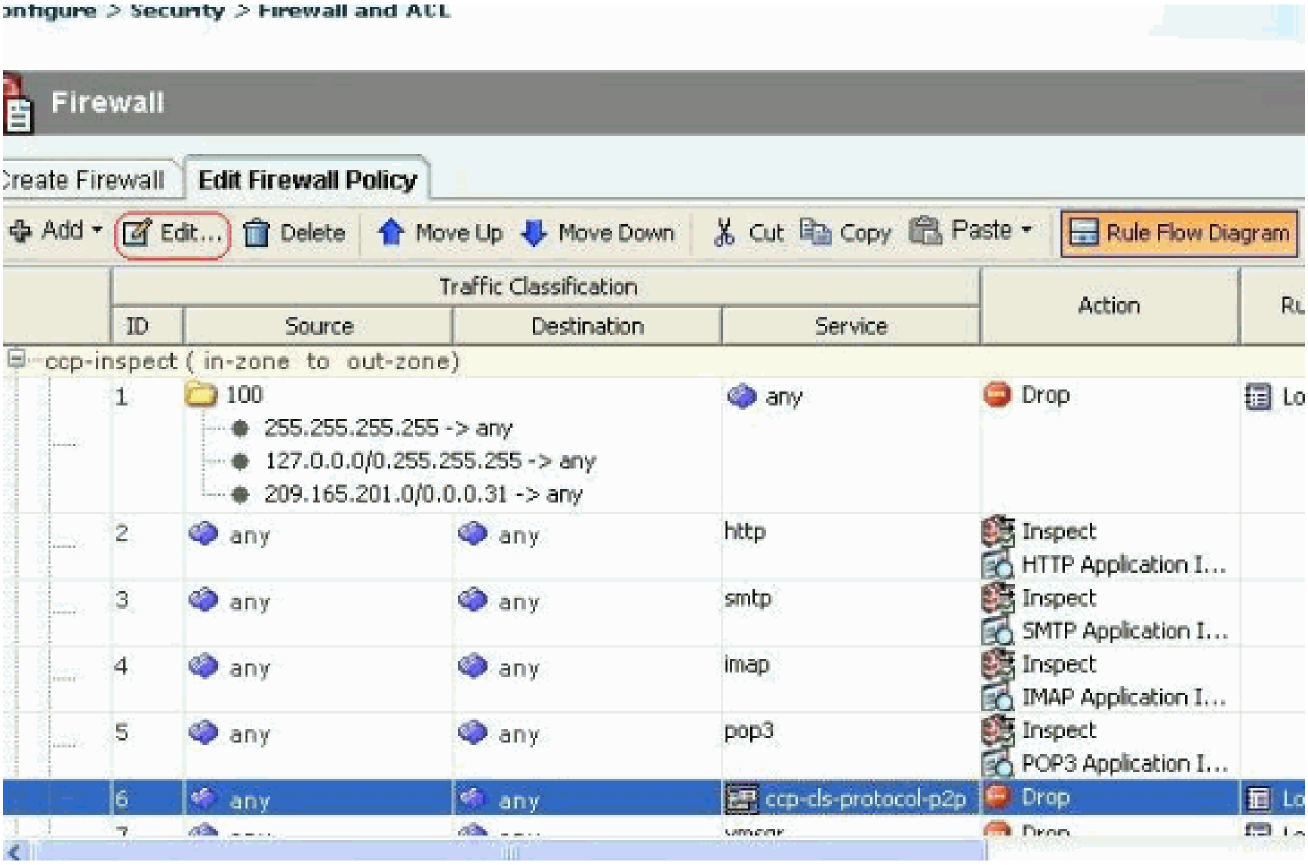
| Element | Description |
|---|---|
| Buttons | To create a new zone pair, click **Add.**<br>To edit an existing zone pair, choose the zone pair and click **Edit.**<br>To remove a zone pair, choose the zone pair, and click **Delete.** |
| Zone Pair | The name of the zone pair. |
| Source | For the selected zone pair, the name of the zone from which traffic enters the router. |
| Destination | For the selected zone pair, the name of the zone to which traffic is sent. |
| Policy | The name of the policy applied to the zone pair. |

Zone Pair Examples ▸

Copyright © 2009, Cisco Systems, Inc. All rights reserved.

12. Per modificare le funzionalità di ispezione specifiche di alcune applicazioni P2P, selezionare **Configurazione > Sicurezza > Firewall e ACL**. Quindi, fare clic su **Modifica criterio firewall** e scegliere la regola corrispondente nella mappa dei criteri. Fare clic su

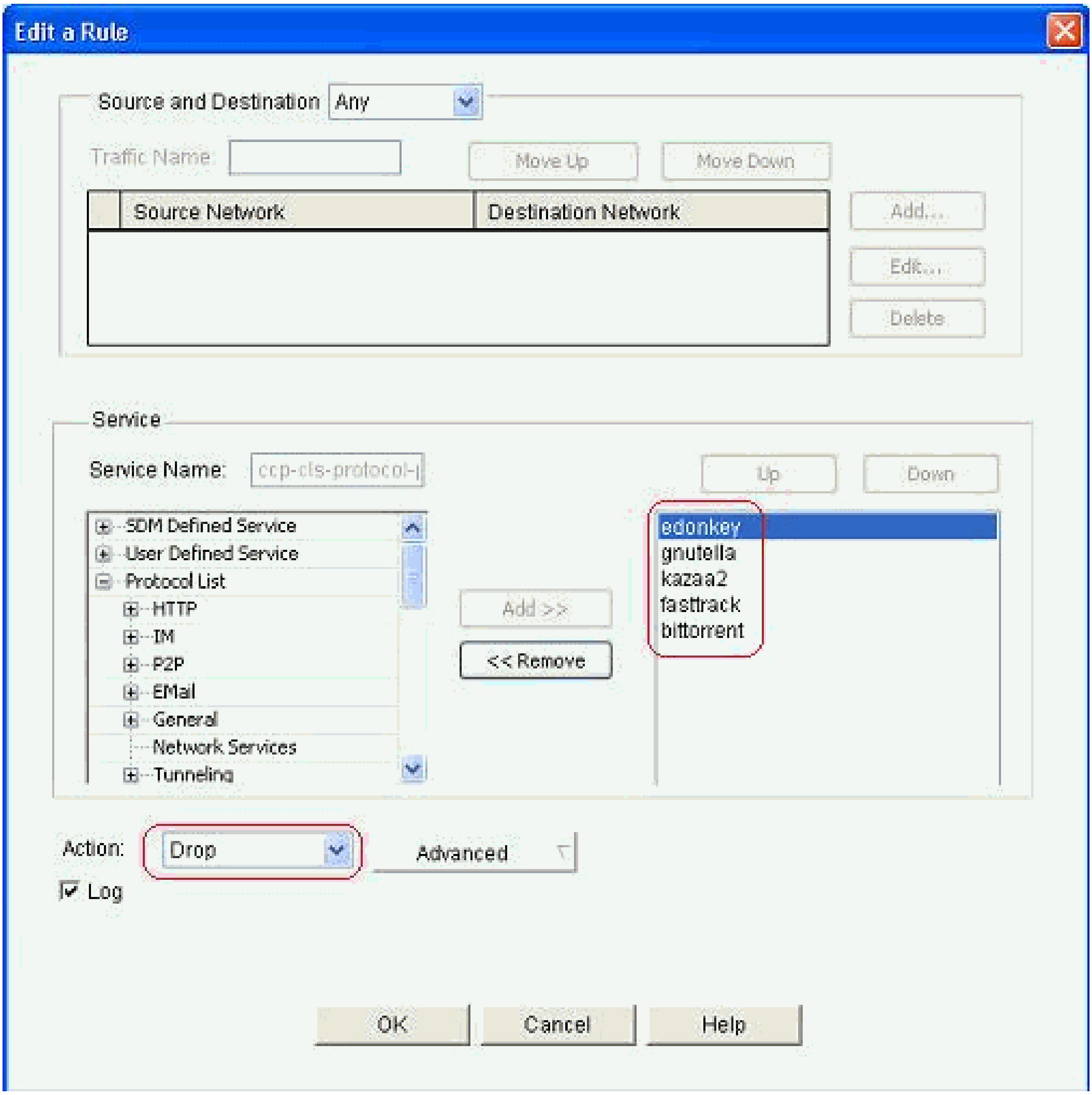
Modifica.



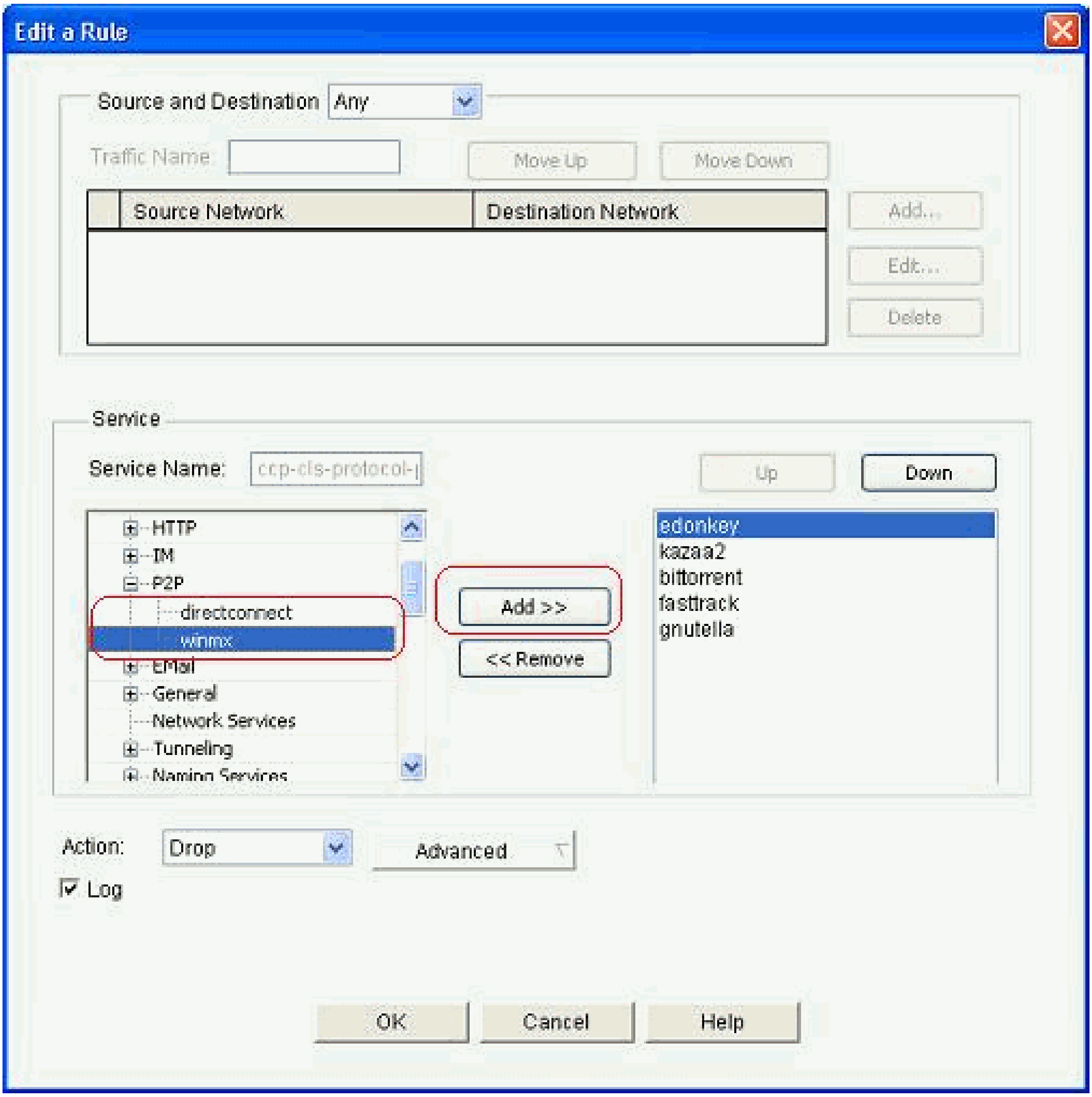
ccp-inspect ( in-zone to out-zone)

| Traffic Classification | | | | Action | Ru |
|---|---|---|---|---|---|
| ID | Source | Destination | Service | | |
| 1 | 100<br>255.255.255.255 -> any<br>127.0.0.0/0.255.255.255 -> any<br>209.165.201.0/0.0.0.31 -> any | | any | Drop | Lo |
| 2 | any | any | http | Inspect<br>HTTP Application I... | |
| 3 | any | any | smtp | Inspect<br>SMTP Application I... | |
| 4 | any | any | imap | Inspect<br>IMAP Application I... | |
| 5 | any | any | pop3 | Inspect<br>POP3 Application I... | |
| 6 | any | any | ccp-cls-protocol-p2p | Drop | Lo |
| 7 | any | any | ymsgr | Drop | Lo |

In questo modo vengono visualizzate le applicazioni P2P correnti che verranno bloccate per impostazione
predefinita.



13. Èpossibile utilizzare i pulsanti Aggiungi e Rimuovi per aggiungere/rimuovere applicazioni specifiche. In questa schermata viene illustrato come aggiungere l'applicazione winmx per bloccarla.



Source and Destination: Any

Traffic Name:

| Source Network | Destination Network |
|---|---|

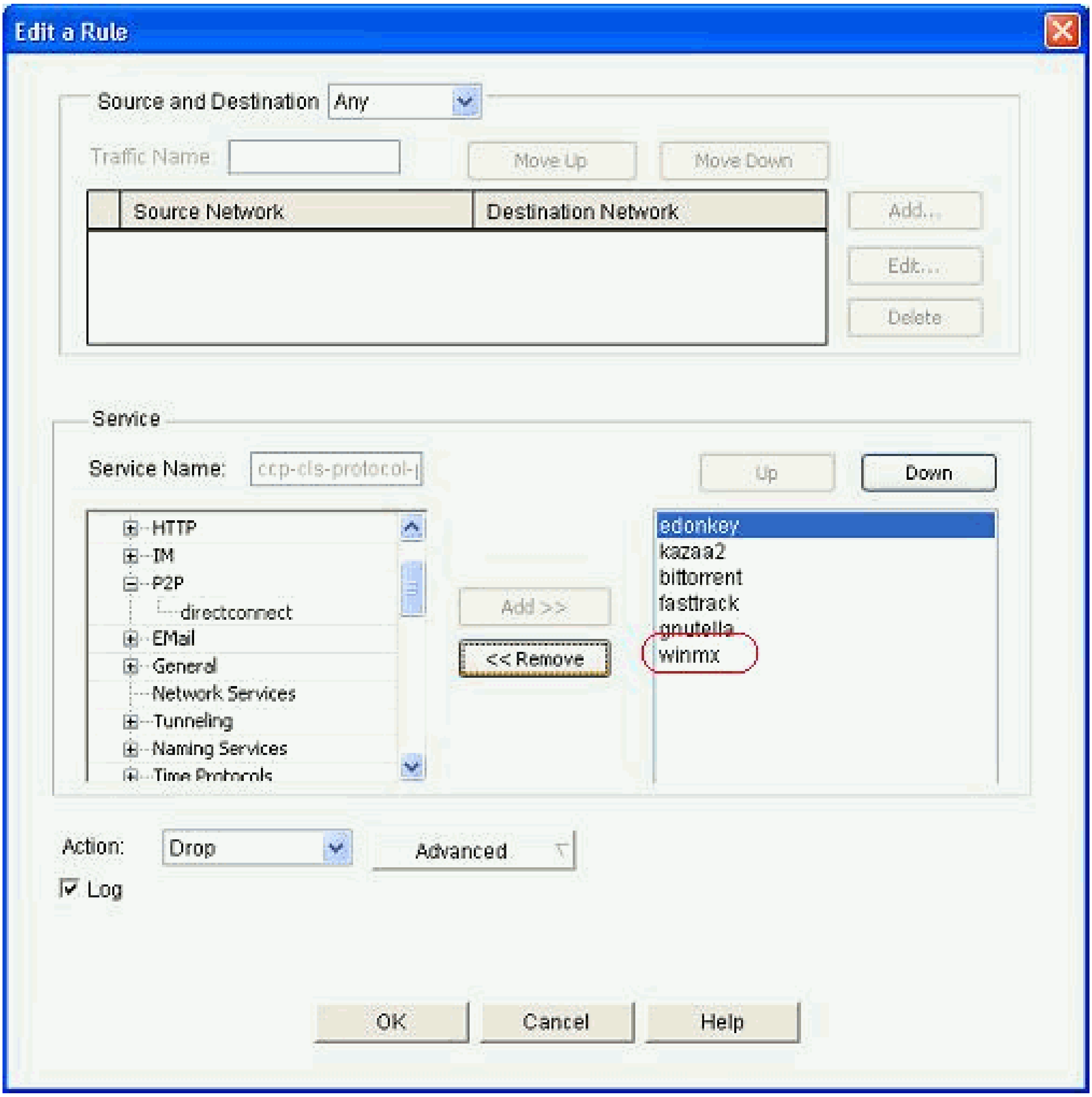
Service

Service Name: ccp-cls-protocol-|

edonkey
kazaa2
bittorrent
fasttrack
gnutella

Action: Drop

☑ Log



Edit a Rule

Source and Destination: Any

Traffic Name:

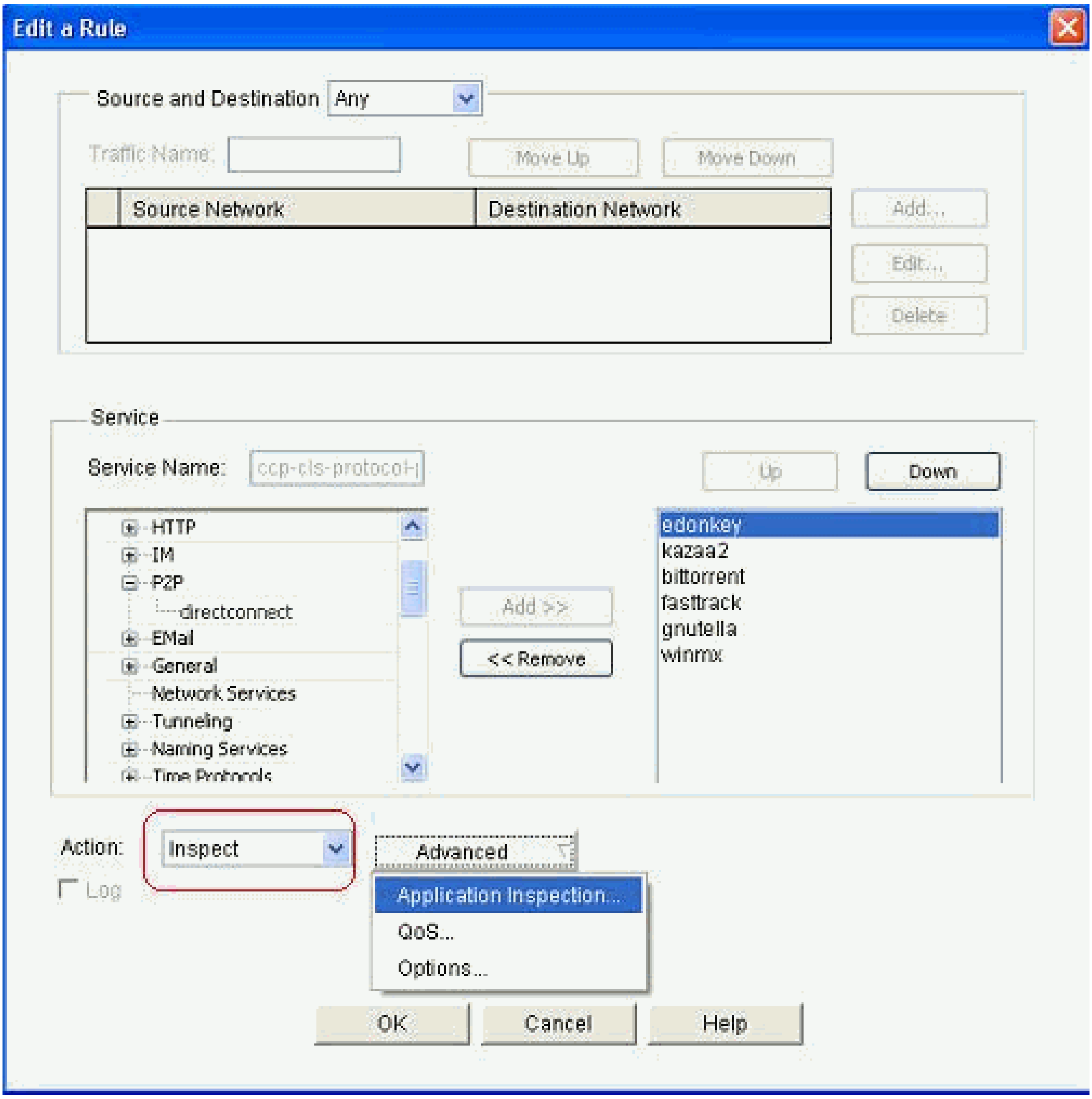
Service Name: ccp-cls-protocol-|

edonkey
kazaa2
bittorrent
fasttrack
gnutella
winmx

Action: Drop

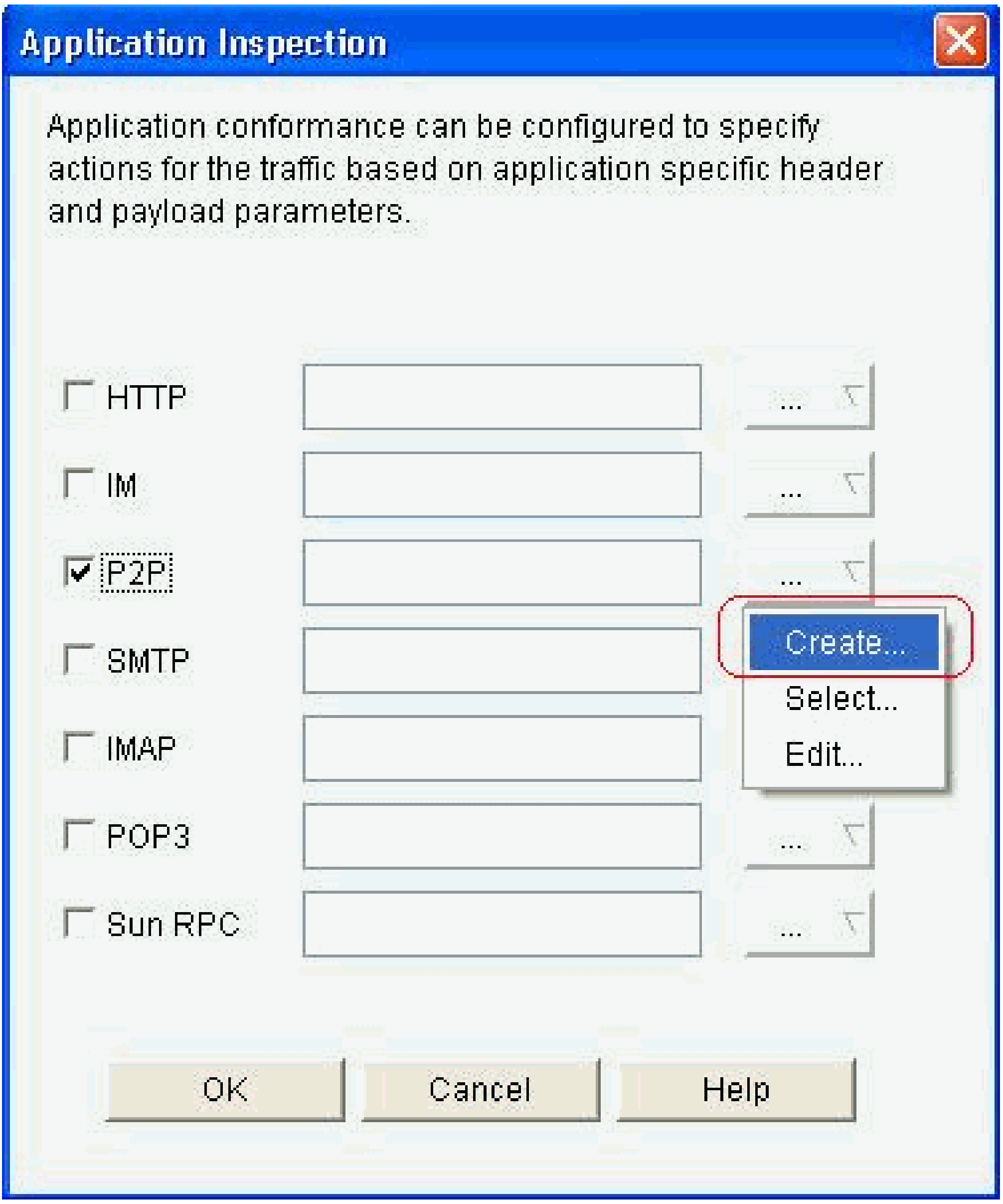
☑ Log

14. Anziché scegliere l'azione di rilascio, è possibile scegliere l'azione Ispeziona per applicare opzioni diverse per l'ispezione approfondita dei pacchetti.



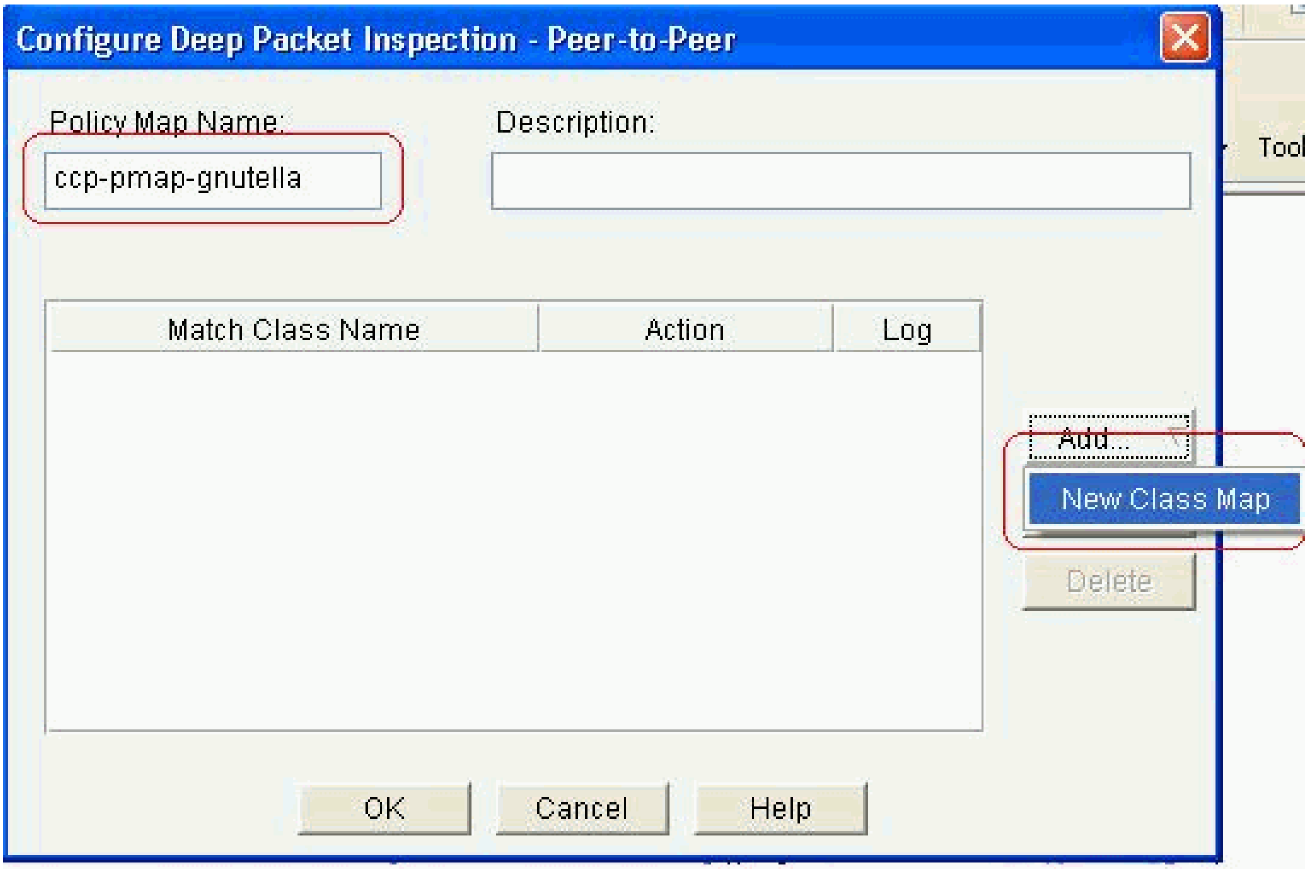
L'ispezione P2P offre policy di layer 4 e layer 7 per il traffico delle applicazioni. Ciò significa che ZFW può fornire un'ispezione stateful di base per autorizzare o negare il traffico, così come un controllo granulare di layer 7 su attività specifiche nei vari protocolli, in modo che alcune attività dell'applicazione siano consentite mentre altre vengono negate. In questa ispezione dell'applicazione è possibile applicare diversi tipi di ispezioni specifiche a livello di intestazione per le applicazioni P2P. Di seguito è riportato un esempio di gnutella.

15. Selezionare l'opzione **P2P** e fare clic su **Crea** per creare una nuova mappa dei criteri per


Application Inspection
Application conformance can be configured to specify actions for the traffic based on application specific header and payload parameters.
□ HTTP
□ IM
☑ P2P
□ SMTP
□ IMAP
□ POP3
□ Sun RPC
...
Create...
Select...
Edit...
OK
Cancel
Help

questa operazione.

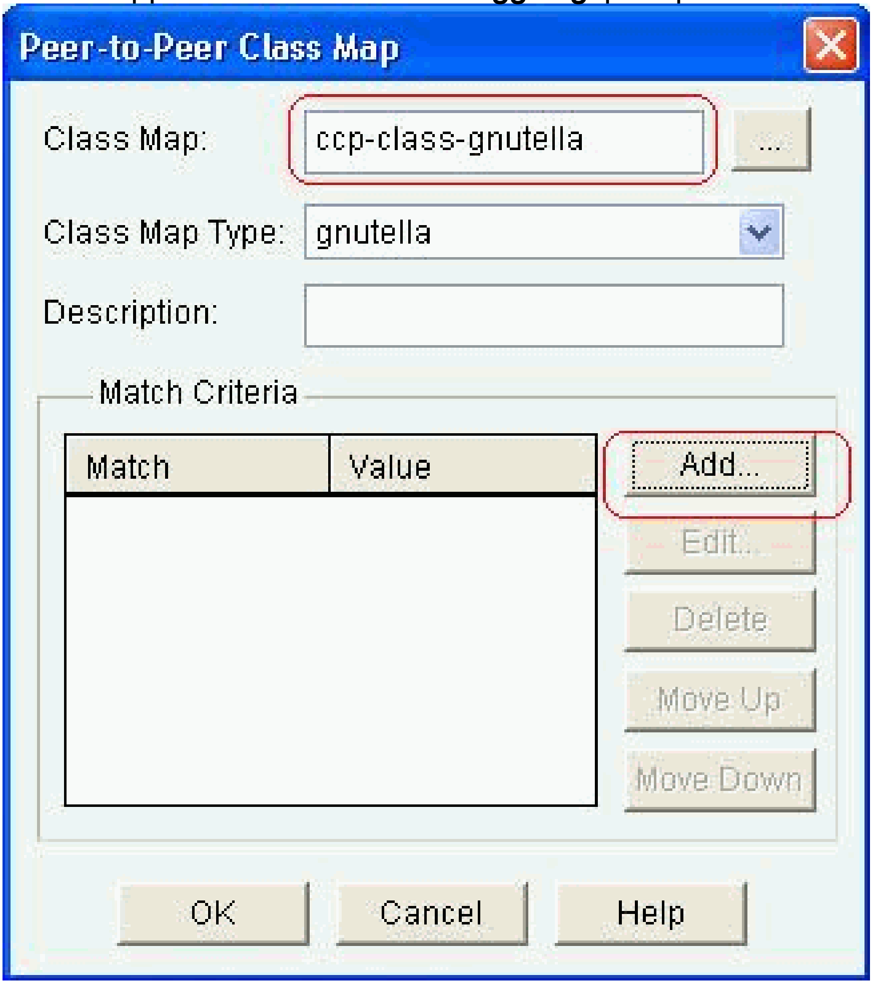
16. Crea una nuova mappa dei criteri per l'ispezione approfondita dei pacchetti per il protocollo gnutella. Fare clic su **Aggiungi**, quindi scegliere **Nuova mappa classi**.



Policy Map Name: ccp-pmap-gnutella

Description:

17. Assegnare un nuovo nome alla mappa classi e fare clic su **Aggiungi** per specificare un criterio di corrispondenza.



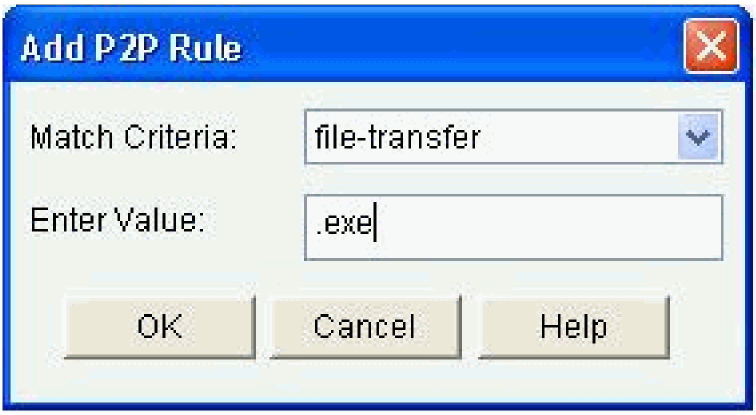
Class Map: ccp-class-gnutella

Class Map Type: gnutella

Description:

18. Utilizzare il trasferimento di file come criterio di corrispondenza e la stringa utilizzata è exe. Ciò indica che tutte le connessioni di trasferimento file gnutella contenenti la stringa exe corrispondono ai criteri di traffico. Fare clic su

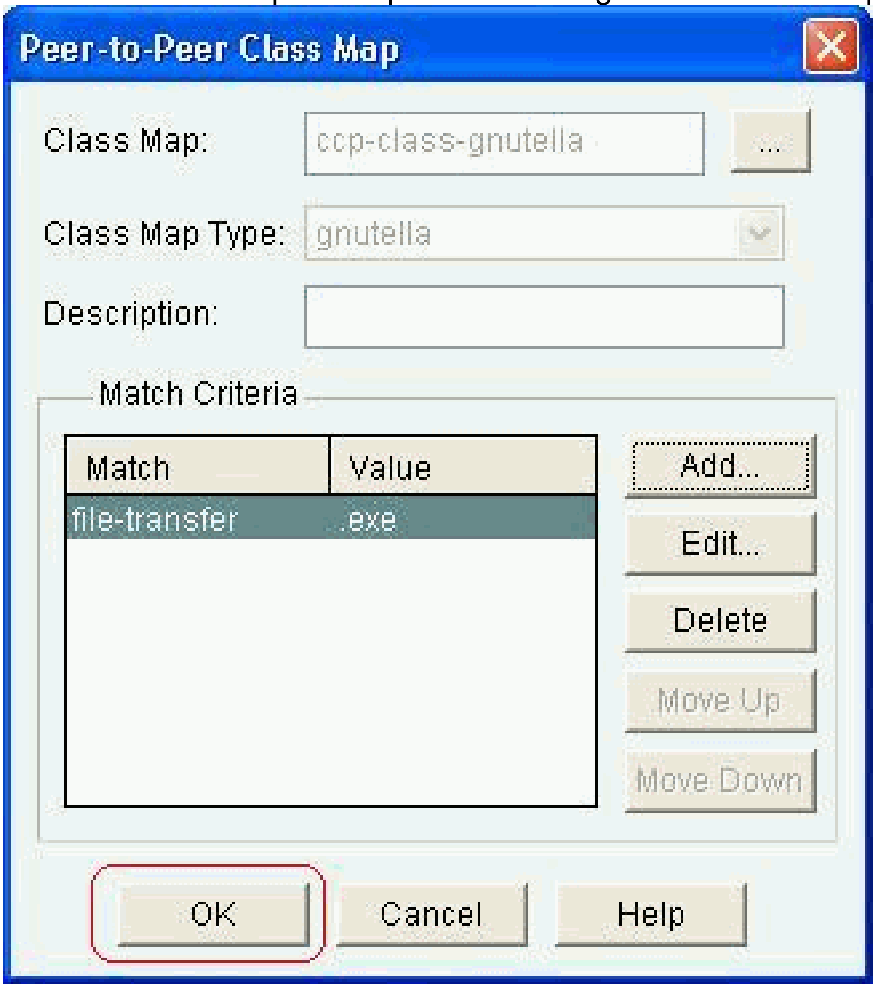
OK.



Match Criteria: file-transfer

Enter Value: .exe

19. Fare di nuovo clic su **OK** per completare la configurazione della mappa delle classi.



Class Map: ccp-class-gnutella

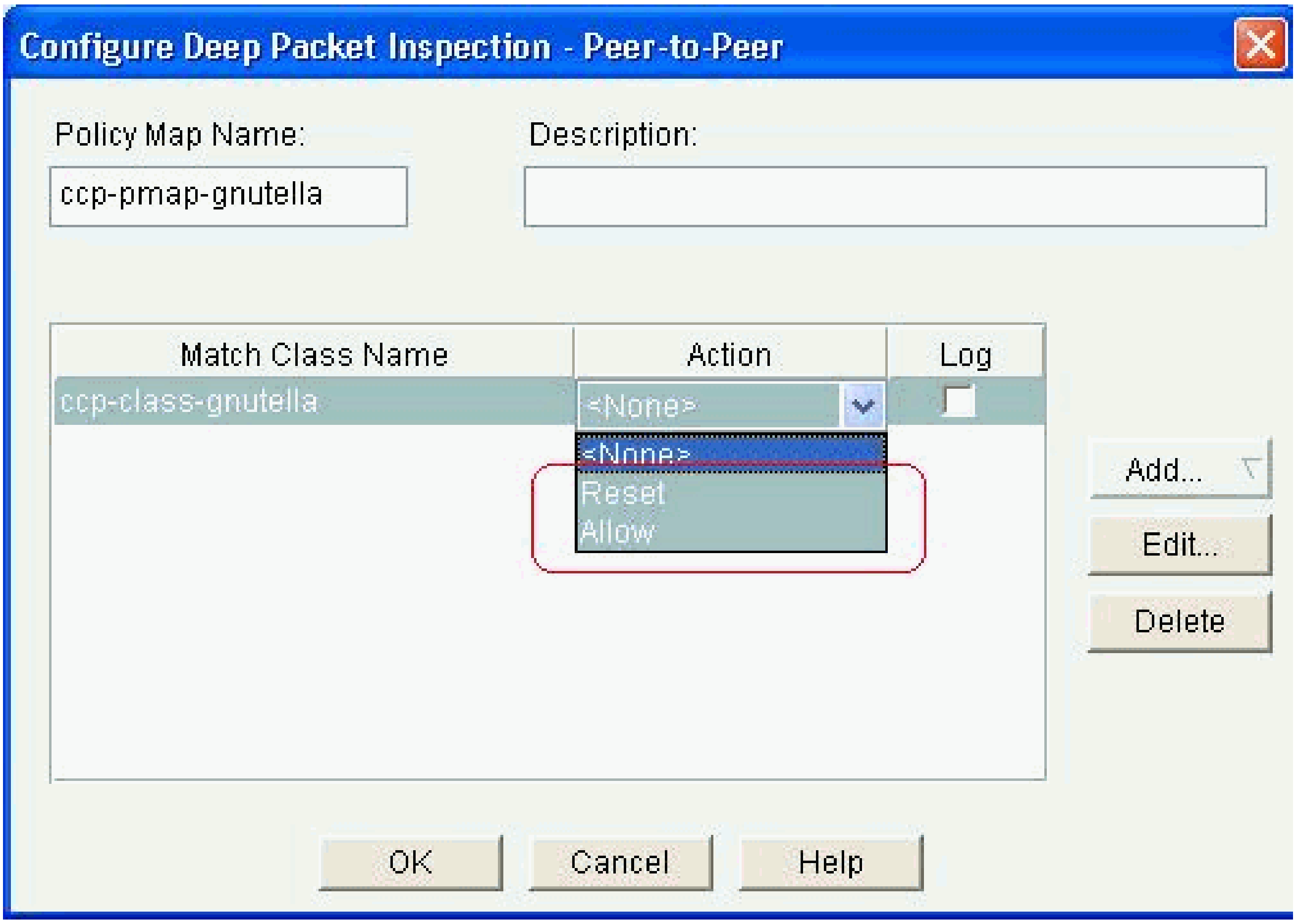
Class Map Type: gnutella

Description:

Match Criteria

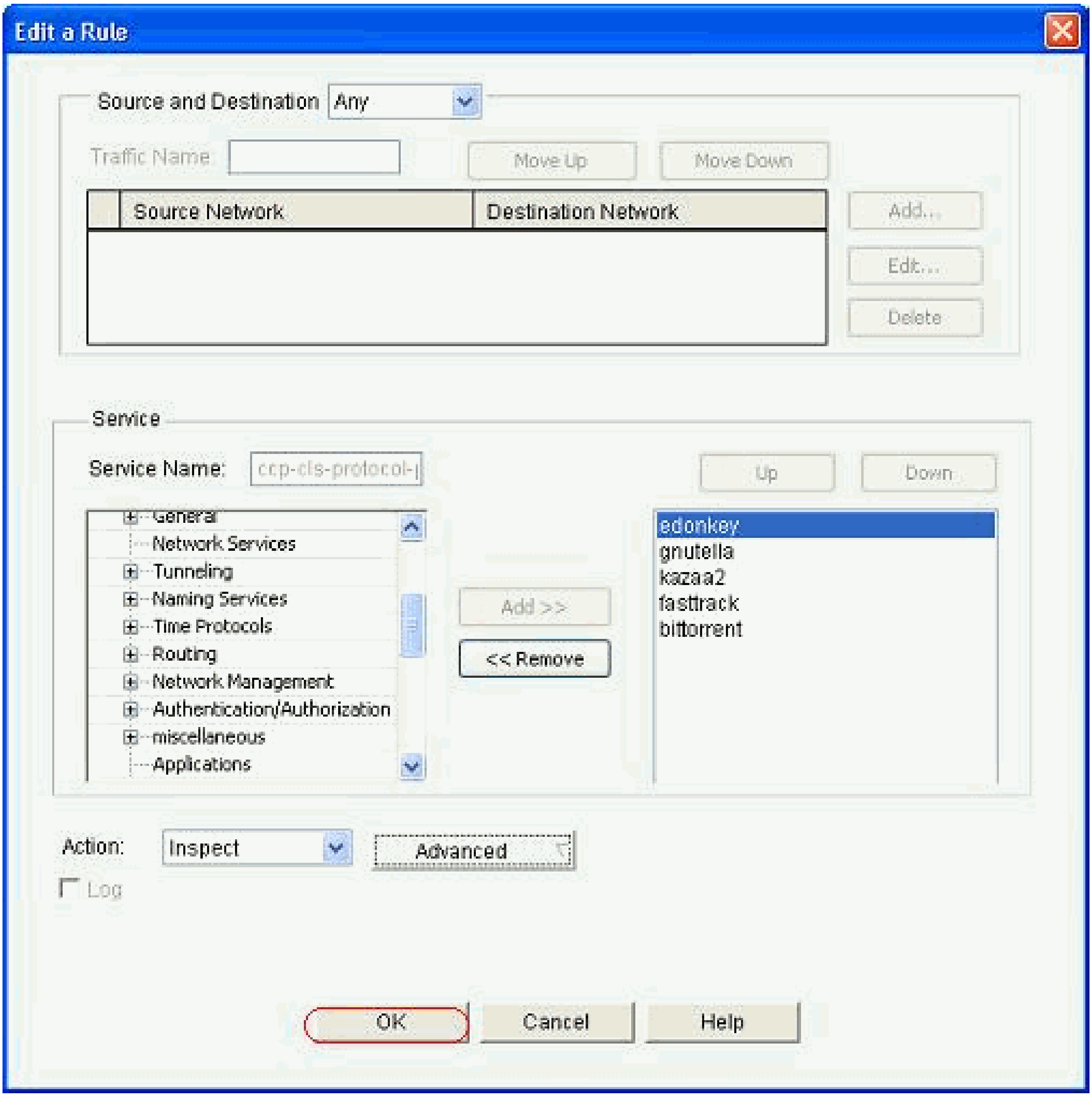
| Match | Value |
|---|---|
| file-transfer | .exe |

20. Selezionare l'opzione **Reset** (Reimposta) o **Allow** (Consenti), che dipende dai criteri di sicurezza della società. Fare clic su **OK** per confermare l'azione con la mappa dei criteri.



In questo modo è possibile aggiungere altre mappe dei criteri per implementare le funzioni di ispezione approfondita per altri protocolli P2P specificando espressioni regolari diverse come criterio di corrispondenza.**Nota:** le applicazioni P2P sono particolarmente difficili da rilevare, a causa del comportamento di "port-hopping" e di altri trucchi per evitare il rilevamento, così come i problemi introdotti da frequenti modifiche e aggiornamenti alle applicazioni P2P che modificano i comportamenti dei protocolli. ZFW combina l'ispezione stateful del firewall nativo con le funzionalità di riconoscimento del traffico di Network-Based Application Recognition (NBAR) per fornire il controllo delle applicazioni P2P.**Nota:** Ispezione applicazione P2P offre funzionalità specifiche per un sottoinsieme di applicazioni supportate dall'ispezione di livello 4:edonkeyfasttrackgnutellakazaa2**Nota:** al momento, ZFW non ha un'opzione per ispezionare il traffico di applicazioni "bittorrent" (bittorrent). I client BitTorrent in genere comunicano con i tracker (server di directory peer) tramite HTTP in esecuzione su alcune porte non standard. Si tratta in genere di TCP 6969, ma potrebbe essere necessario controllare la porta di tracciamento specifica del torrent. Se si desidera consentire BitTorrent, il metodo migliore per supportare la porta aggiuntiva è configurare HTTP come uno dei protocolli di corrispondenza e aggiungere TCP 6969 a HTTP utilizzando questo comando ip port-map: **ip port-map http port tcp 6969**. È necessario definire http e bitTorrent come criteri di corrispondenza applicati nella mappa delle classi.

21. Fare clic su **OK** per completare la configurazione Ispezione avanzata.



Source and Destination: Any

Service Name: ccp-cls-protocol-|

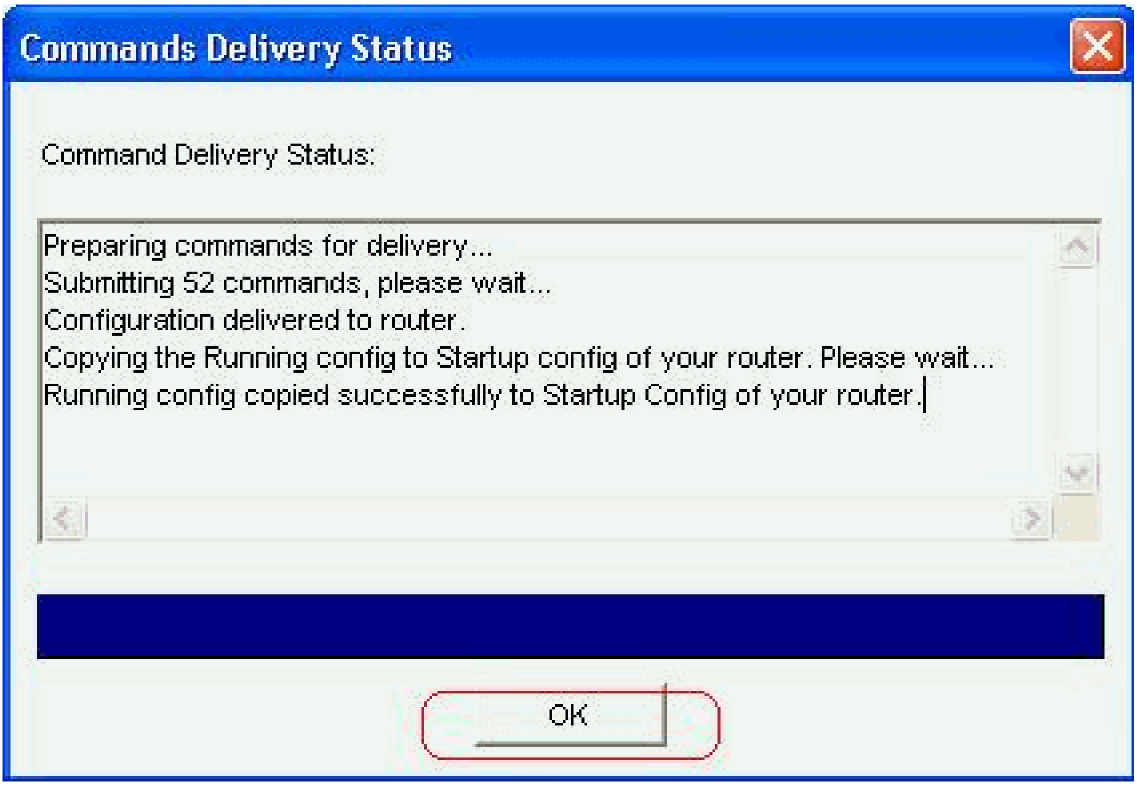
edonkey
gnutella
kazaa2
fasttrack
bittorrent

Action: Inspect

Il set di comandi corrispondente viene consegnato al router.

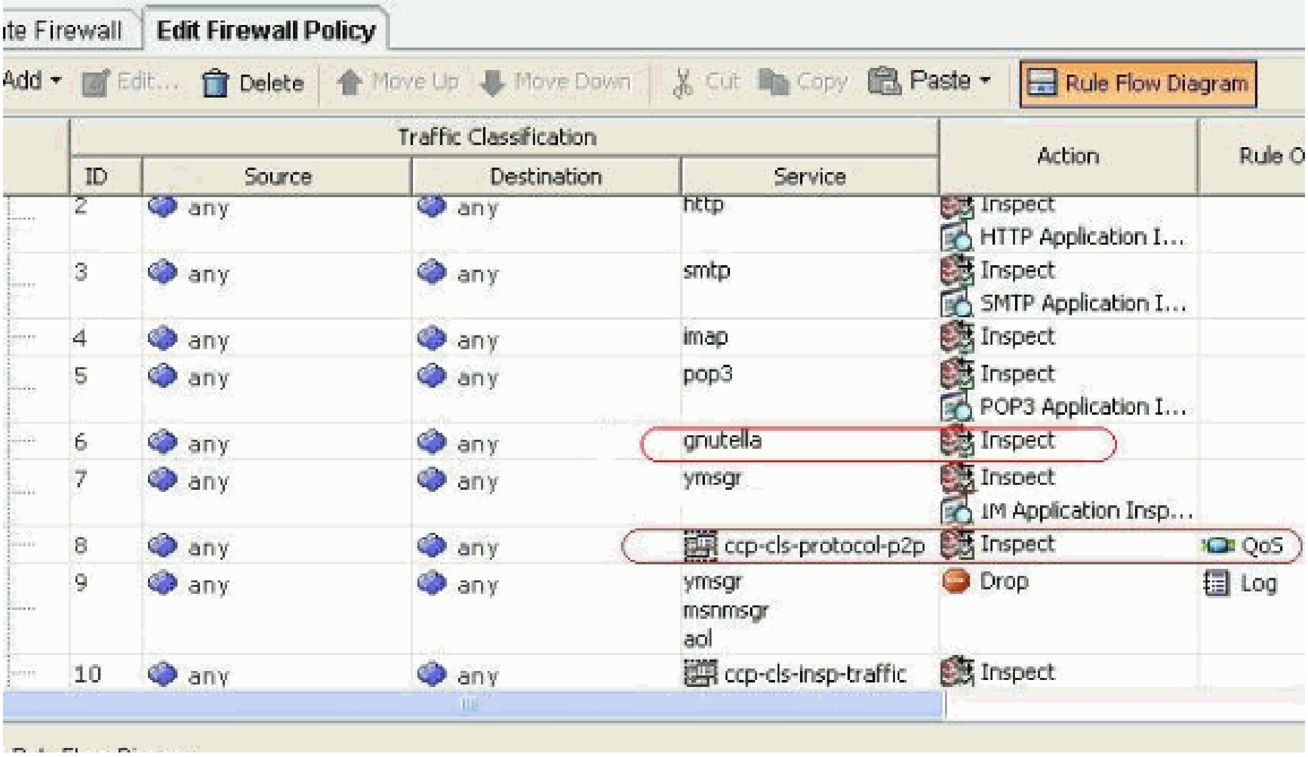
22. Fare clic su **OK** per completare la copia del gruppo di comandi sul

router.



```
Preparing commands for delivery...
Submitting 52 commands, please wait...
Configuration delivered to router.
Copying the Running config to Startup config of your router. Please wait...
Running config copied successfully to Startup Config of your router.
```

23. Èpossibile osservare le nuove regole che vengono applicate dalla scheda Modifica criterio firewall in **Configurazione > Protezione > Firewall e ACL**.



| Traffic Classification | | | | Action | Rule O |
|---|---|---|---|---|---|
| ID | Source | Destination | Service | | |
| 2 | any | any | http | Inspect<br>HTTP Application I... | |
| 3 | any | any | smtp | Inspect<br>SMTP Application I... | |
| 4 | any | any | imap | Inspect | |
| 5 | any | any | pop3 | Inspect<br>POP3 Application I... | |
| 6 | any | any | gnutella | Inspect | |
| 7 | any | any | ymsgr | Inspect<br>IM Application Insp... | |
| 8 | any | any | ccp-cls-protocol-p2p | Inspect | QoS |
| 9 | any | any | ymsgr<br>msnmsgr<br>aol | Drop | Log |
| 10 | any | any | ccp-cls-insp-traffic | Inspect | |

## Configurazione della riga di comando del router ZFW

La configurazione nella sezione precedente di Cisco CP restituisce questa configurazione sul router ZFW:

| Router ZBF |
|---|
| `ZBF-Router#`**`show run`** |

```
Building configuration...

Current configuration : 9782 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ZBF-Router
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
ip cef
!
!
!
!
ip name-server 10.77.230.45
!
multilink bundle-name authenticated
parameter-map type protocol-info msn-servers
 server name messenger.hotmail.com
 server name gateway.messenger.hotmail.com
 server name webmessenger.msn.com

parameter-map type protocol-info aol-servers
 server name login.oscar.aol.com
 server name toc.oscar.aol.com
 server name oam-d09a.blue.aol.com

parameter-map type protocol-info yahoo-servers
 server name scs.msg.yahoo.com
 server name scsa.msg.yahoo.com
 server name scsb.msg.yahoo.com
 server name scsc.msg.yahoo.com
 server name scsd.msg.yahoo.com
 server name cs16.msg.dcn.yahoo.com
 server name cs19.msg.dcn.yahoo.com
 server name cs42.msg.dcn.yahoo.com
 server name cs53.msg.dcn.yahoo.com
 server name cs54.msg.dcn.yahoo.com
 server name ads1.vip.scd.yahoo.com
 server name radio1.launch.vip.dal.yahoo.com
 server name in1.msg.vip.re2.yahoo.com
 server name data1.my.vip.sc5.yahoo.com
 server name address1.pim.vip.mud.yahoo.com
 server name edit.messenger.yahoo.com
 server name messenger.yahoo.com
 server name http.pager.yahoo.com
 server name privacy.yahoo.com
 server name csa.yahoo.com
 server name csb.yahoo.com
 server name csc.yahoo.com

parameter-map type regex ccp-regex-nonascii
 pattern [^\x00-\x80]

!
!
```

```
!
crypto pki trustpoint TP-self-signed-1742995674
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1742995674
 revocation-check none
 rsakeypair TP-self-signed-1742995674
!
!
crypto pki certificate chain TP-self-signed-1742995674
 certificate self-signed 02
  30820242 308201AB A0030201 02020102 300D0609 2A864886
F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967
6E65642D 43657274
  69666963 6174652D 31373432 39393536 3734301E 170D3130
31313236 31303332
  32315A17 0D323030 31303130 30303030 305A3031 312F302D
06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361
74652D31 37343239
  39353637 3430819F 300D0609 2A864886 F70D0101 01050003
818D0030 81890281
  8100A84A 980D15F0 6A6B5F1B 5A3359DE 5D552EFE FAA8079B
DA927DA2 4AF210F0
  408131CE BB5B0189 FD82E22D 6A6284E3 5F4DB2A7 7517772B
1BC5624E A1A6382E
  6A07EE71 E93A98C9 B8494A55 0CDD6B4C 442065AA DBC9D9CC
14D10B65 2FEFECC8
  AA9B3064 59105FBF B9B30219 2FD53ECA 06720CA1 A6D30DA5
564FCED4 C53FC7FD
  835B0203 010001A3 6A306830 0F060355 1D130101 FF040530
030101FF 30150603
  551D1104 0E300C82 0A5A4246 2D526F75 74657230 1F060355
1D230418 30168014
  0BDBE585 15377DCA 5F00A1A2 6644EC22 366DE590 301D0603
551D0E04 1604140B
  DBE58515 377DCA5F 00A1A266 44EC2236 6DE59030 0D06092A
864886F7 0D010104
  05000381 810037F4 8EEC7AF5 85429563 F78F2F41 A060EEE8
F23D8F3B E0913811
  A143FC44 8CCE71C3 A5E9D979 C2A8CD38 C272A375 4FCD459B
E02A9427 56E2F1A0
  DA190B50 FA091669 CD8C066E CD1A095B 4E015326 77B3E567
DFD55A71 53220F86
  F006D31E 02CB739E 19D633D6 61E49866 C31AD865 DC7F4380
FFEDDBAB 89E3B3E9
  6139E472 DC62
        quit
!
!
username cisco privilege 15 password 0 cisco123
archive
 log config
  hidekeys
!
!
class-map type inspect match-all sdm-cls-im
 match protocol ymsgr
class-map type inspect imap match-any ccp-app-imap
 match  invalid-command
class-map type inspect match-any ccp-cls-protocol-p2p
 match protocol  signature
 match protocol gnutella signature
 match protocol kazaa2 signature
 match protocol fasttrack signature
 match protocol bitTorrent signature
class-map type inspect smtp match-any ccp-app-smtp
 match  data-length gt 5000000
class-map type inspect http match-any ccp-app-nonascii
 match  req-resp header regex ccp-regex-nonascii
class-map type inspect match-any CCP-Voice-permit
 match protocol h323
 match protocol skinny
 match protocol sip
class-map type inspect gnutella match-any ccp-class-
gnutella
 match  file-transfer .exe
class-map type inspect match-any ccp-cls-insp-traffic
 match protocol dns
 match protocol https
 match protocol icmp
 match protocol imap
 match protocol pop3
 match protocol tcp
 match protocol udp
class-map type inspect match-all ccp-insp-traffic
 match class-map ccp-cls-insp-traffic
class-map type inspect match-any ccp-cls-icmp-access
 match protocol icmp
 match protocol tcp
 match protocol udp
!!--- Output suppressed ! class-map type inspect match-
all sdm-cls-p2p match protocol gnutella class-map type
inspect match-all ccp-protocol-pop3 match protocol pop3
class-map type inspect kazaa2 match-any ccp-cls-p2p
match file-transfer class-map type inspect pop3 match-
any ccp-app-pop3 match invalid-command class-map type
inspect match-all ccp-protocol-p2p match class-map ccp-
cls-protocol-p2p class-map type inspect match-all ccp-
protocol-im match class-map ccp-cls-protocol-im class-
map type inspect match-all ccp-invalid-src match access-
group 100 class-map type inspect match-all ccp-icmp-
access match class-map ccp-cls-icmp-access class-map
type inspect http match-any ccp-app-httpmethods match
request method bcopy match request method bdelete match
request method bmove match request method bpropfind
match request method bproppatch match request method
connect match request method copy match request method
delete match request method edit match request method
getattribute match request method getattributenames
match request method getproperties match request method
index match request method lock match request method
mkcol match request method mkdir match request method
move match request method notify match request method
options match request method poll match request method
post match request method propfind match request method
proppatch match request method put match request method
revadd match request method revlabel match request
method revlog match request method revnum match request
method save match request method search match request
method setattribute match request method startrev match
request method stoprev match request method subscribe
match request method trace match request method unedit
match request method unlock match request method
unsubscribe class-map type inspect http match-any ccp-
http-blockparam match request port-misuse im match
request port-misuse p2p match request port-misuse
tunneling match req-resp protocol-violation class-map
```

```
type inspect match-all ccp-protocol-imap match protocol
imap class-map type inspect match-all ccp-protocol-smtp
match protocol smtp class-map type inspect match-all
ccp-protocol-http match protocol http ! ! policy-map
type inspect ccp-permit-icmpreply class type inspect
ccp-icmp-access inspect class class-default pass ! !---
Output suppressed ! policy-map type inspect http ccp-
action-app-http class type inspect http ccp-http-
blockparam log reset class type inspect http ccp-app-
httpmethods log reset class type inspect http ccp-app-
nonascii log reset class class-default policy-map type
inspect smtp ccp-action-smtp class type inspect smtp
ccp-app-smtp reset class class-default policy-map type
inspect imap ccp-action-imap class type inspect imap
ccp-app-imap log reset class class-default policy-map
type inspect pop3 ccp-action-pop3 class type inspect
pop3 ccp-app-pop3 log reset class class-default policy-
map type inspect ccp-inspect class type inspect ccp-
invalid-src drop log class type inspect ccp-protocol-
http inspect service-policy http ccp-action-app-http
class type inspect ccp-protocol-smtp inspect service-
policy smtp ccp-action-smtp class type inspect ccp-
protocol-imap inspect service-policy imap ccp-action-
imap class type inspect ccp-protocol-pop3 inspect
service-policy pop3 ccp-action-pop3 class type inspect
sdm-cls-p2p inspect ! !--- Output suppressed ! class
type inspect ccp-protocol-im drop log class type inspect
ccp-insp-traffic inspect class type inspect CCP-Voice-
permit inspect class class-default pass policy-map type
inspect ccp-permit class class-default policy-map type
inspect p2p ccp-pmap-gnutella class type inspect
gnutella ccp-class-gnutella ! zone security out-zone
zone security in-zone zone-pair security ccp-zp-self-out
source self destination out-zone service-policy type
inspect ccp-permit-icmpreply zone-pair security ccp-zp-
in-out source in-zone destination out-zone service-
policy type inspect ccp-inspect zone-pair security ccp-
zp-out-self source out-zone destination self service-
policy type inspect ccp-permit ! ! ! interface
FastEthernet0/0 description $FW_OUTSIDE$ ip address
209.165.201.2 255.255.255.224 zone-member security out-
zone duplex auto speed auto ! interface FastEthernet0/1
description $FW_INSIDE$ ip address 10.77.241.114
255.255.255.192 zone-member security in-zone duplex auto
speed auto ! ! !--- Output suppressed ! ! ip http server
ip http authentication local ip http secure-server ! !
!--- Output suppressed ! ! ! control-plane ! ! line con
0 line aux 0 line vty 0 4 privilege level 15 login local
transport input ssh ! scheduler allocate 20000 1000 !
webvpn cef end ZBF-Router#
```

# Verifica

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

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

- ZBF-Router#**show policy-map type inspect zone-pair sessions**: visualizza le statistiche della mappa dei criteri del tipo di inspect runtime per tutte le coppie di zone esistenti.

## Informazioni correlate

- Guida alla progettazione e all'applicazione di firewall per i criteri basati su zone
- Esempio di configurazione di un'applicazione Cisco IOS Firewall classica e Virtual Firewall basata su zona
- Home page di Cisco Configuration Professional