Cisco CP — 配置ZFW以阻止對等流量

目錄

簡介

本文提供使用思科配置專業版(Cisco CP)中的高級防火牆配置嚮導將Cisco IOS路由器配置為基於區域的防火牆以阻止對等(P2P)流量的逐步方法。

基於區域的策略防火牆（也稱為區域策略防火牆，或ZFW）將防火牆配置從較舊的基於介面的模型更改為更靈活、更易於理解的基於區域的模型。介面分配給區域，檢查策略應用於區域之間移動的流量。區域間策略提供了相當大的靈活性和精細度。因此，可以將不同的檢查策略應用於連線到同一路由器介面的多個主機組。區域建立網路的安全邊界。區域定義一個邊界，在該邊界中，流量在穿過網路的其他區域時會受到策略限制。區域之間的ZFW預設策略是deny all。如果沒有明確配置策略，則會阻止在區域之間移動的所有流量。

P2P應用是網際網路上應用最廣泛的應用之一。P2P網路可以作為蠕蟲等惡意威脅的管道，提供繞過防火牆的簡單路徑，並引起對隱私和安全性的擔憂。Cisco IOS軟體版本12.4(9)T引入了對P2P應用的ZFW支援。P2P檢測為應用流量提供第4層和第7層策略。這意味著ZFW可以提供允許或拒絕流量的基本狀態檢測，以及對各種協定中的特定活動進行精細的第7層控制，從而允許某些應用活動而拒絕其他應用活動。

Cisco CP提供了一種易於遵循的分步方法，通過使用高級防火牆配置嚮導將IOS路由器配置為基於區域的防火牆。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- IOS路由器的軟體版本必須是12.4(9)T或更高版本。
- 有關支援Cisco CP的IOS路由器型號，請參閱Cisco CP發行說明。

運行Cisco CP的路由器配置

註：要在Cisco路由器上運行Cisco CP，請執行以下配置步驟：

```
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
```

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行IOS軟體版本12.4(15)T的Cisco 1841 IOS路由器
- 思科組態專業版(Cisco CP)版本2.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

在本檔案的示例中，路由器配置為基於區域的防火牆，以阻止P2P流量。ZFW路由器有兩個介面，一個內部（受信）介面在區域內一個外部（不受信）介面在外部區域內。ZFW路由器通過日誌記錄操作阻止從In-zone傳輸到Out-zone的P2P應用，例如edonkey、fasttrack、gnutella和kazaa2。

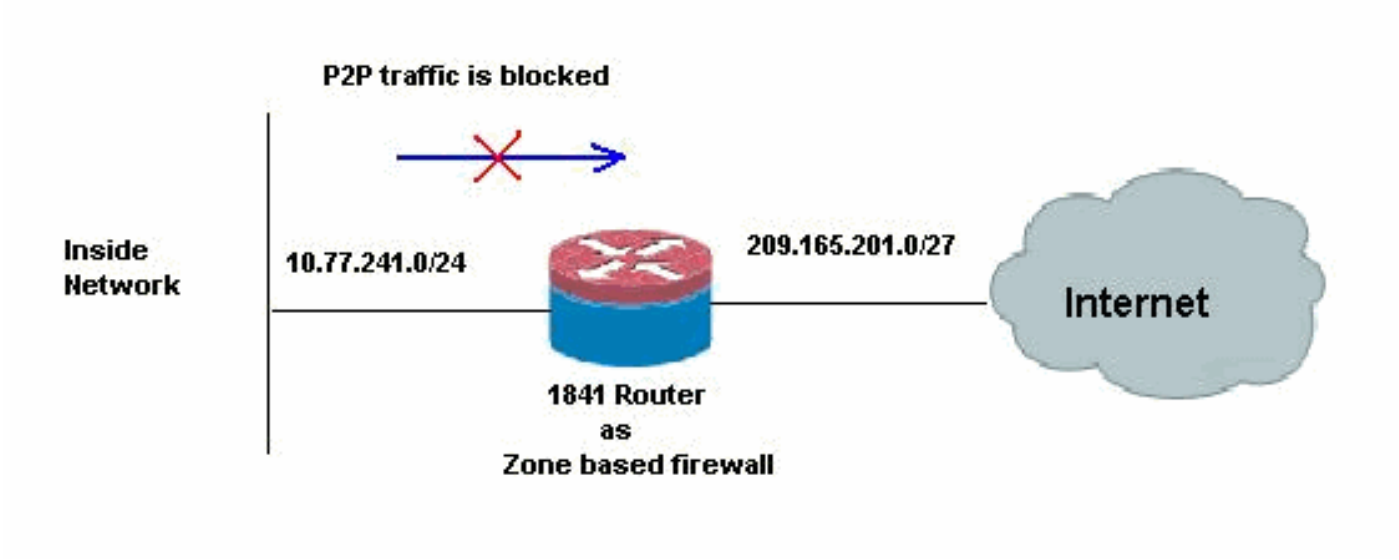
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：

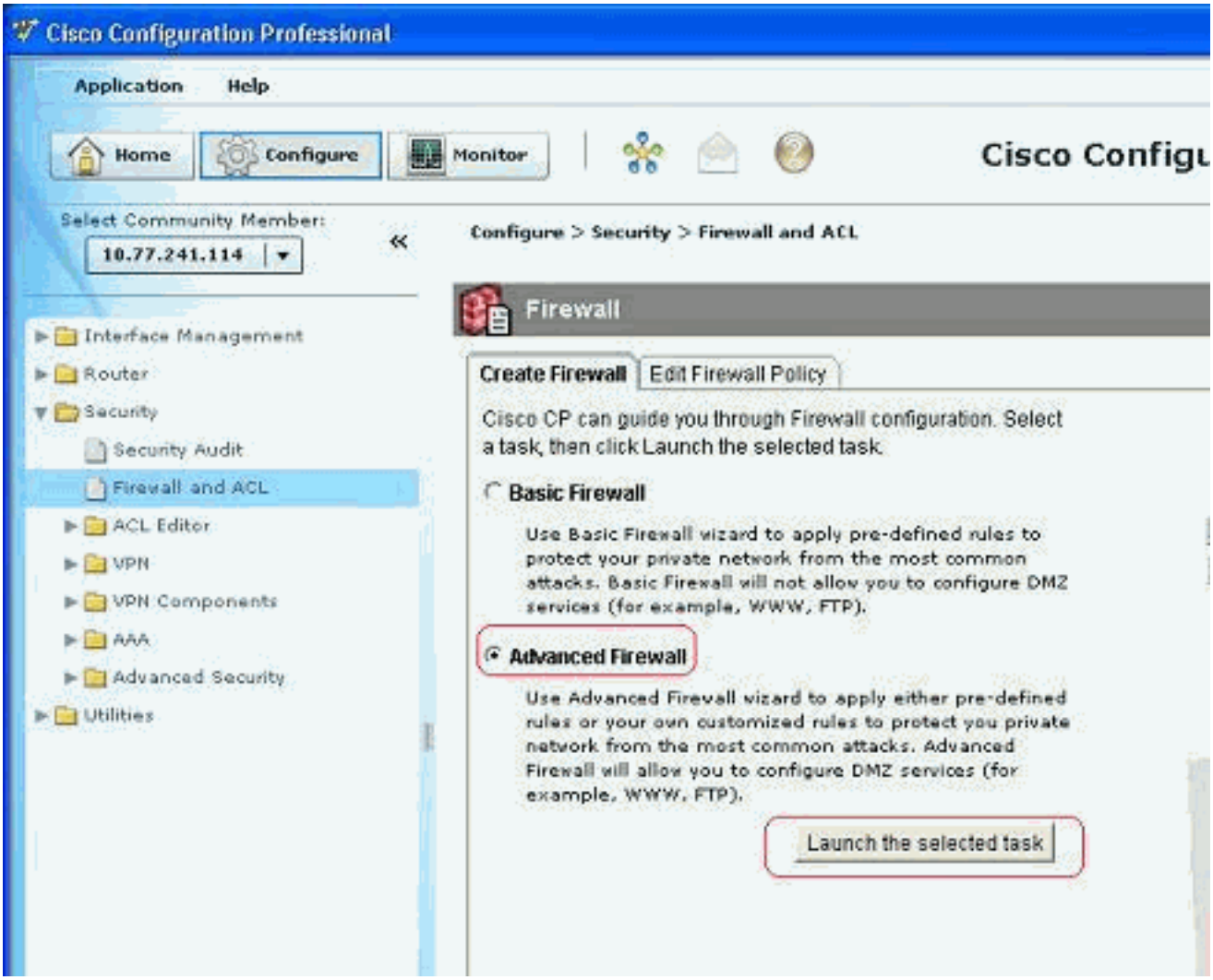


通過Cisco Configuration Professional進行配置

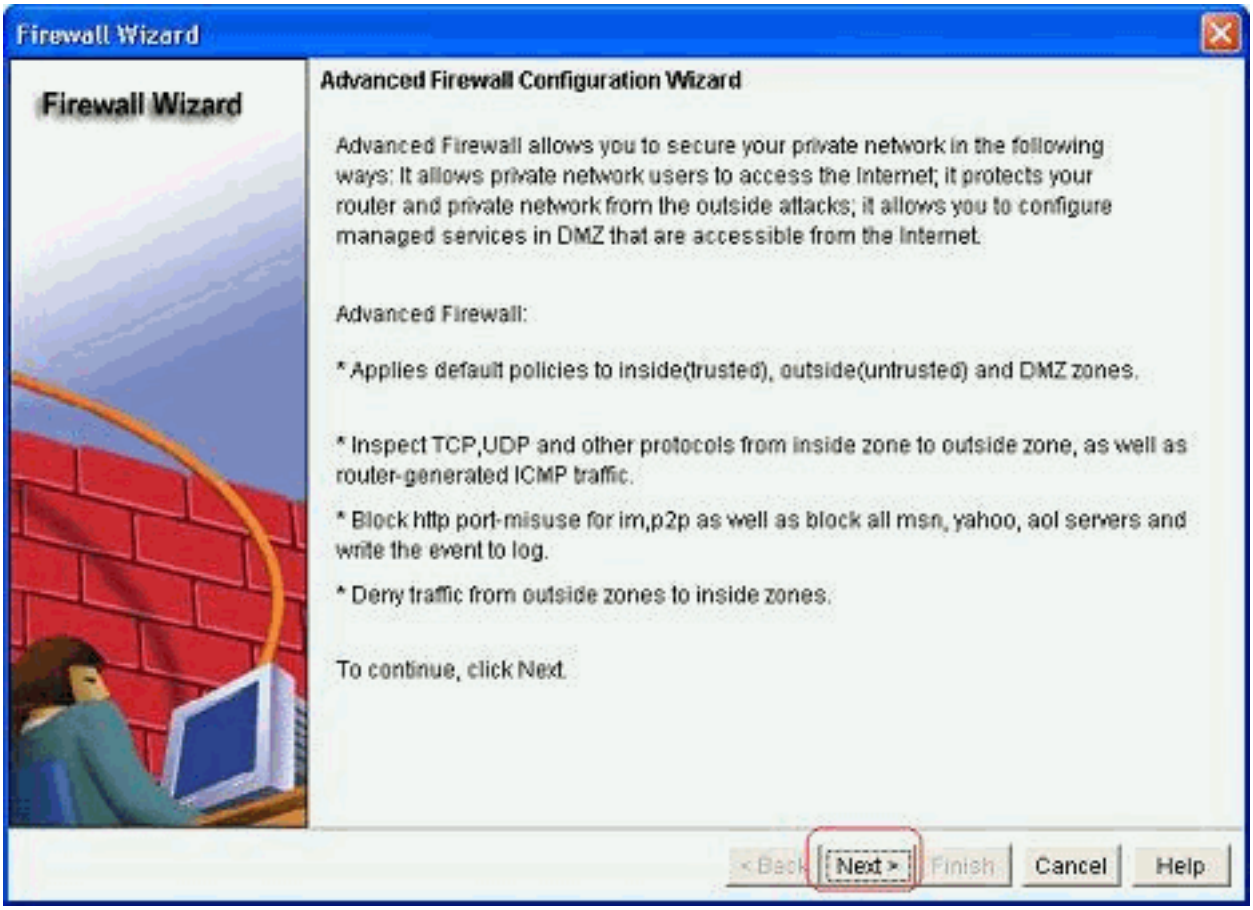
本節包含有關如何使用嚮導將IOS路由器配置為基於區域的防火牆的逐步過程。

請完成以下步驟：

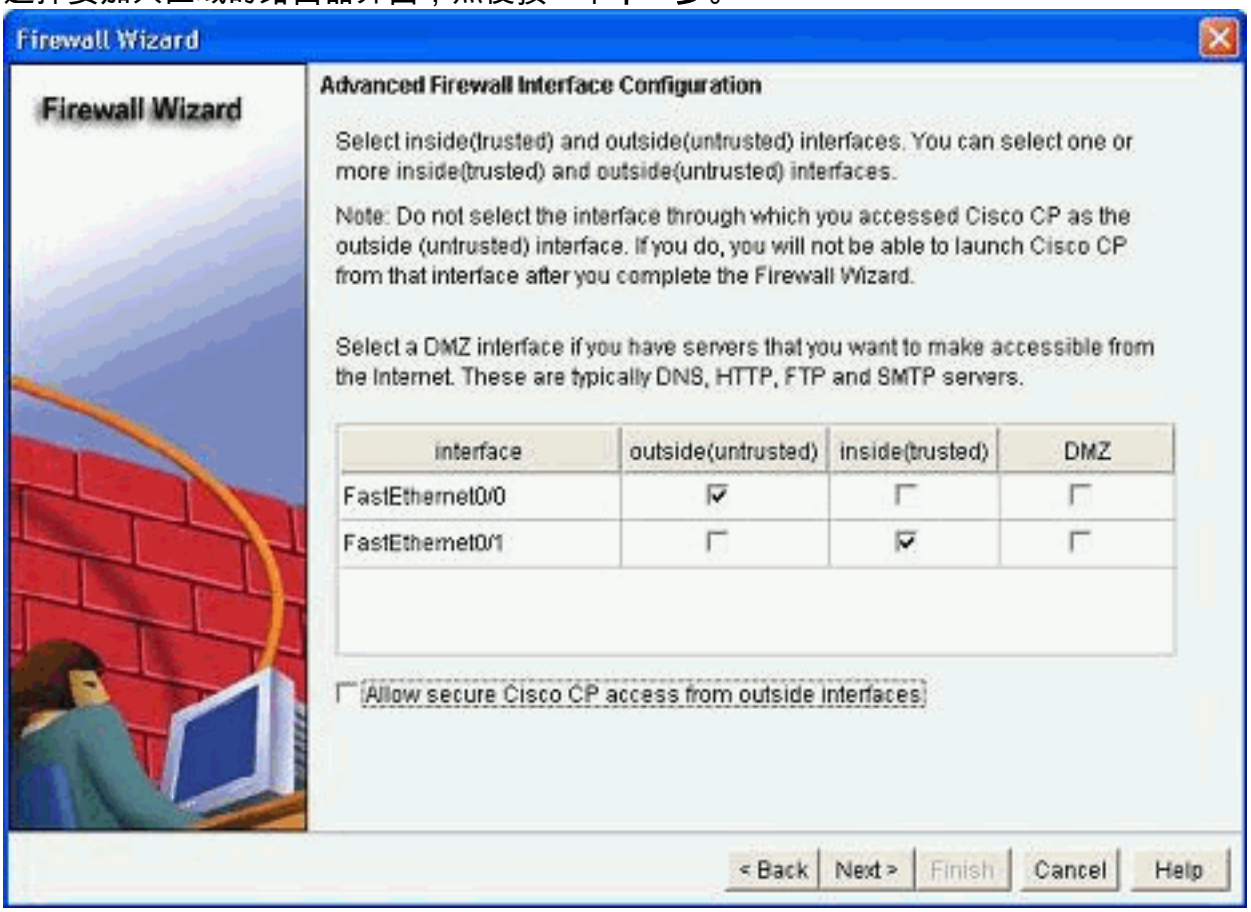
1. 前往**Configure > Security > Firewall and ACL**。然後，選擇**Advanced Firewall**單選按鈕。按一下**Launch the selected task**。



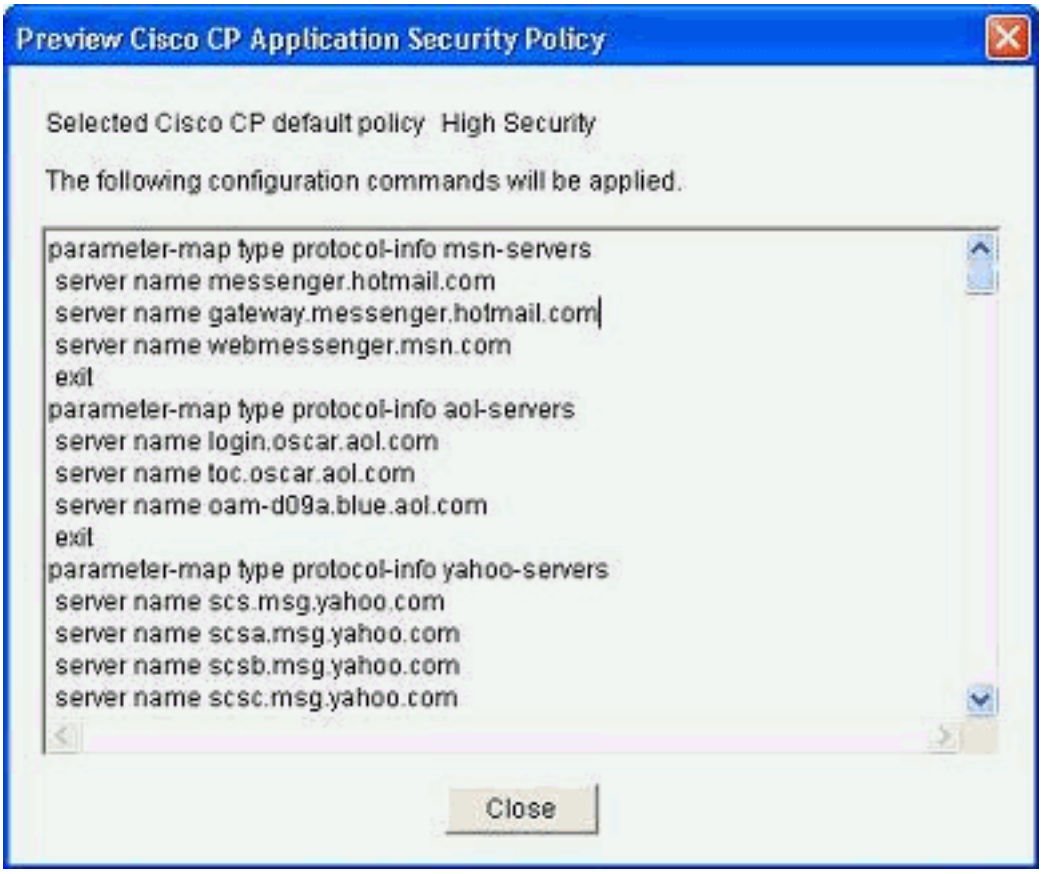
2. 下一個螢幕顯示有關防火牆嚮導的簡介。按一下**下一步**開始配置防火牆。



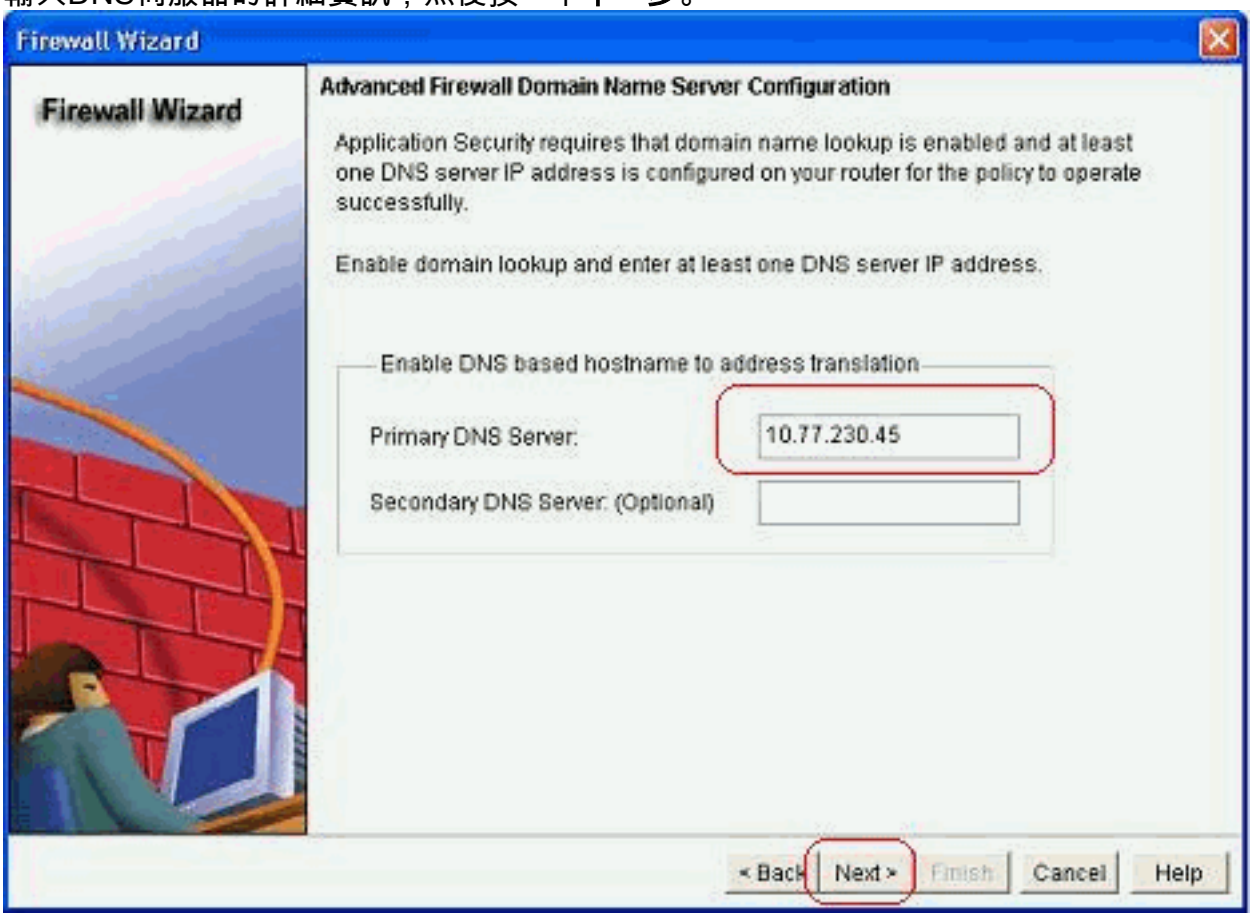
3. 選擇要加入區域的路由器介面，然後按一下**下一步**。



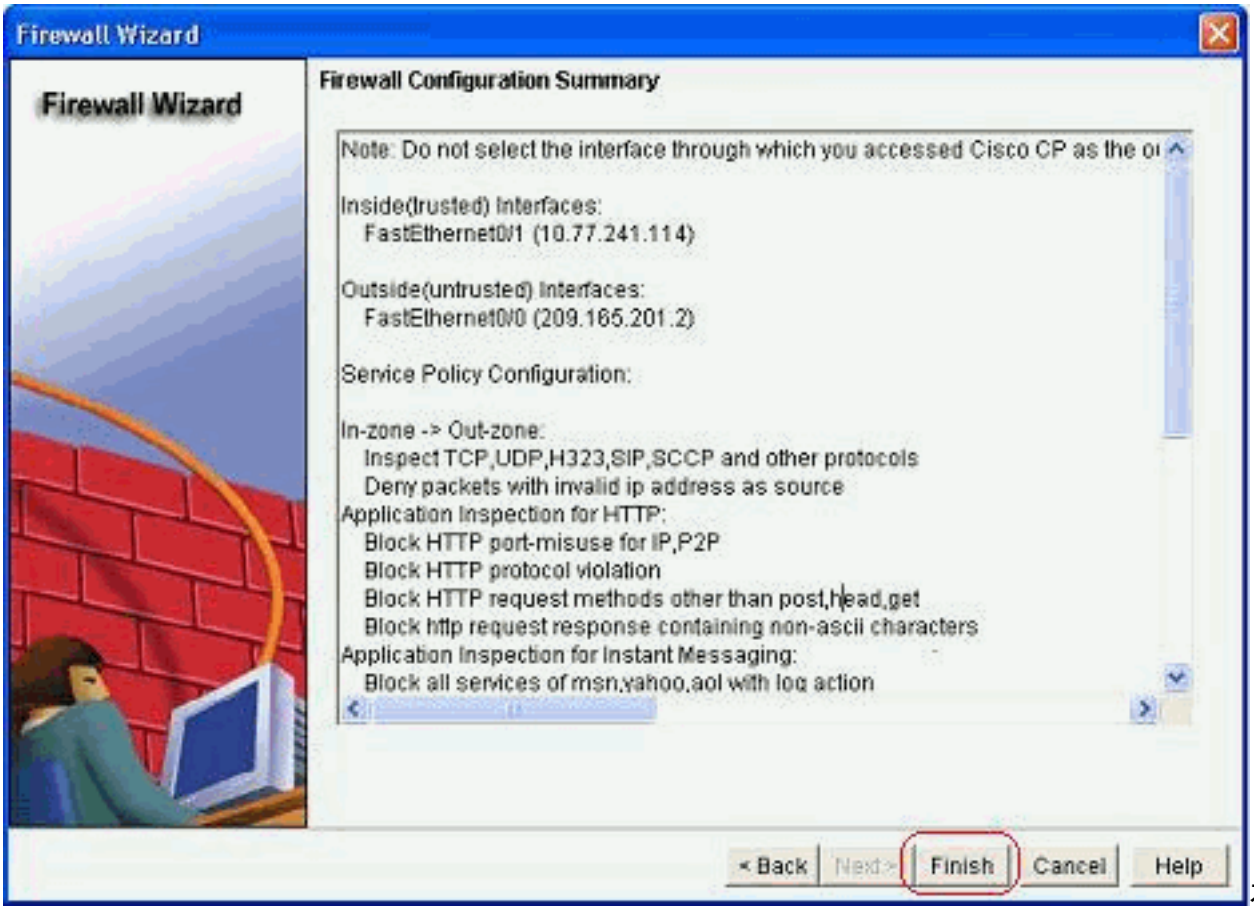
4. 具有高安全性的預設策略以及命令集顯示在下一個視窗中。按一下**Close**繼續。



5. 輸入DNS伺服器的詳細資訊，然後按一下**下一步**。

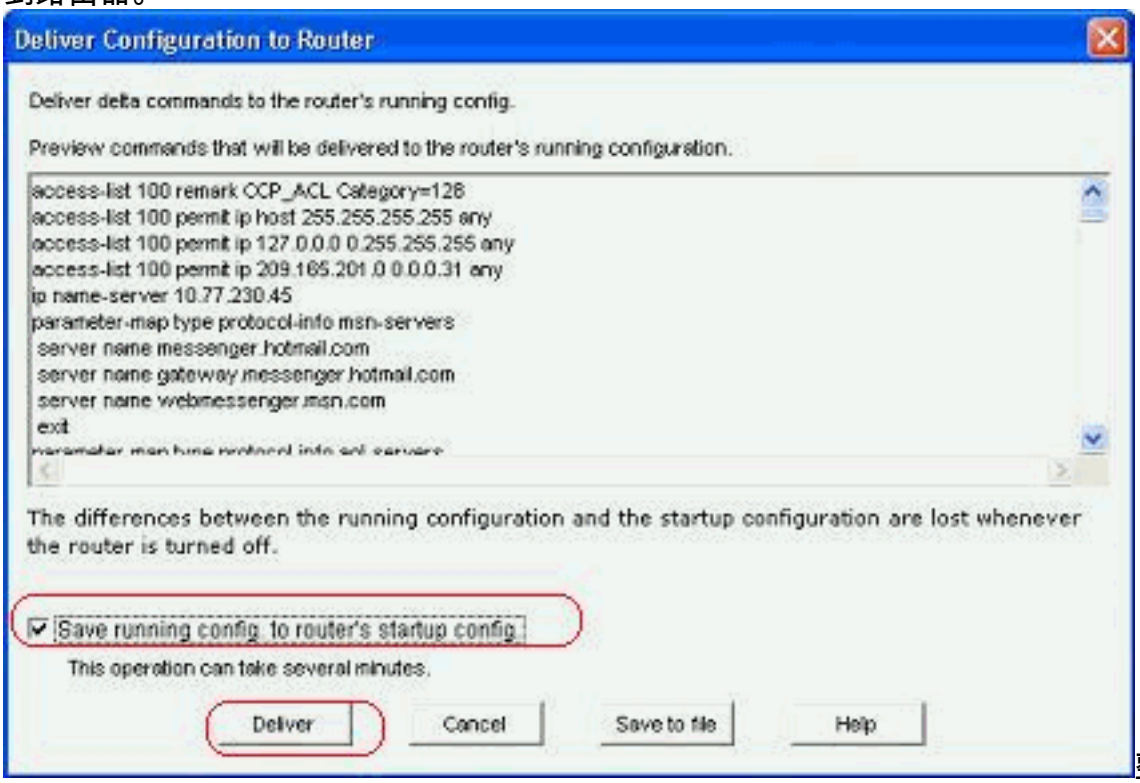


6. Cisco CP提供配置摘要，如圖所示。按一下「**Finish**」完成設定。

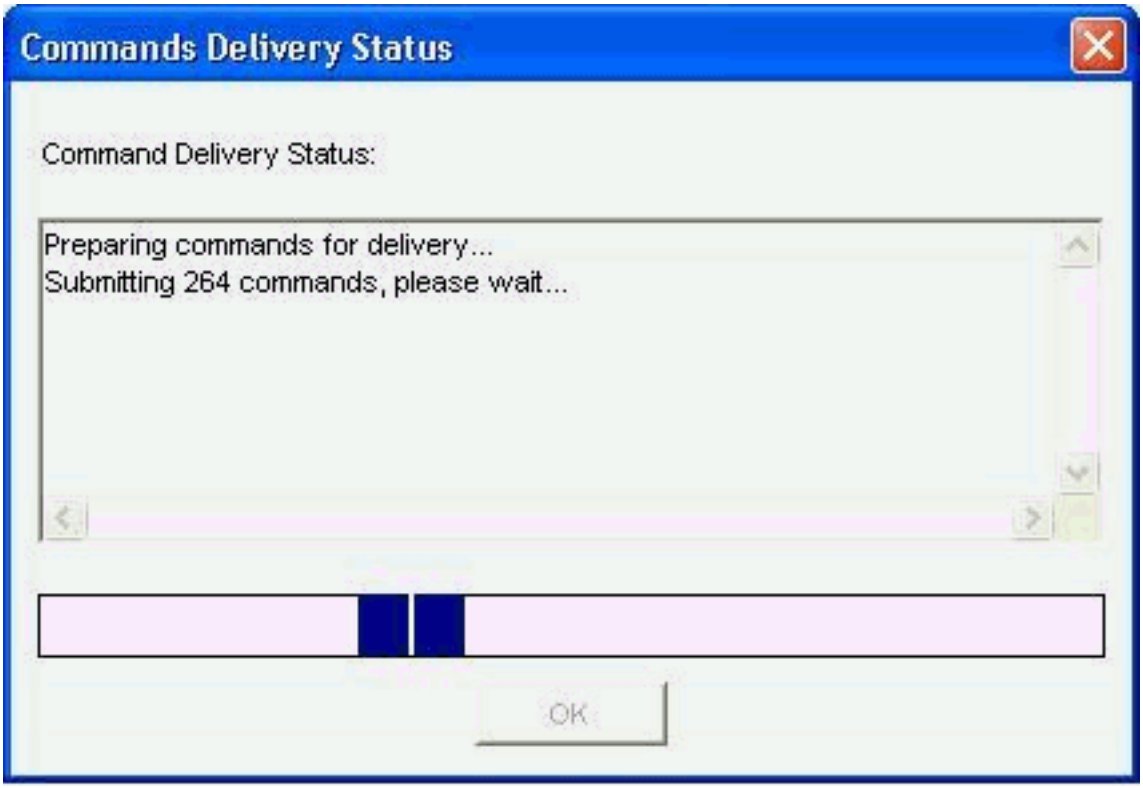


本表中提供了詳細的配置摘要。這是根據Cisco CP的高安全策略的預設配置。

7. 選中**Save the running config to router』s startup config復**選框。按一下**Deliver**將此配置傳送到路由器。



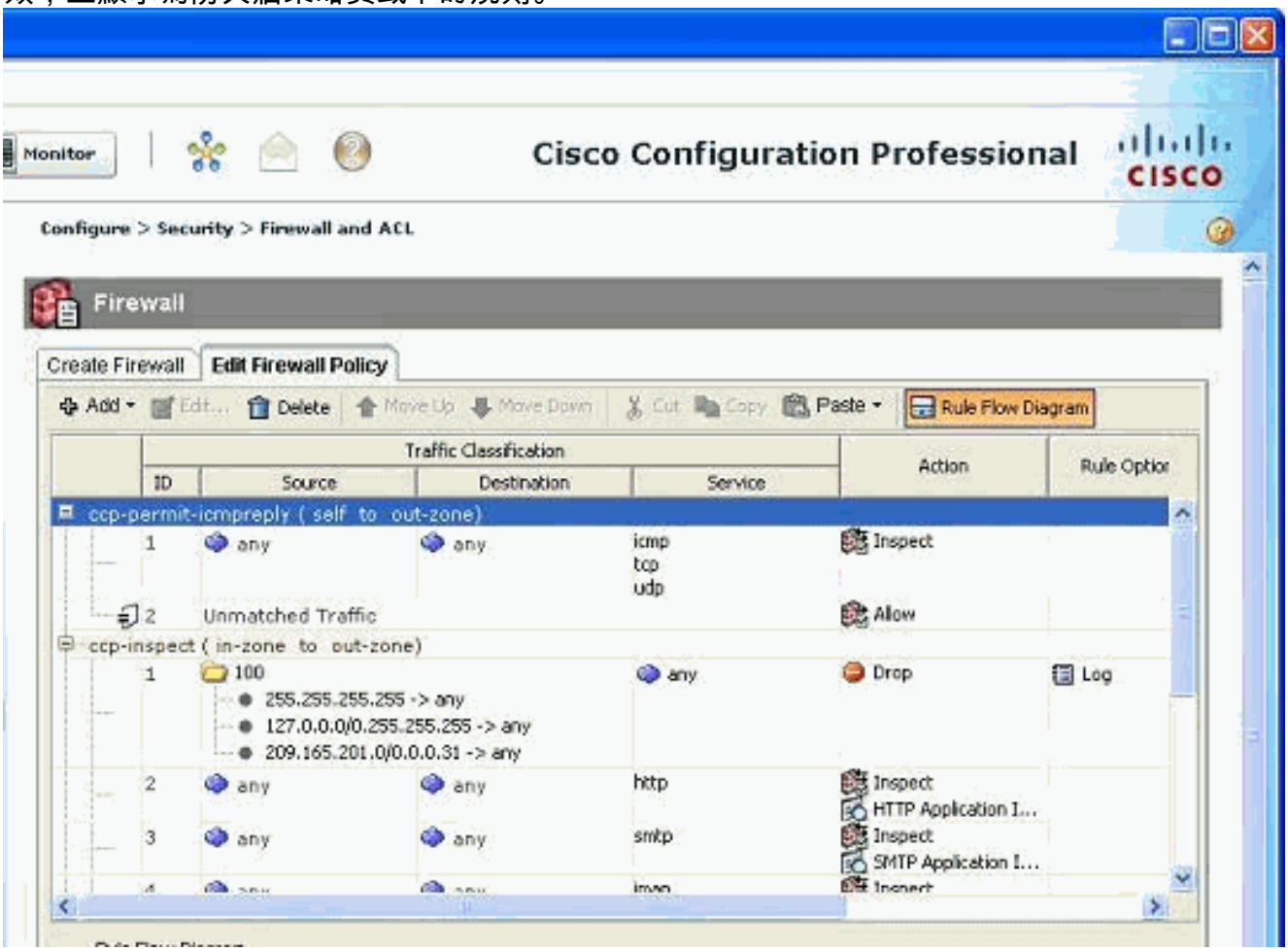
整個組態都會傳送到路由器。這需要一些時間進行處理。



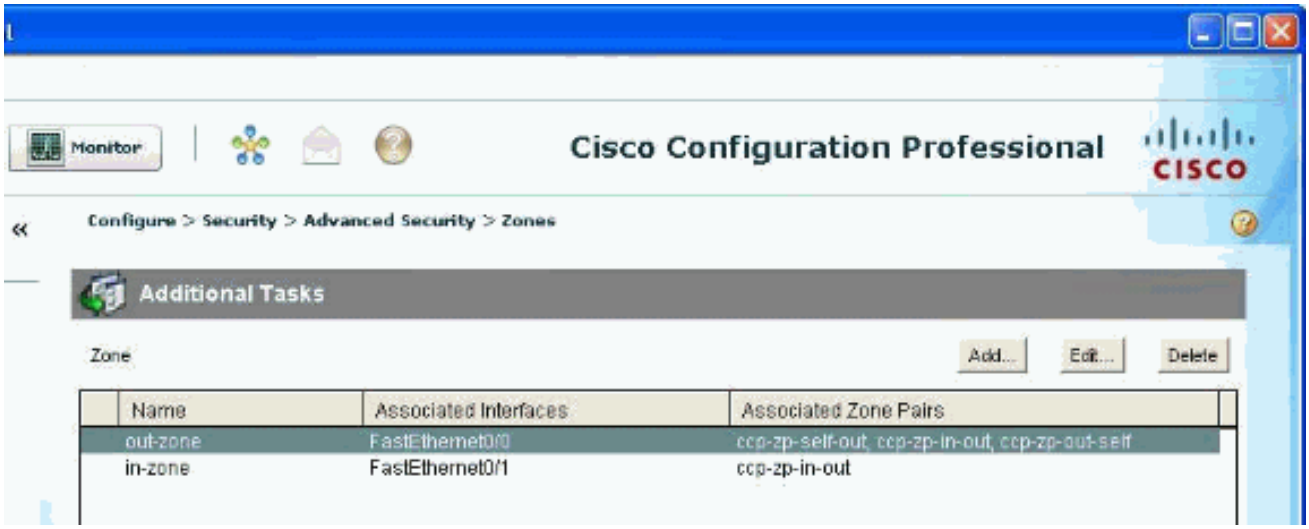
8. 按一下**OK**繼續。

9. 再次按一下**OK**。

配置現在生效，並顯示為防火牆策略頁籤下的規則。

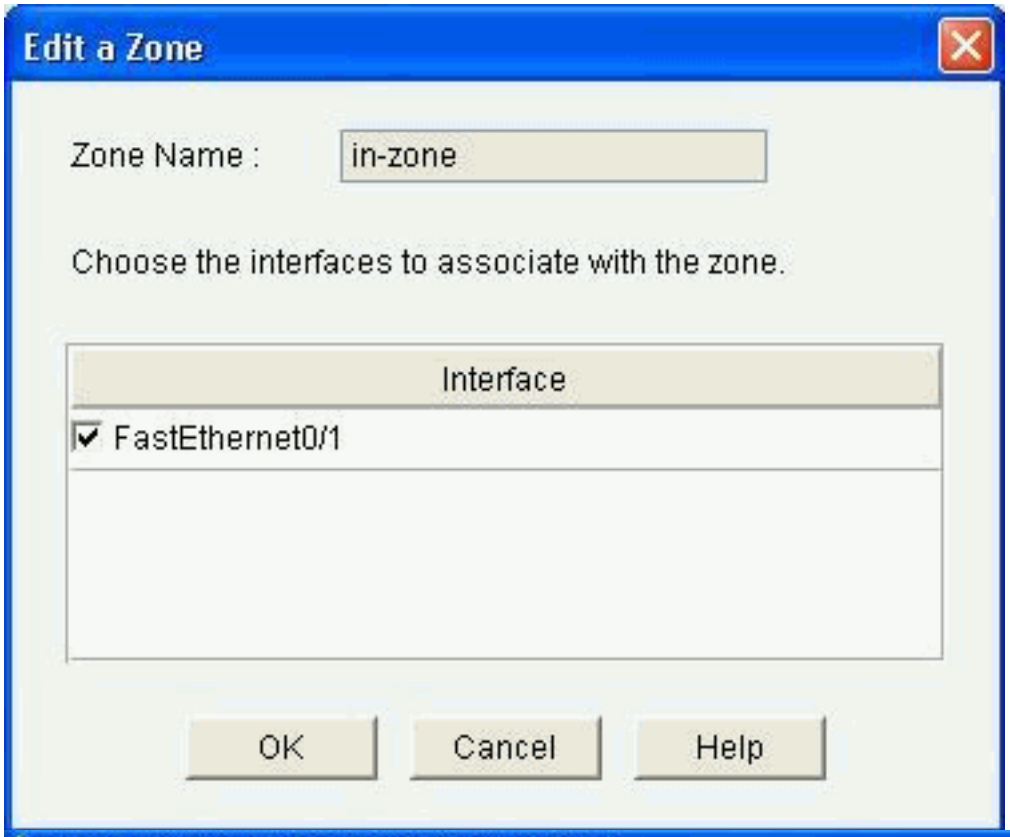


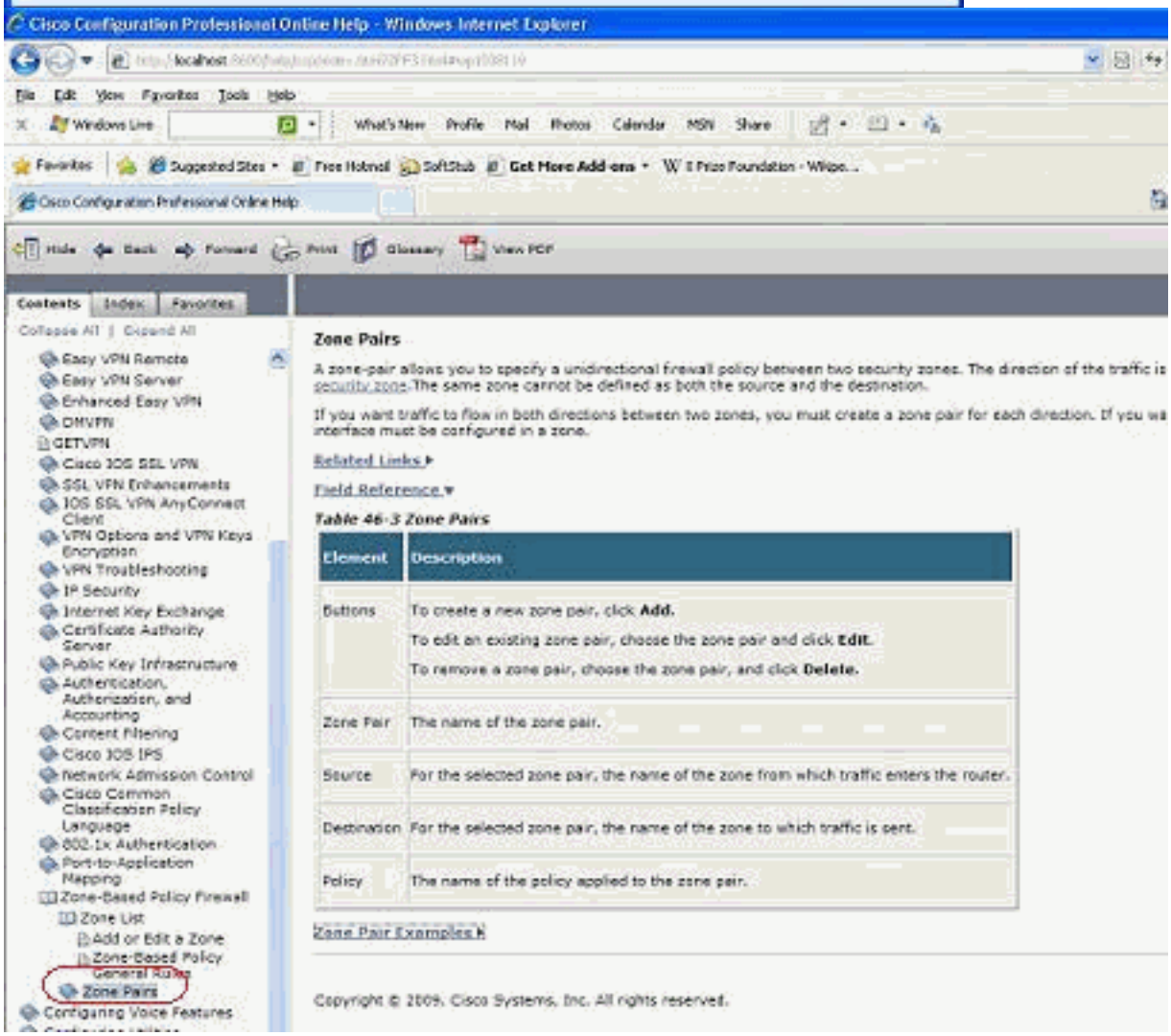
10. 如果轉至**配置>安全性>高級安全性>區域**，可以檢視區域以及與其關聯的區域對。還可以通過按一下**Add**新增新區域，或者通過按一下**Edit**修改現有區域。



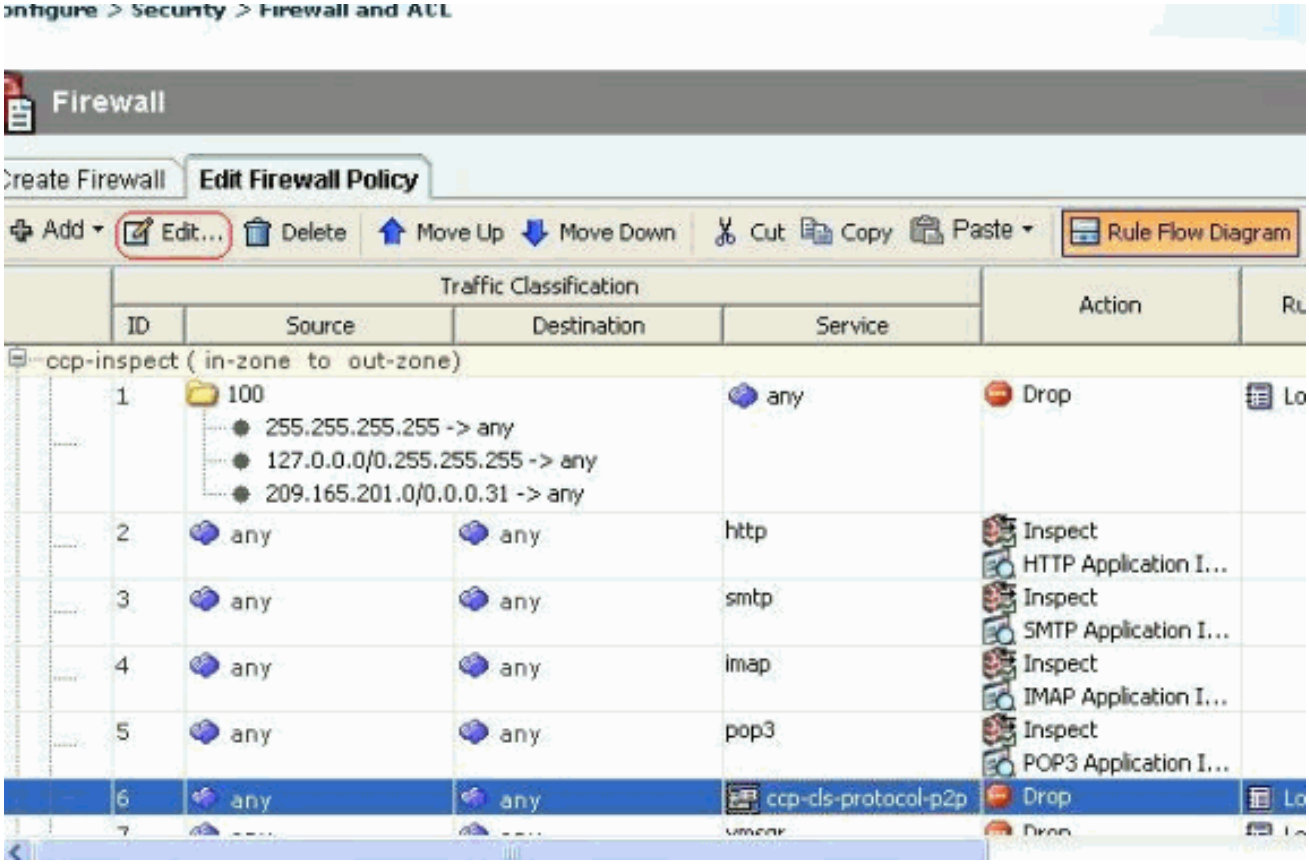
11. 轉到**Configure > Security > Advanced Security > Zone Pairs**以檢視區域對的詳細資訊。

有關修改/新增/刪除區域/區域對及其他相關資訊的即時幫助可通過Cisco CP中的內建網頁獲得。

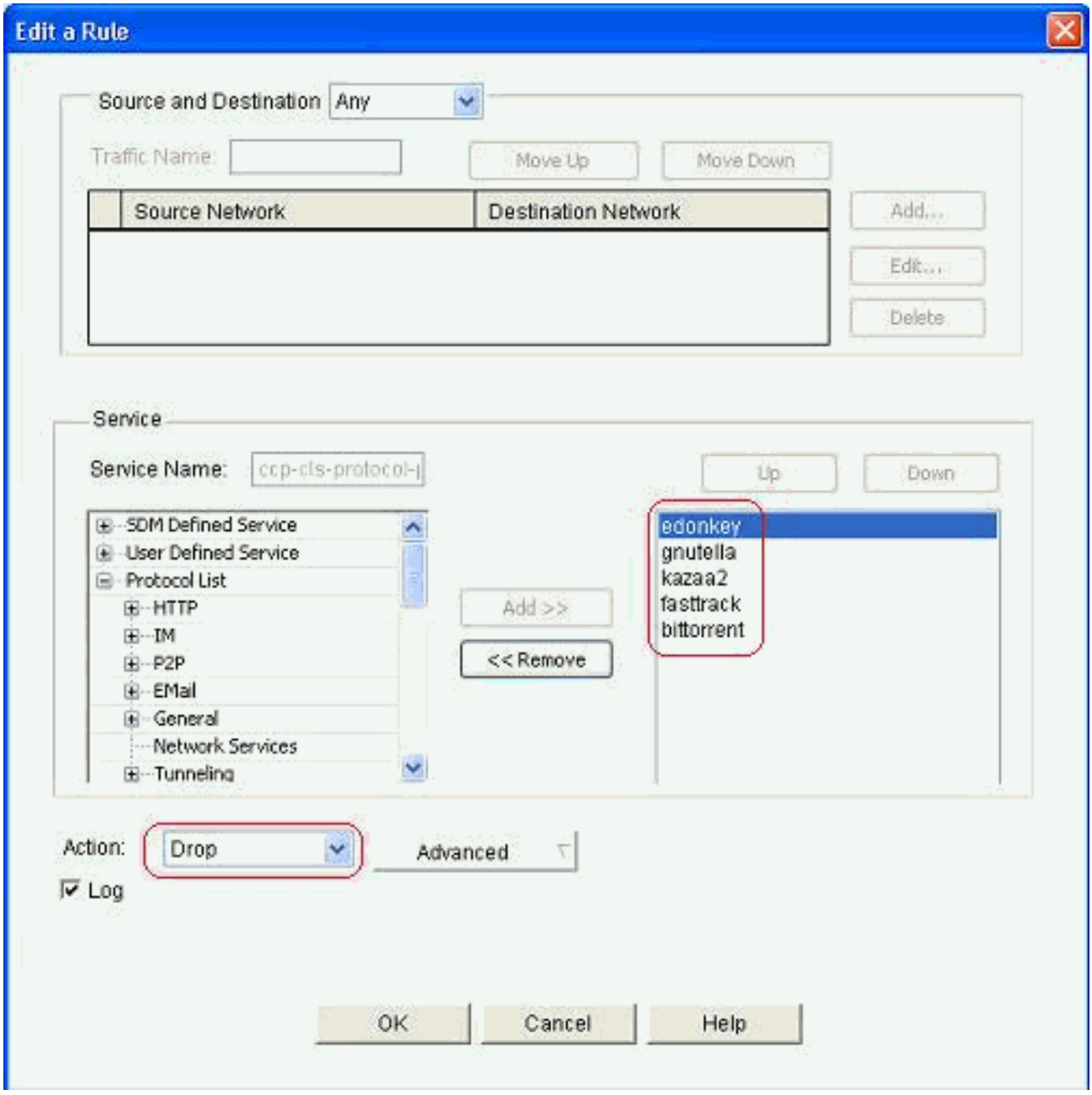




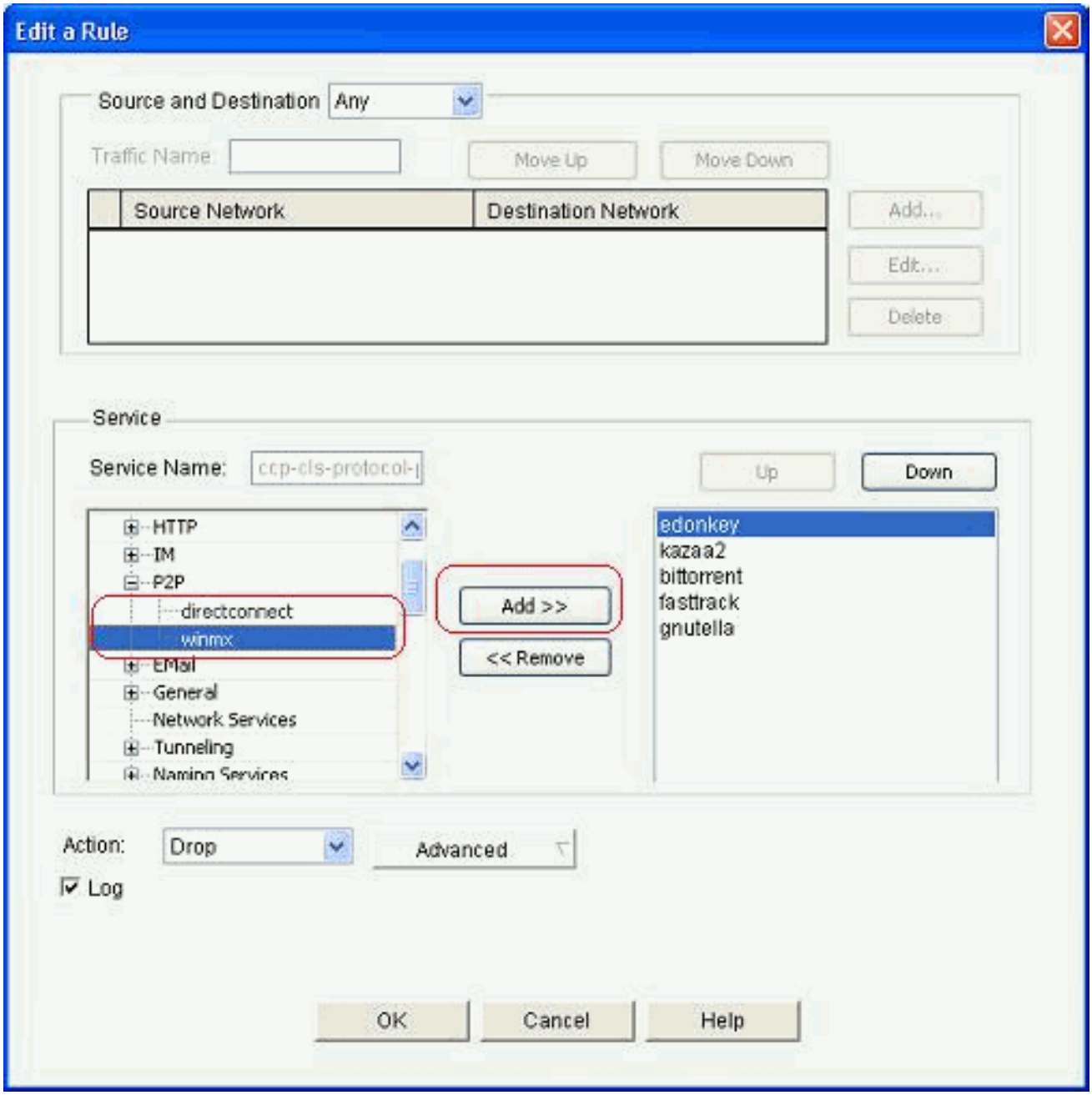
12. 若要修改某些P2P應用程式的應用程式特定檢查功能，請轉至**Configuration > Security > Firewall and ACL**。然後，按一下**Edit Firewall Policy**，並在策略對映中選擇相應的規則。按一下「**Edit**」。

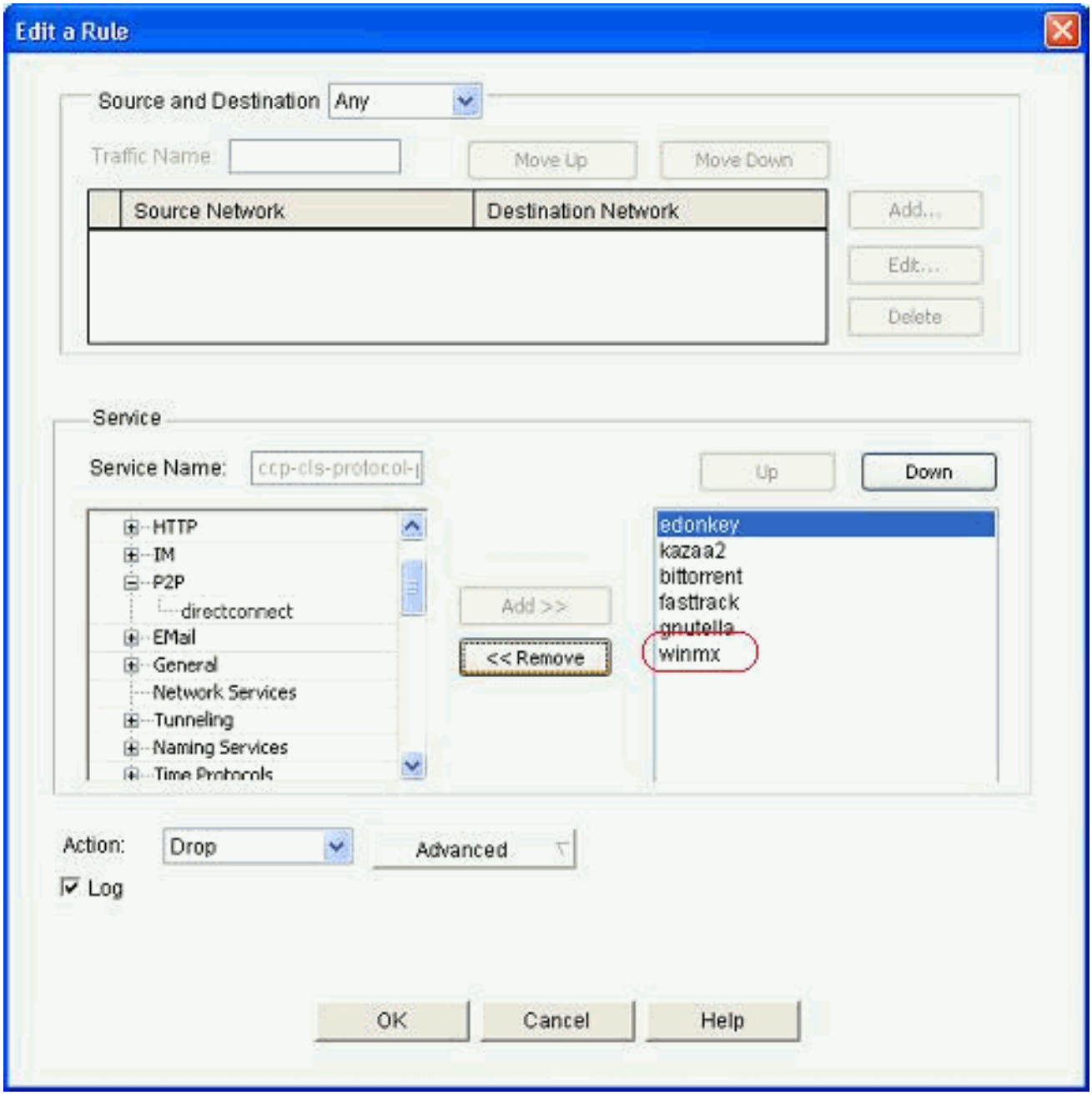


這顯示預設配置將阻止的當前P2P應用程式。

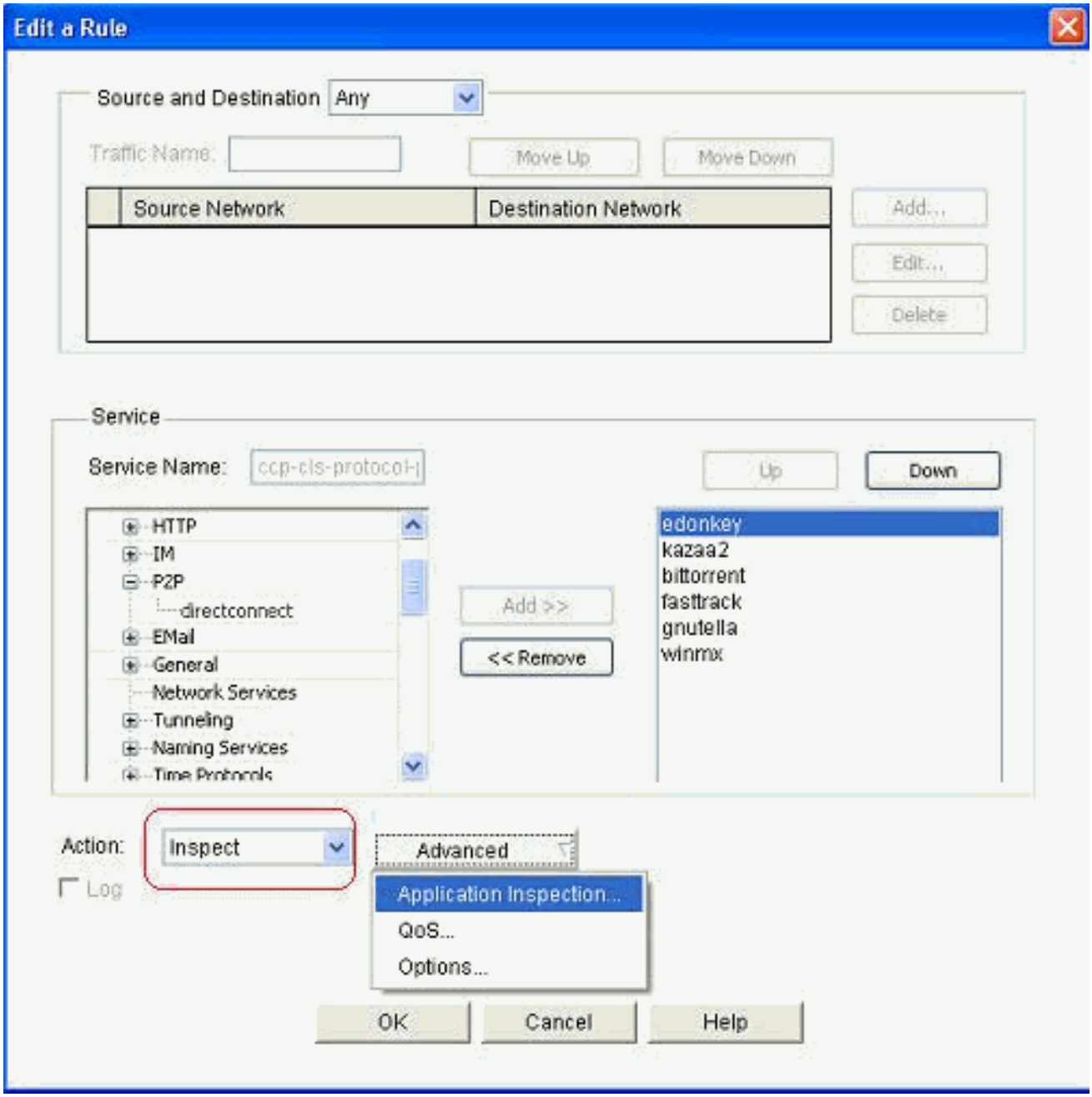


13. 您可以使用「新增」和「刪除」按鈕來新增/刪除特定的應用程式。此螢幕截圖顯示如何新增winmx應用程式以阻止該操作。


Edit a Rule
Source and Destination
Any
Traffic Name
Move Up
Move Down
Source Network
Destination Network
Add...
Edit...
Delete
Service
Service Name:
ccp-cls-protocol-
Up
Down
HTTP
IM
P2P
directconnect
winmx
EMail
General
Network Services
Tunneling
Add >>
<< Remove
edonkey
kazaa2
bittorrent
fasttrack
gnutella
Action:
Drop
Advanced
Log
OK
Cancel
Help

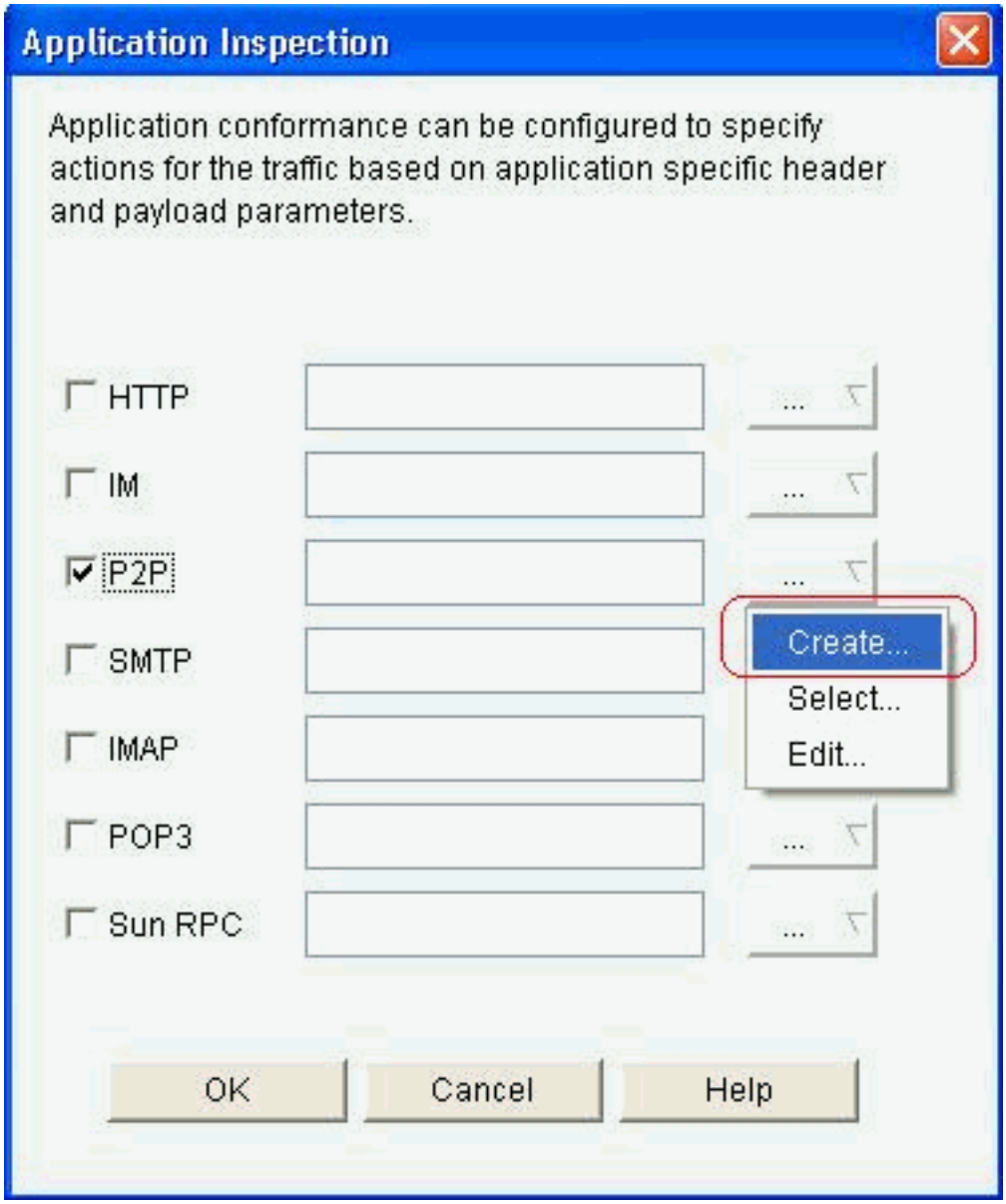


14. 也可以選擇Inspect（檢查）操作來應用不同的選項進行深度資料包檢查，而不是選擇丟棄操作。

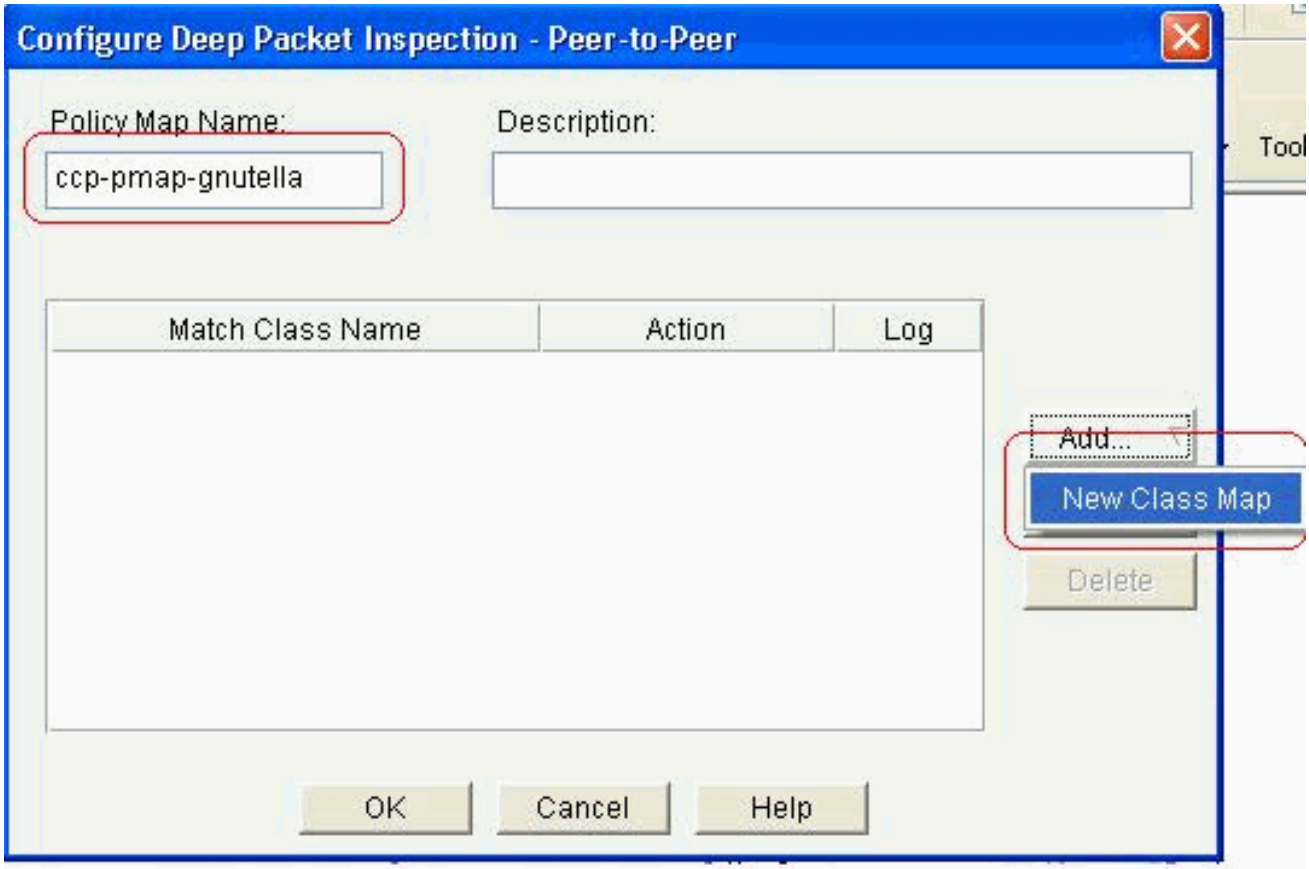


P2P檢測為應用流量提供第4層和第7層策略。這意味著ZFW可以提供允許或拒絕流量的基本狀態檢測，以及對各種協定中的特定活動進行精細的第7層控制，從而允許某些應用活動而拒絕其他應用活動。在此應用程式檢測中，您可以對P2P應用程式應用不同型別的具體標題級別檢測。下面顯示了gnutella的一個示例。

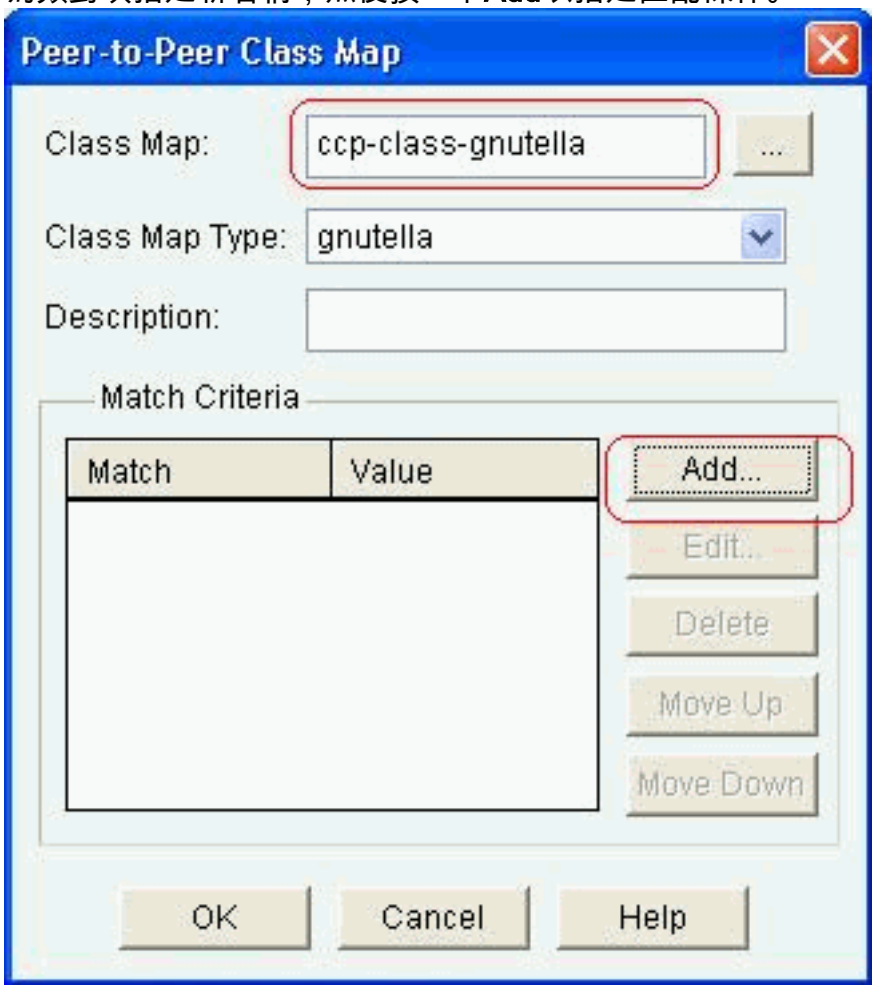
15. 選中**P2P**選項，然後按一下**Create**以為此選項建立新的策略對映。



16. 為gnutella協定建立用於深度資料包檢測的新策略對映。按一下**Add**，然後選擇**New Class Map**。

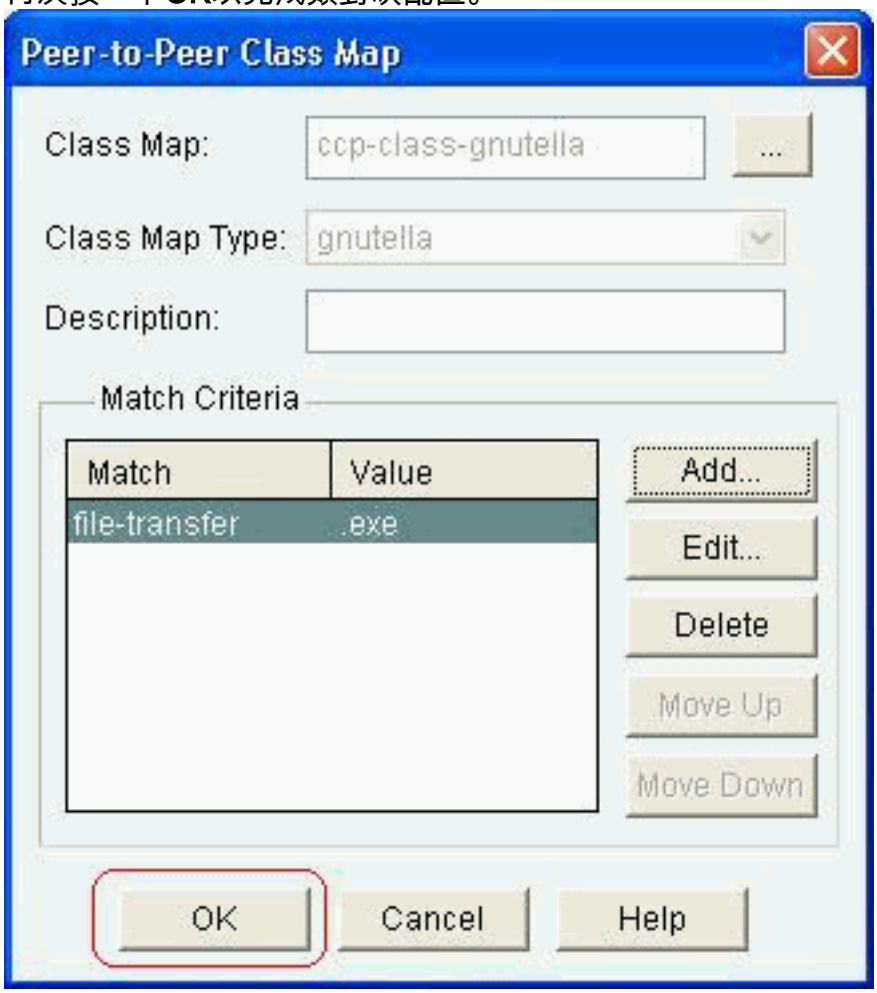


17. 為類對映指定新名稱，然後按一下**Add**以指定匹配條件。

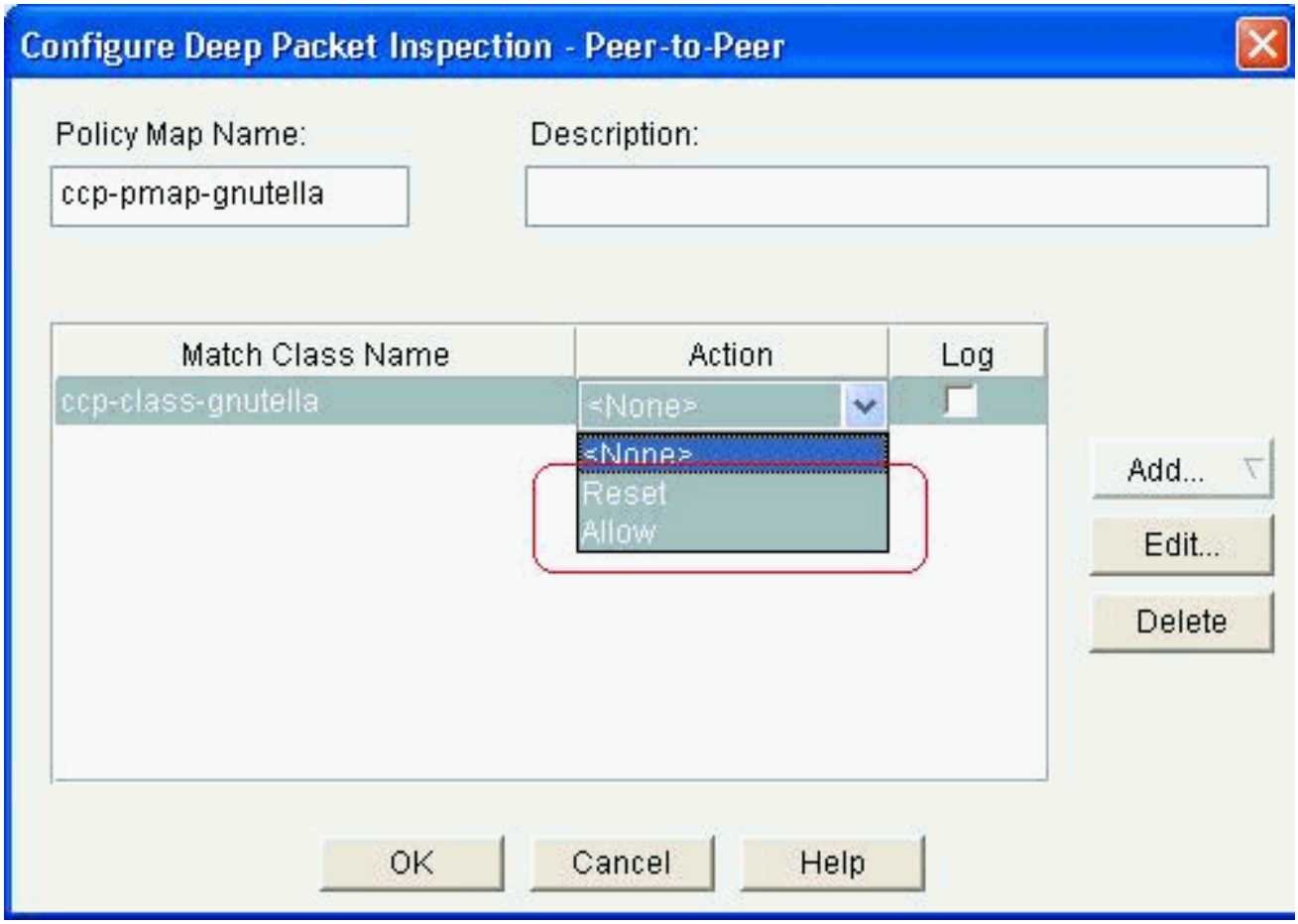


18. 使用file-transfer作為匹配條件，使用的字串是.exe。這表示所有包含.exe字串的gnutella檔案傳輸連線都與流量策略匹配。按一下「**OK**」（確定）。

19. 再次按一下**OK**以完成類對映配置。

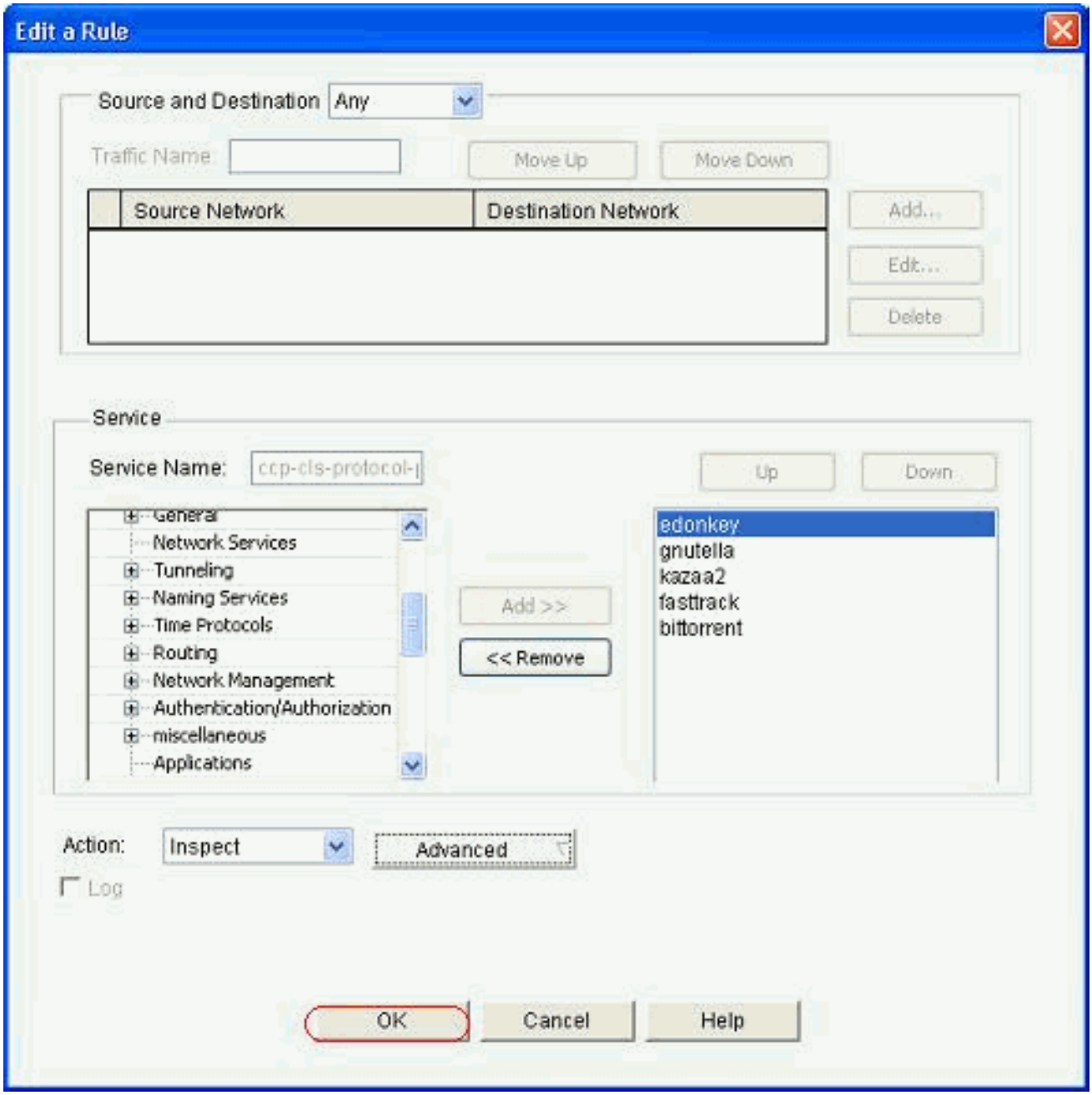


20. 選擇**Reset**或**Allow**選項，取決於貴公司的安全策略。按一下**OK**以使用策略對映確認操作。



同樣，通過指定不同的正規表示式作為匹配條件，您可以新增其他策略對映來為其他P2P協定實現深度檢測功能。**註**意：由於「埠跳躍」行為和其他避免檢測的技巧，以及頻繁更改和更新修改協定行為的P2P應用所引起的問題，P2P應用尤其難以檢測。ZFW將本地防火牆狀態檢測與基於網路的應用識別(NBAR)的流量識別功能相結合，提供P2P應用控制。**注意**：P2P應用檢測為第4層檢測所支援的應用子集提供特定於應用的功能：edonkeyfasttrack格努特拉kazaa2**注意：**目前，ZFW沒有檢查「bittorrent」應用流量的選項。BitTorrent客戶端通常通過運行在某些非標準埠上的HTTP與跟蹤器（對等目錄伺服器）通訊。這通常是TCP 6969，但您可能需要檢查Torrent特定的跟蹤器埠。如果您希望允許BitTorrent，容納額外埠的最佳方法是將HTTP配置為匹配協定之一，並使用以下ip port-map命令將TCP 6969新增到HTTP:**ip port-map http port tcp 6969**。您需要將http和bitTorrent定義為應用於類對映的匹配條件。

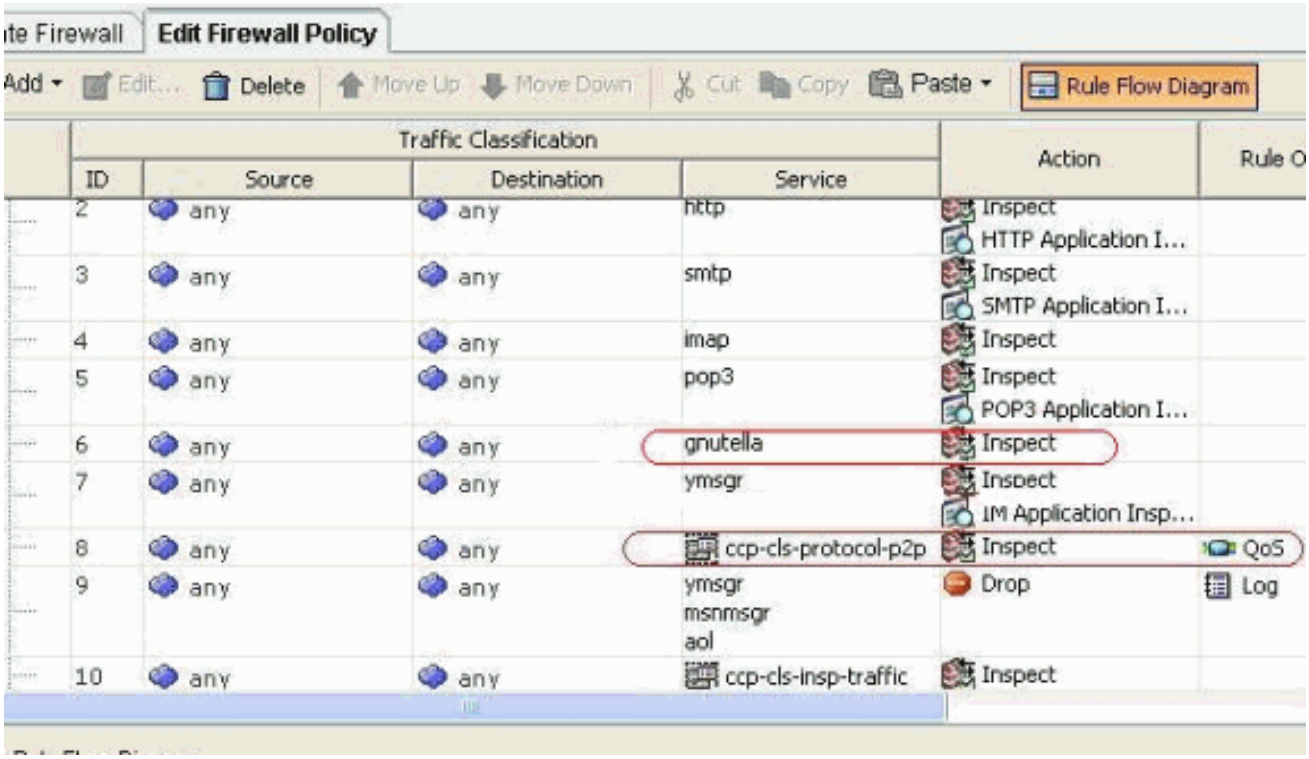
21. 按一下**OK**完成Advanced Inspection配置。



相應的命令集將傳送給路由器。

22. 按一下「**OK**」，將一組命令複製到路由器。

23. 您可以從**Configure > Security > Firewall and ACL**下的Edit Firewall Policy頁籤中觀察新規則的執行情況。



ZFW路由器的命令列配置

Cisco CP上一節中的配置導致ZFW路由器上的以下配置：

ZBF路由器
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#
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

- ZBF-Router**#show policy-map type inspect zone-pair sessions** — 顯示所有現有區域對的運行時檢查型別策略對映統計資訊。

相關資訊

- 基於區域的策略防火牆設計和應用指南
- Cisco IOS防火牆經典和基於區域的虛擬防火牆應用配置示例
- 思科配置專業版首頁