Cisco CP — 配置ZFW以阻止点对点流量

目录

[简介](#)
[先决条件](#)
[要求](#)
[运行 Cisco CP 的路由器配置](#)
[使用的组件](#)
[规则](#)
[背景信息](#)
[配置](#)
[网络图](#)
[通过Cisco Configuration Professional进行配置](#)
[ZFW路由器的命令行配置](#)
[验证](#)
[相关信息](#)

简介

本文档提供了使用思科配置专家(Cisco CP)中的高级防火墙配置向导将Cisco IOS路由器配置为基于区域的防火墙以阻止点对点(P2P)流量的分步方法。

区域策略防火墙（也称为区域-策略防火墙，简称 ZFW）弃用了传统的基于接口的防火墙配置模型，而改用更加灵活并且易于理解的区域模型。这种模型首先将接口指定给区域，然后对区域之间往来的数据流应用检查策略。区域间策略提供了相当大的灵活性和精细度。因此，可以将不同的检查策略应用于连接到同一路由器接口的多个主机组。区域建立了网络的安全边界。区域定义了数据流在流向网络中其他区域的过程中受策略限制的边界。ZFW 的默认区域间策略是“全部拒绝”。如果未明确配置任何策略，则将阻止所有数据流在区域间移动。

P2P应用是互联网上应用最广泛的应用之一。P2P网络可以充当蠕虫等恶意威胁的通道，提供绕过防火墙的简单路径，并引起对隐私和安全的担忧。思科IOS软件版本12.4(9)T引入了对P2P应用的ZFW支持。P2P检测为应用流量提供第4层和第7层策略。这意味着ZFW可以提供基本状态检测以允许或拒绝流量，以及对各种协议中特定活动的精细第7层控制，从而允许某些应用活动，而拒绝其他应用活动。

Cisco CP通过使用高级防火墙配置向导，提供了一种易于跟踪的分步方法，将IOS路由器配置为基于区域的防火墙。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- IOS路由器的软件版本必须为12.4(9)T或更高版本。
- 有关支持Cisco CP的IOS路由器型号，请参阅Cisco CP版本说明。

运行 Cisco CP 的路由器配置

注意：要在Cisco路由器上运行Cisco CP，请执行以下配置步骤：

```
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
```

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行IOS软件版本12.4(15)T的思科1841 IOS路由器
- 思科配置专家（思科CP）版本2.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

在本文档示例中，路由器配置为基于区域的防火墙以阻止P2P流量。ZFW路由器有两个接口，一个内部（受信任）接口位于区域内，另一个外部（不受信任）接口位于区域外。ZFW路由器对从In-zone传输到Out-zone的流量执行日志记录操作，阻止P2P应用，如edonkey、fasttrack、gnutella和kazaa2。

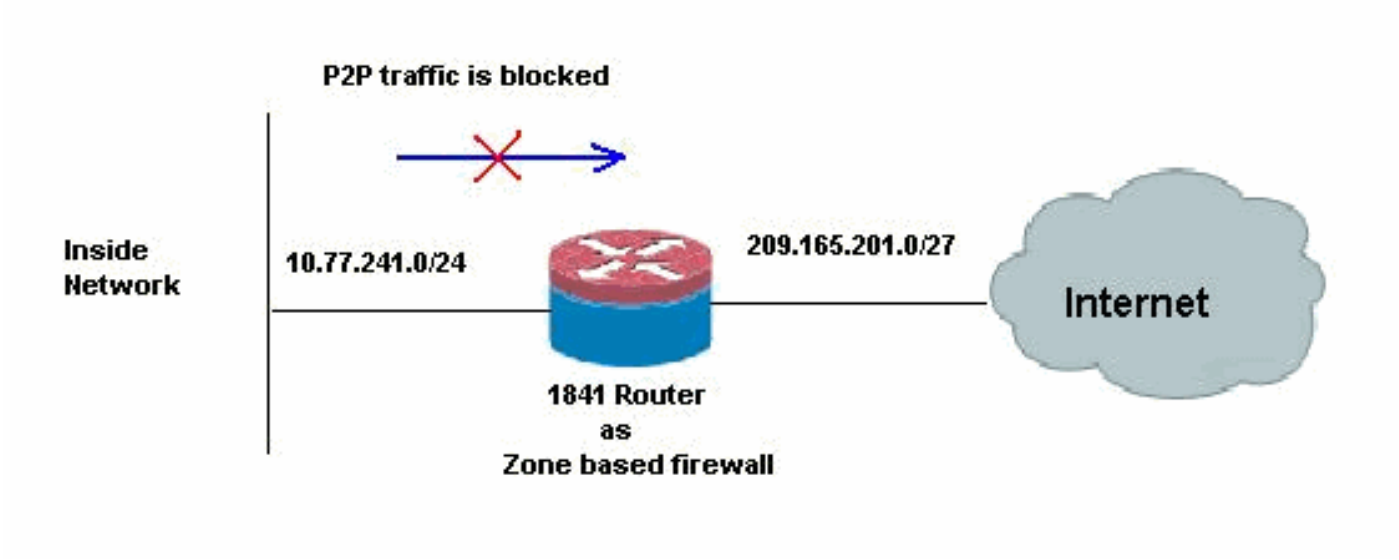
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

网络图

本文档使用以下网络设置：

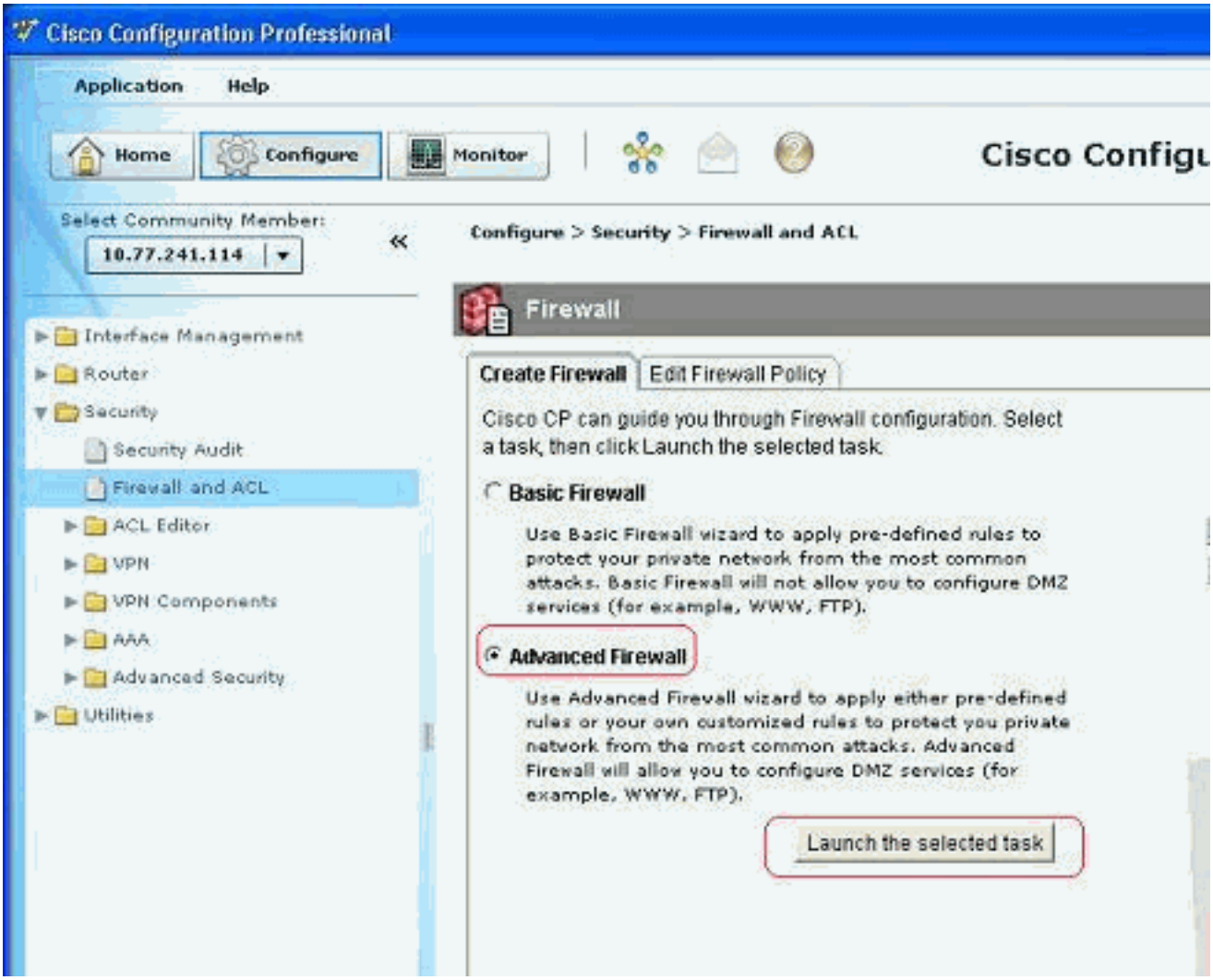


通过Cisco Configuration Professional进行配置

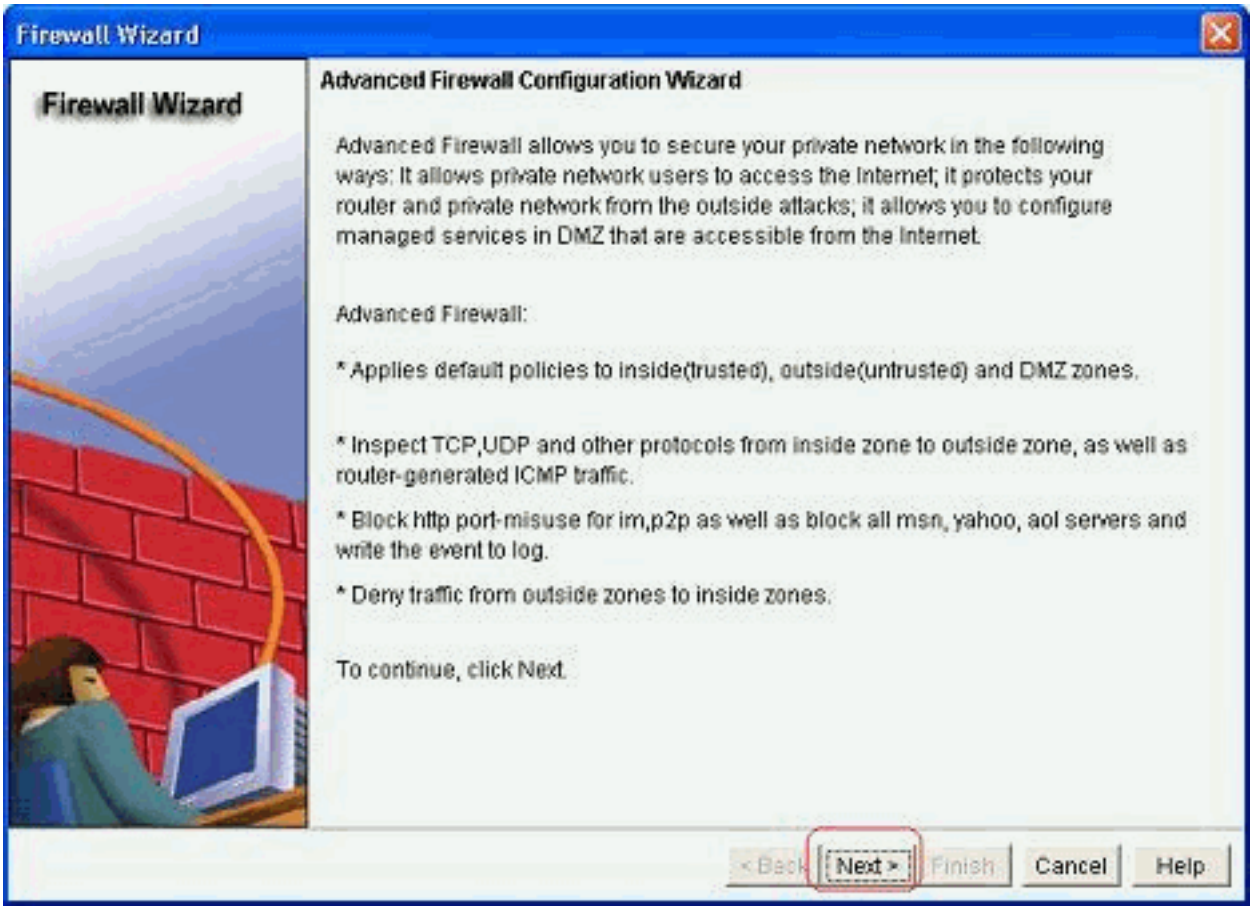
本节包含有关如何使用向导将IOS路由器配置为基于区域的防火墙的分步过程。

请完成以下步骤：

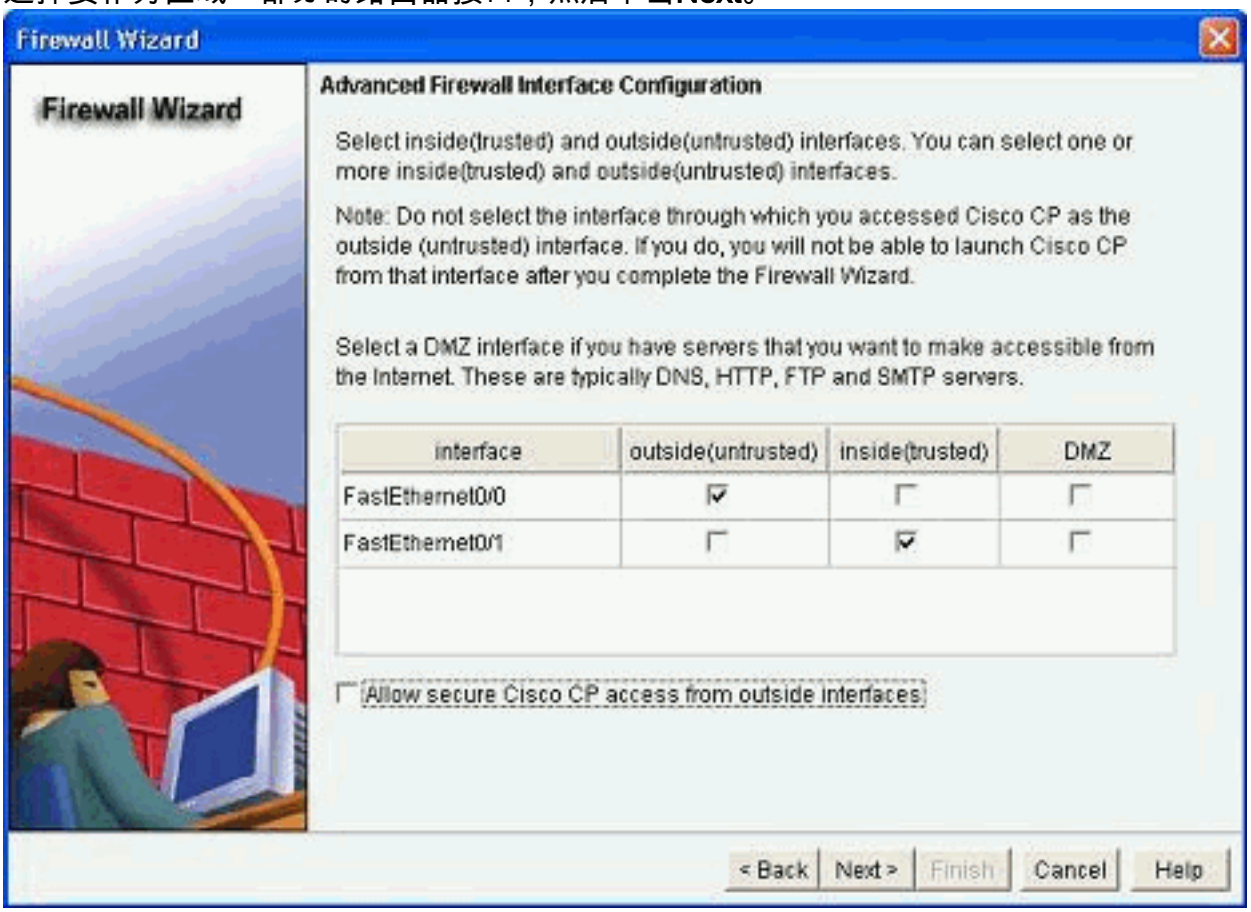
1. 转到**Configure > Security > Firewall and ACL**。然后，选择“高级**防火墙**”单选按钮。单击**Launch the selected task**。



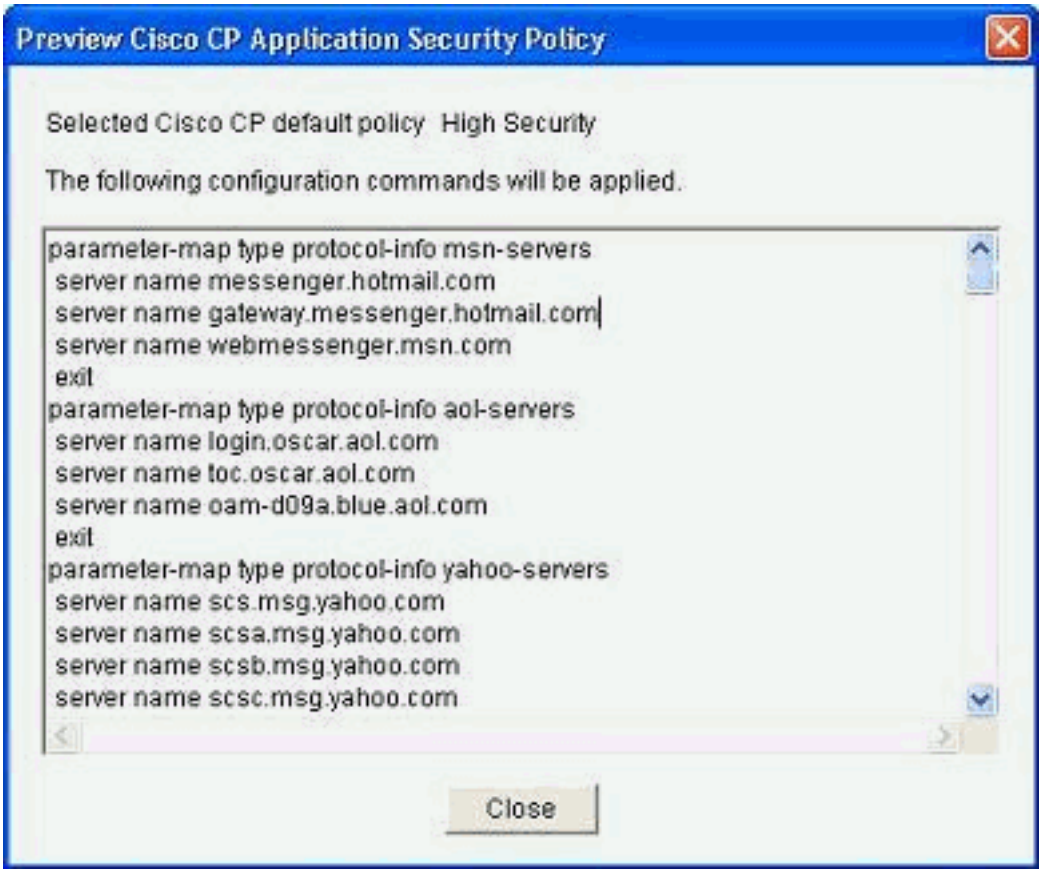
2. 下一个屏幕显示有关防火墙向导的简要介绍。单击**Next**开始配置防火墙。



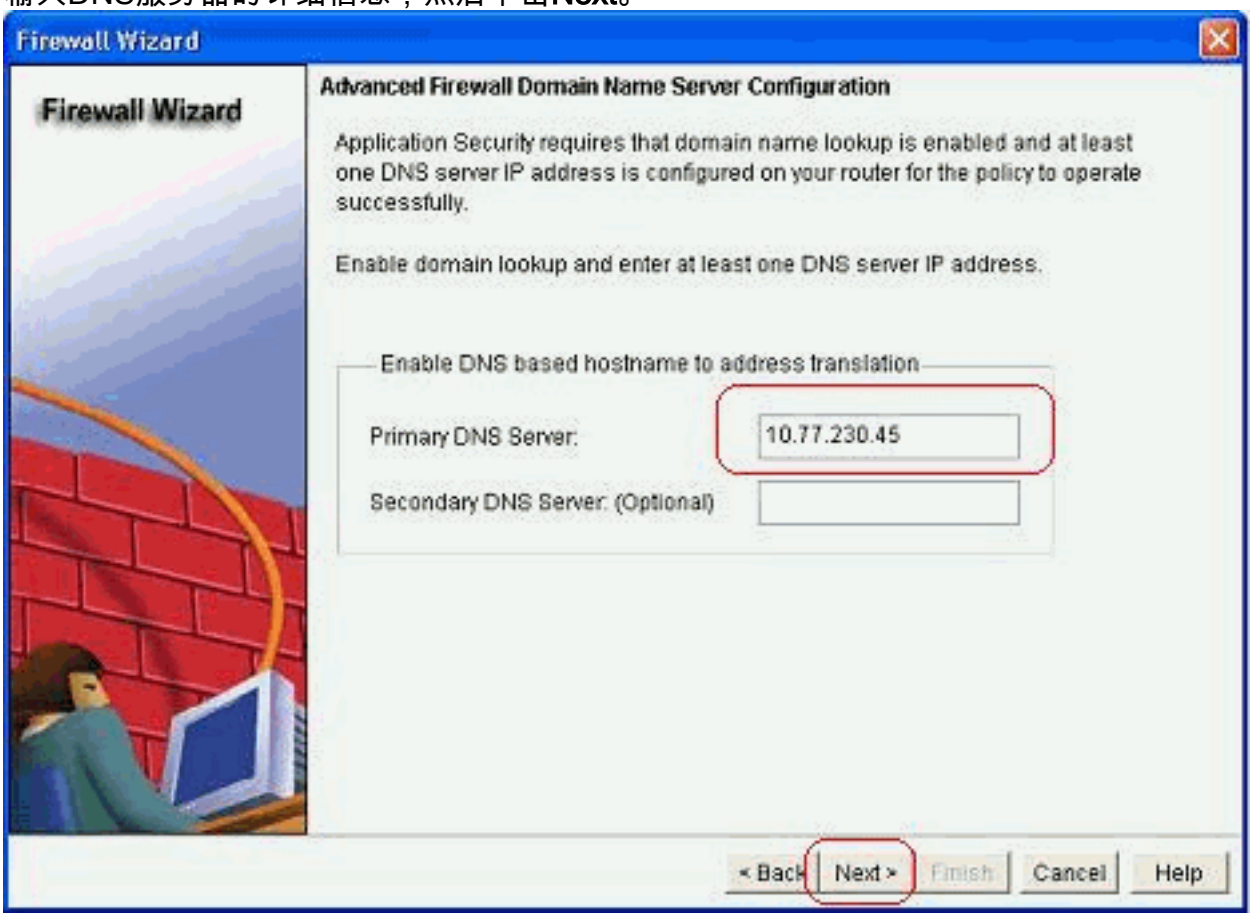
3. 选择要作为区域一部分的路由器接口，然后单击**Next**。



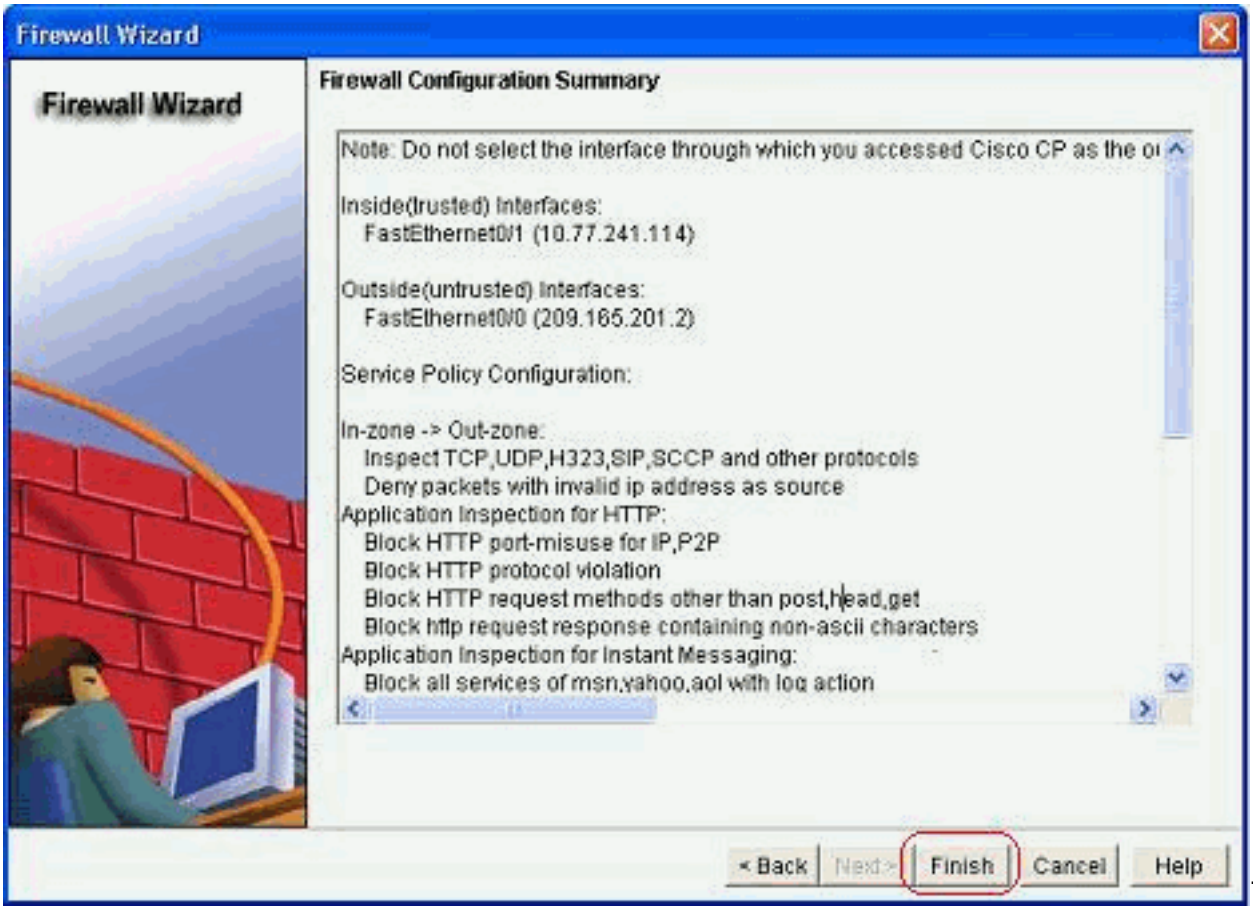
4. 下一个窗口中显示了High Security和命令集的默认策略。单击**关闭**继续。



5. 输入DNS服务器的详细信息，然后单击**Next**。

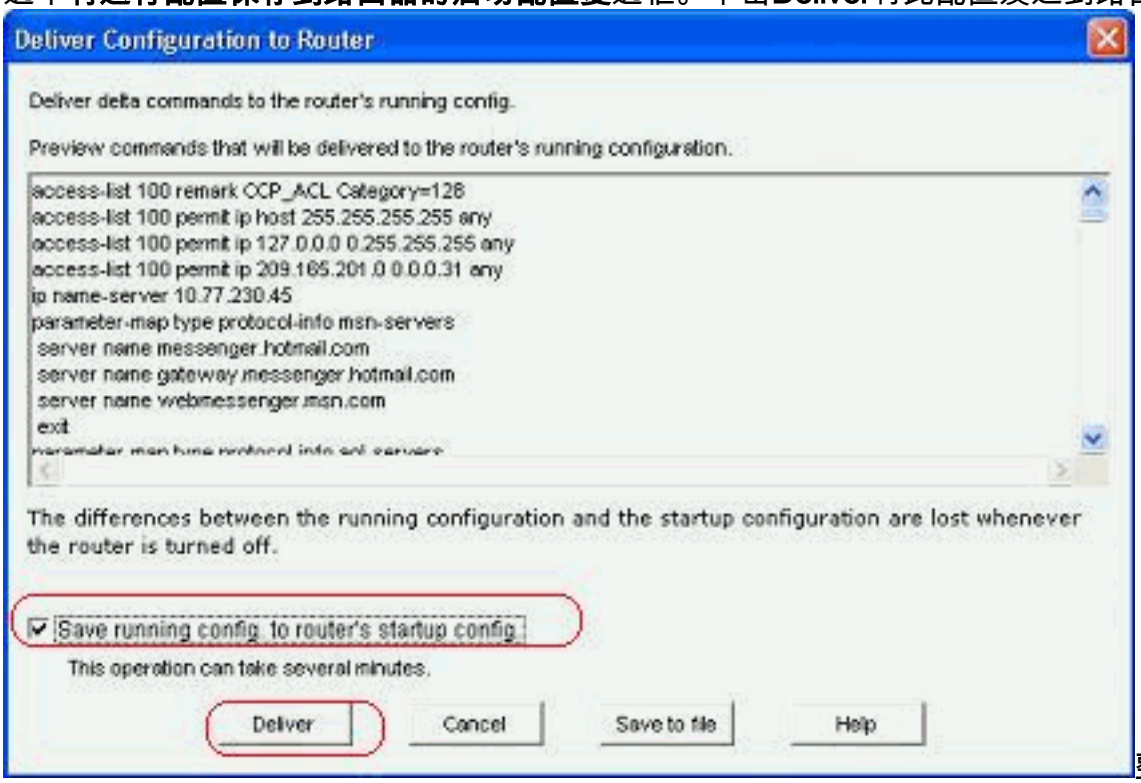


6. 思科CP提供配置摘要，如此处所示。单击**Finish**完成配置。

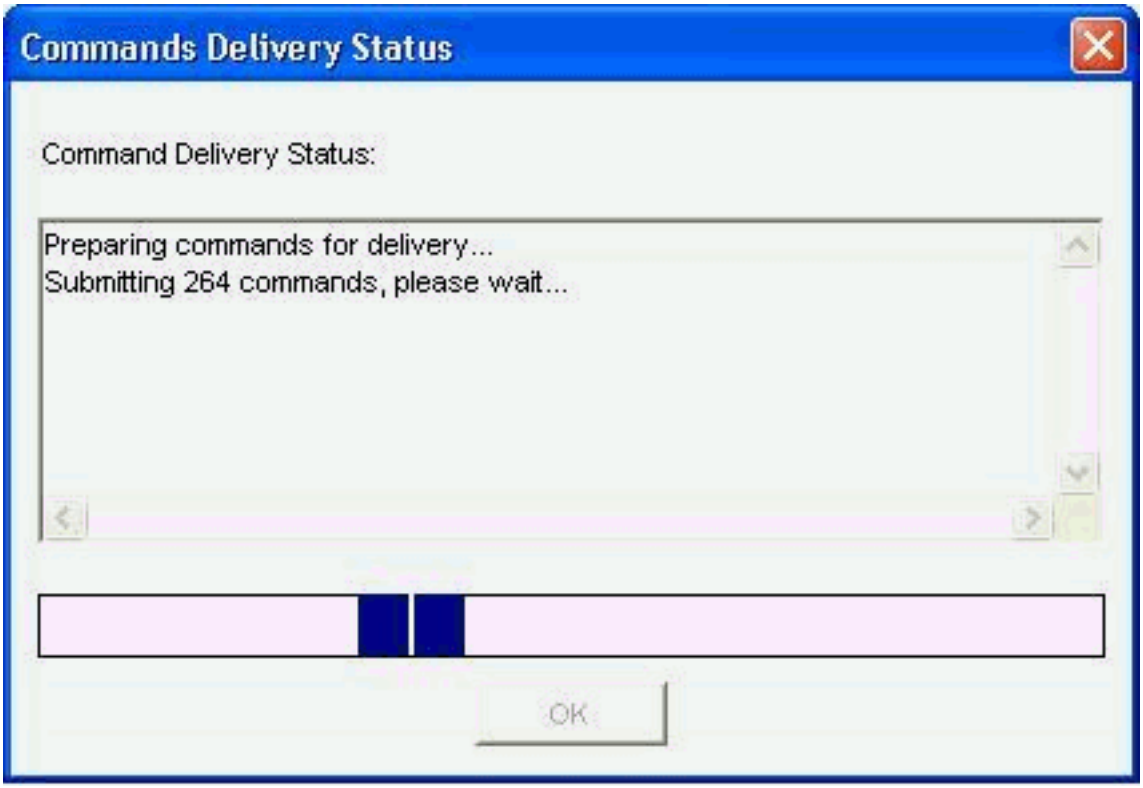


下表提供了详细的配置摘要。这是根据思科CP的高安全策略进行的默认配置。

7. 选中**将运行配置保存到路由器的启动配置复**选框。单击Deliver将此配置发送到路由器。



整个配置将传送到路由器。这需要一些时间才能处理。



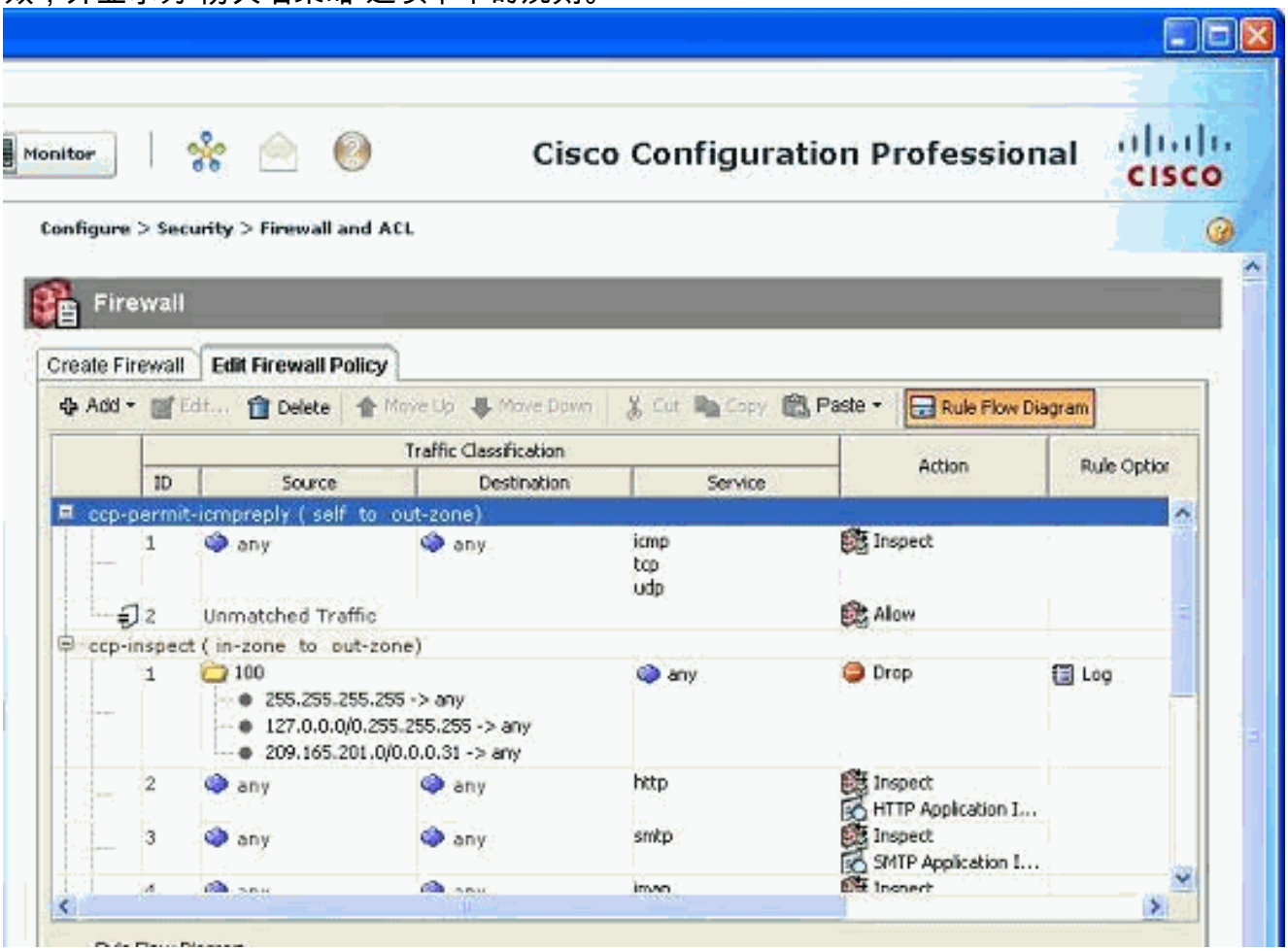
8. 单击**确定**继续。



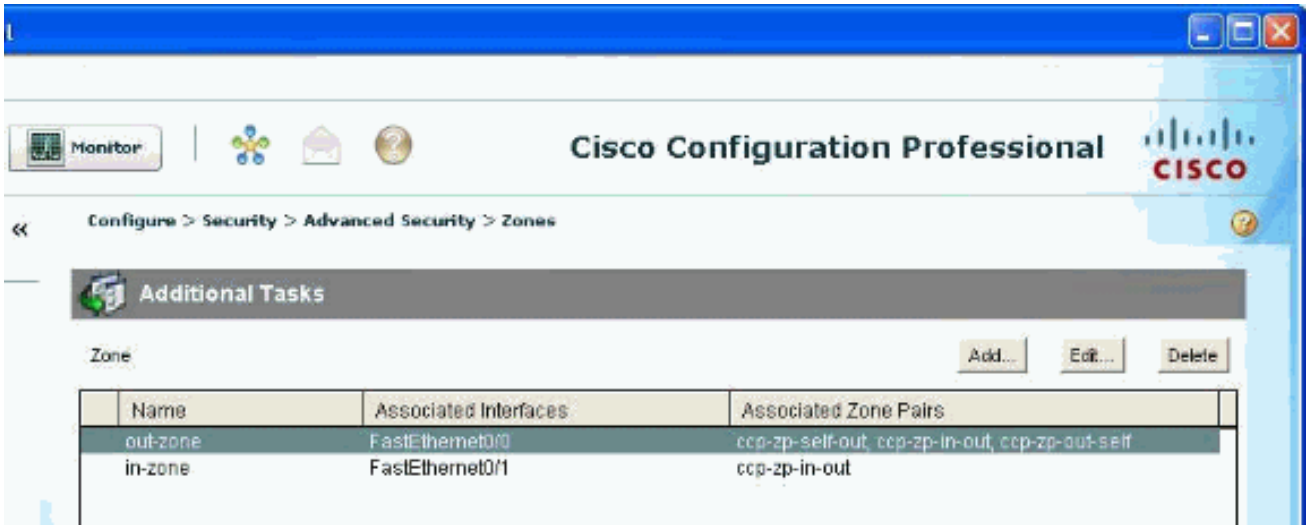
9. 再次单**击"确**定"。



配置现在生效，并显示为“防火墙策略”选项卡下的规则。



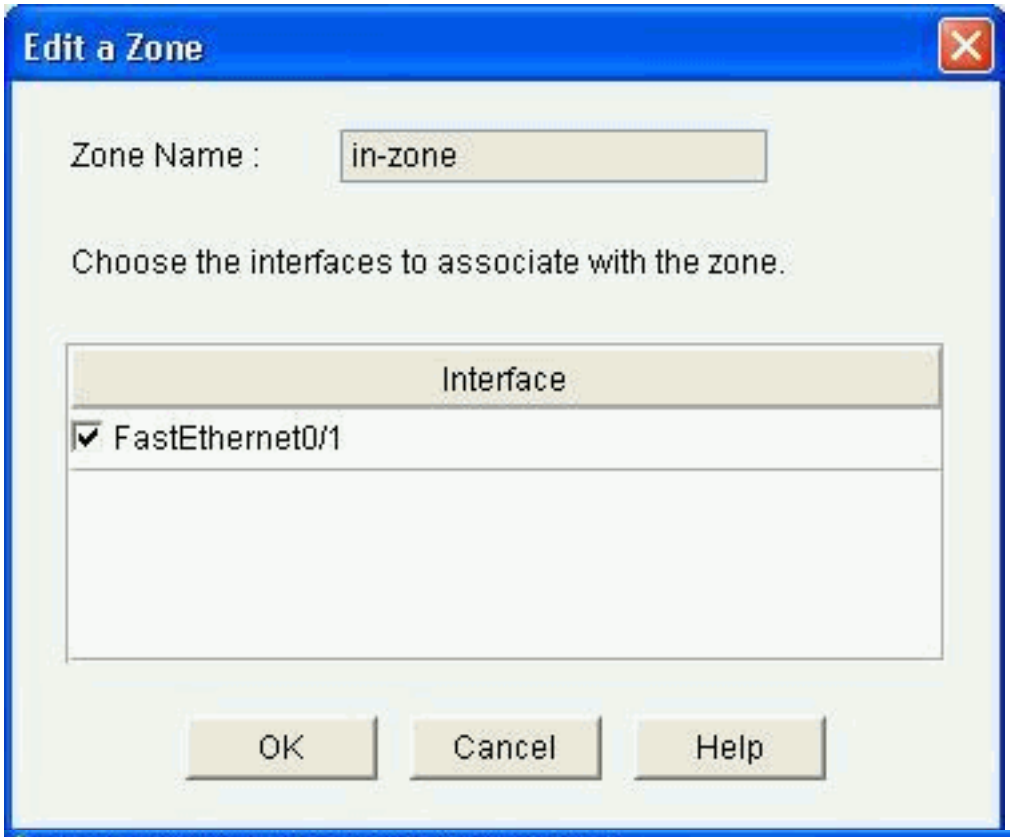
10. 如果转至Configure > Security > Advanced Security > Zones，则可以查看区域及其关联的区域对。您也可以通过单击“添加”(**Add)添**加新区域，或通过单击“编辑”(**Edit)修改现有区**域。

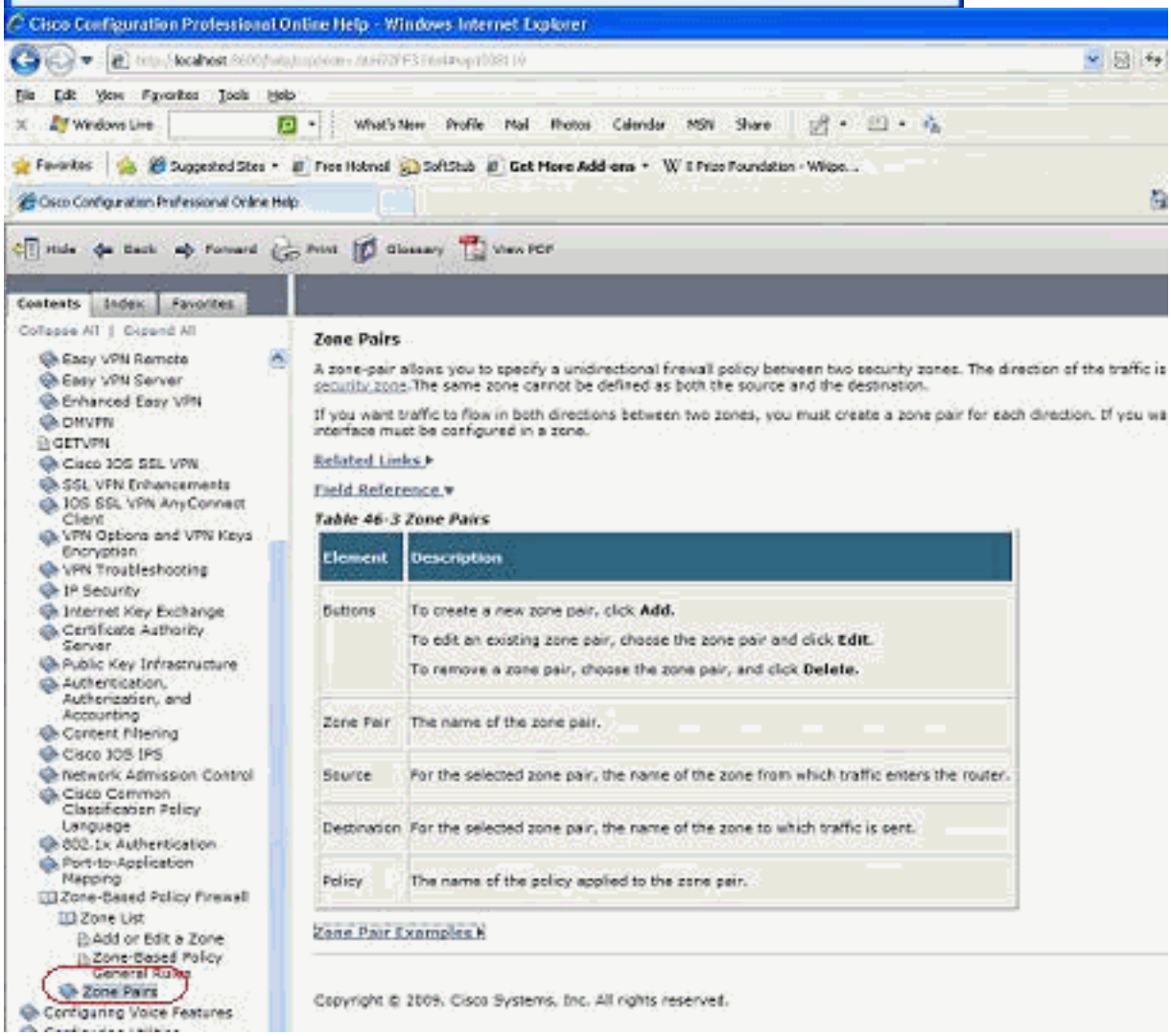


11. 转到**Configure > Security > Advanced Security > Zone Pairs**，查看区域对的详细信息。

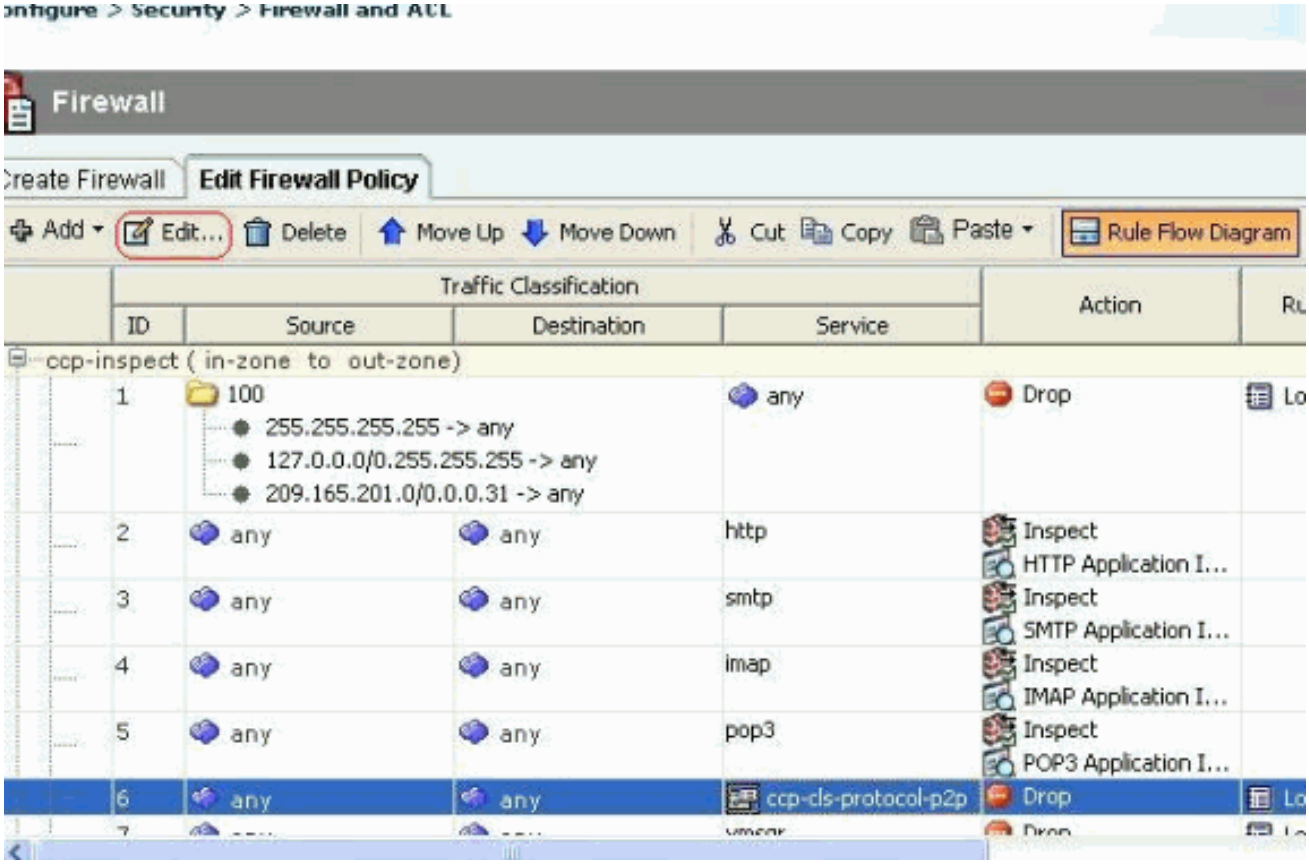


有关如何修改/添加/删除区域/区域对和其他相关信息的即时帮助，可通过思科CP中的内置网页获得。

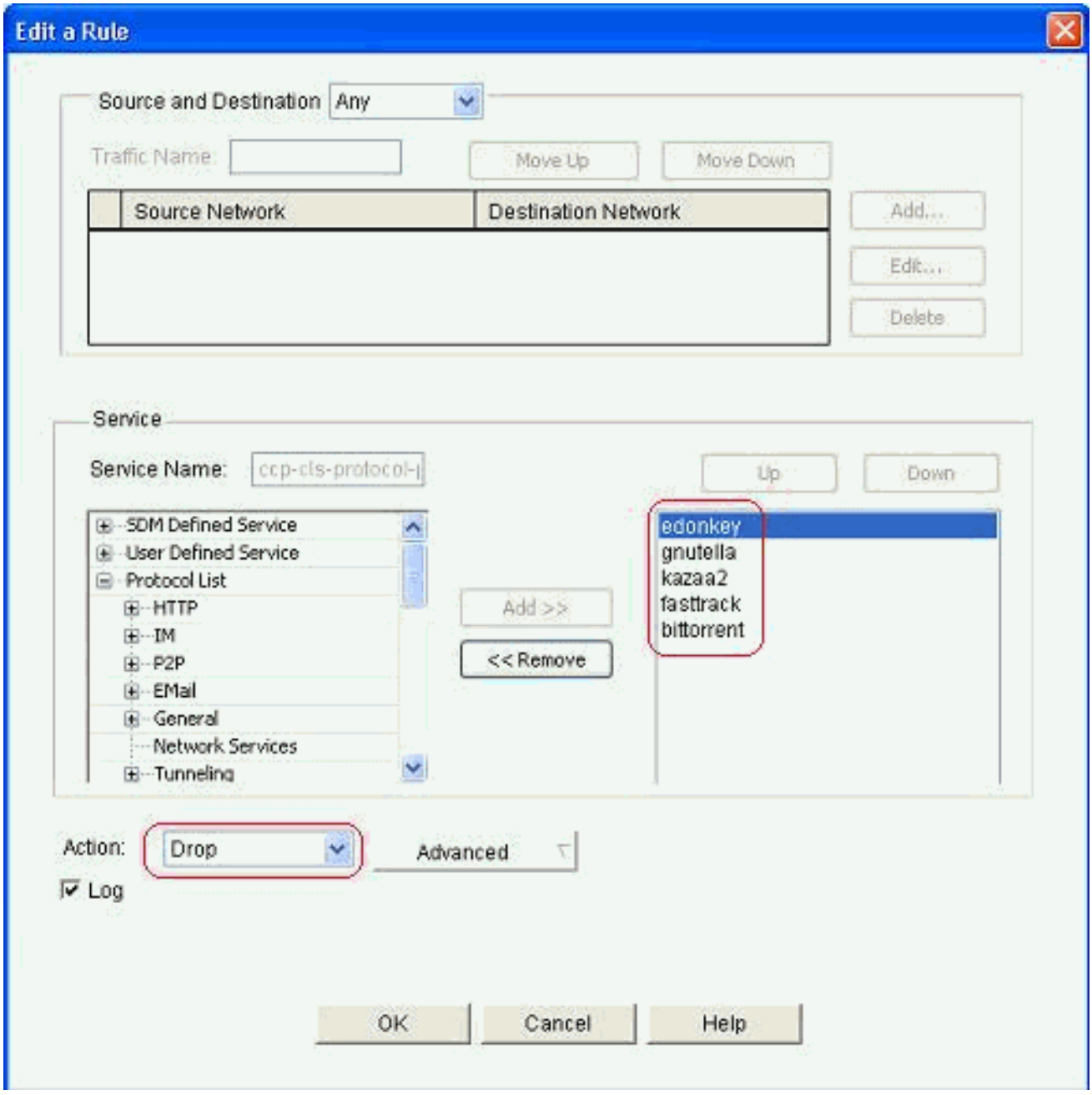




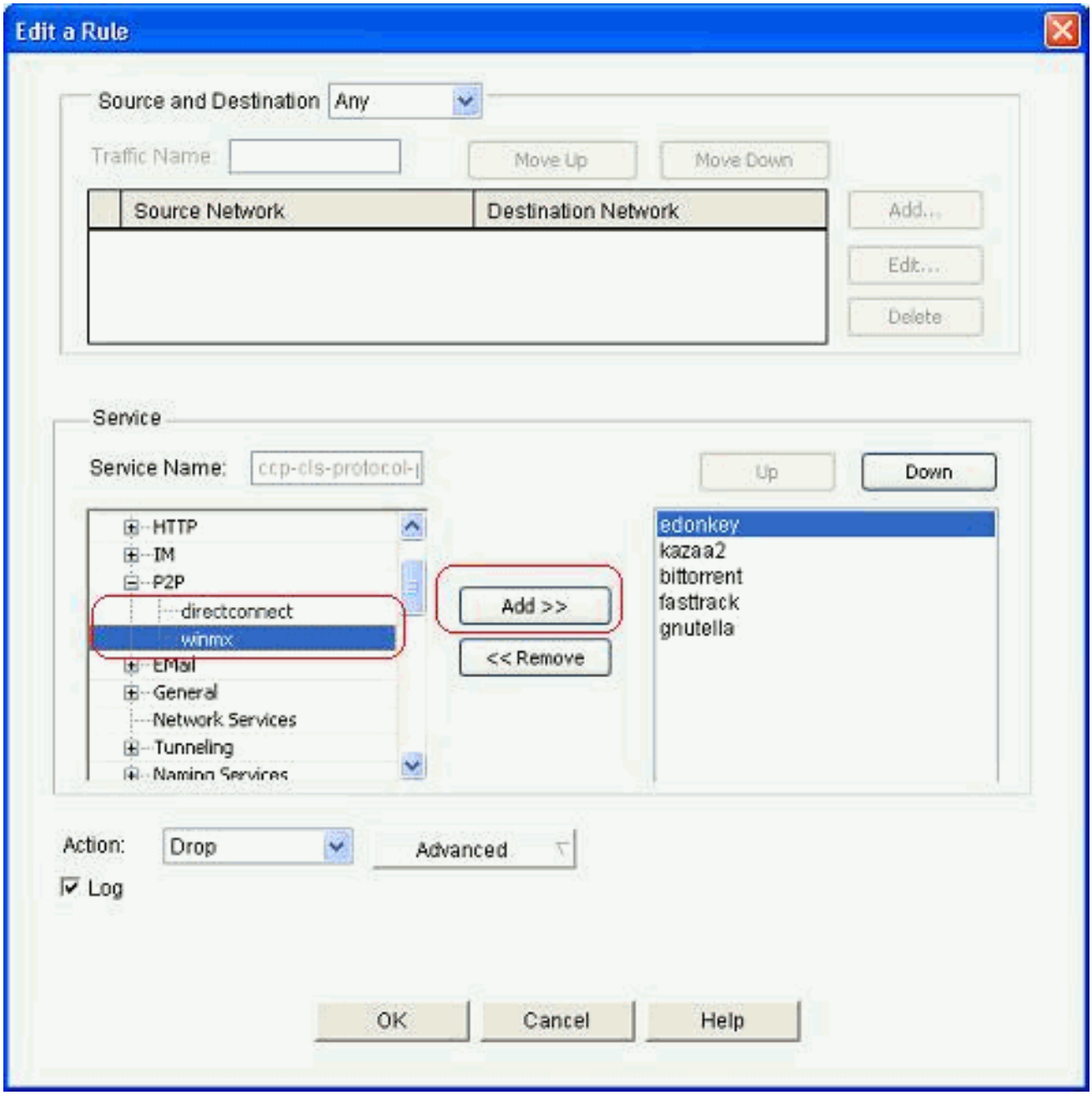
12. 要修改特定P2P应用的应用特定检测功能，请转至**Configuration > Security > Firewall and ACL**。然后，单击**Edit Firewall Policy**，并在策略映射中选择相应的规则。单击 **Edit**。

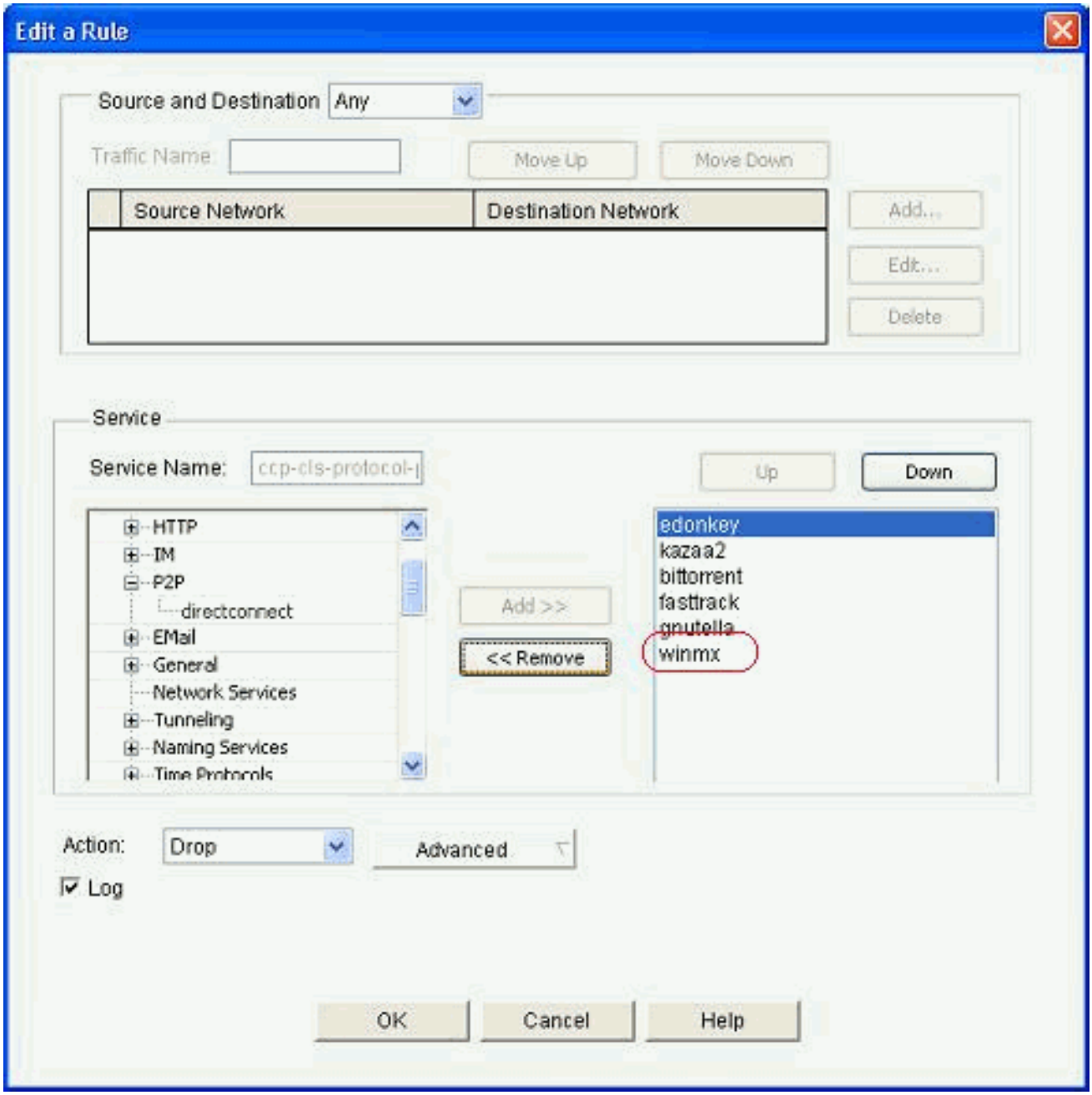


这显示默认配置将阻止的当前P2P应用。

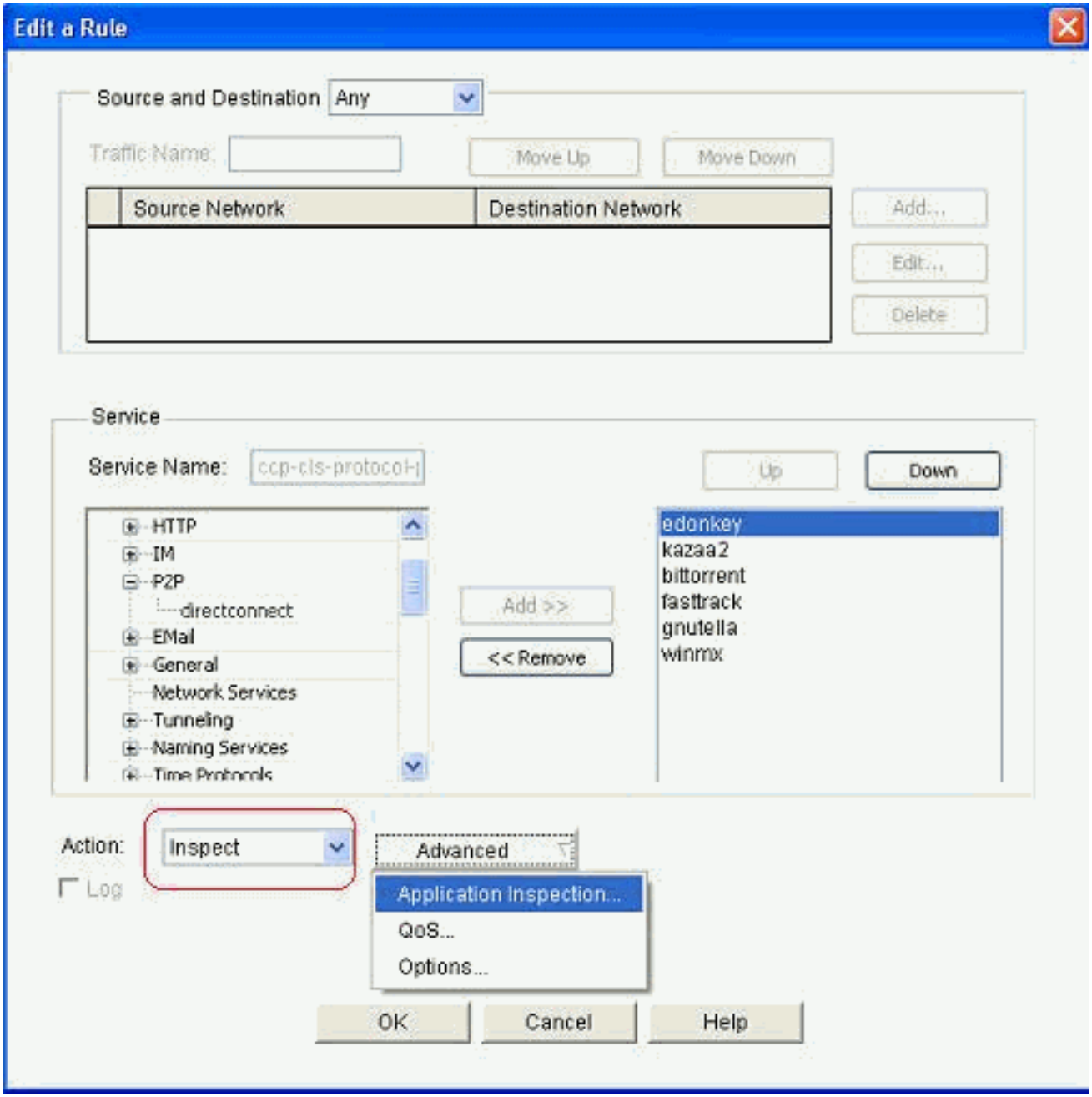


13. 您可以使用Add和Remove按钮添加/删除特定应用。此屏幕截图显示如何添加winmx应用以阻止该应用。


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

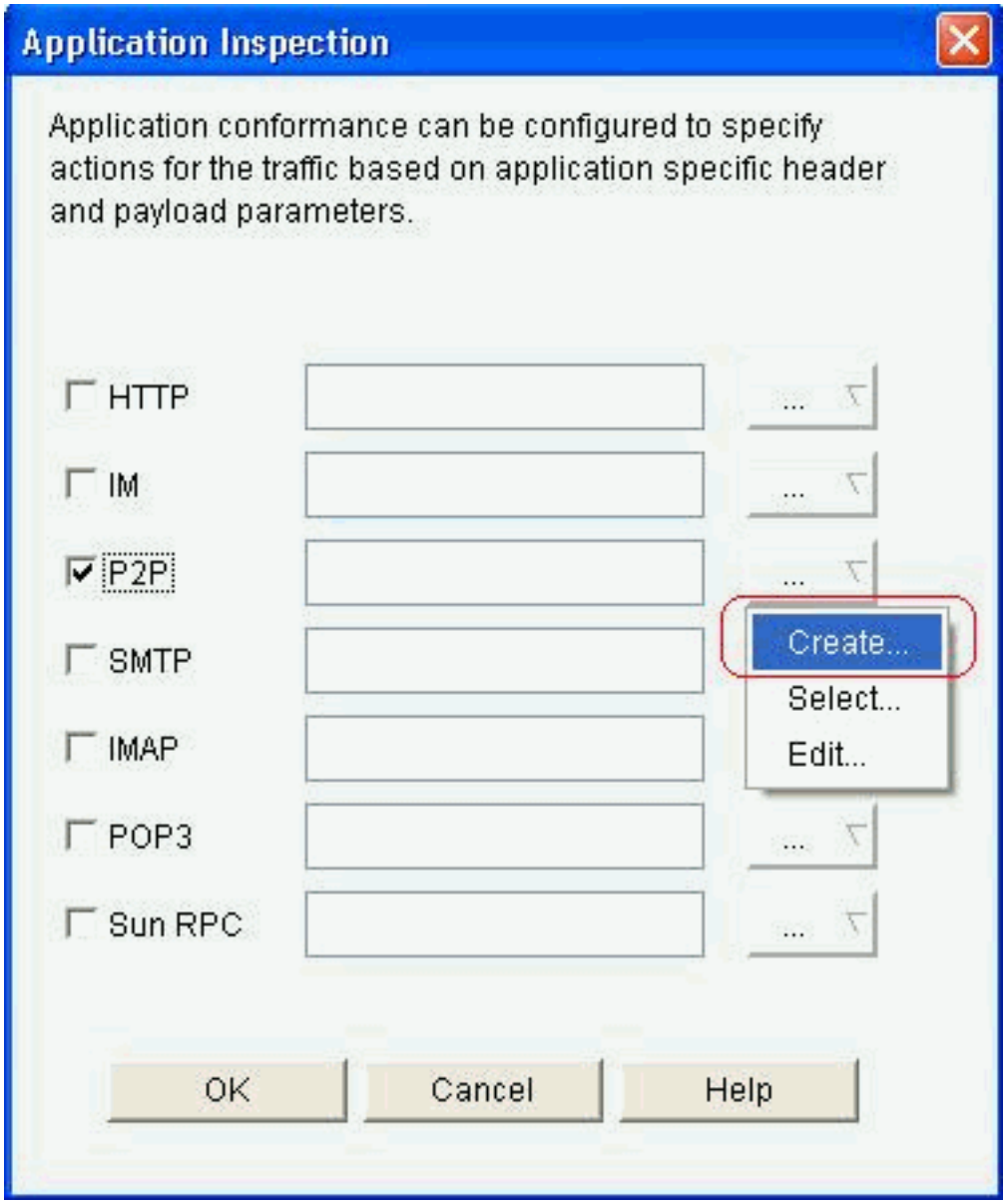


14. 除了选择丢弃操作，您还可以选择Inspect操作以应用不同的选项进行深度数据包检测。

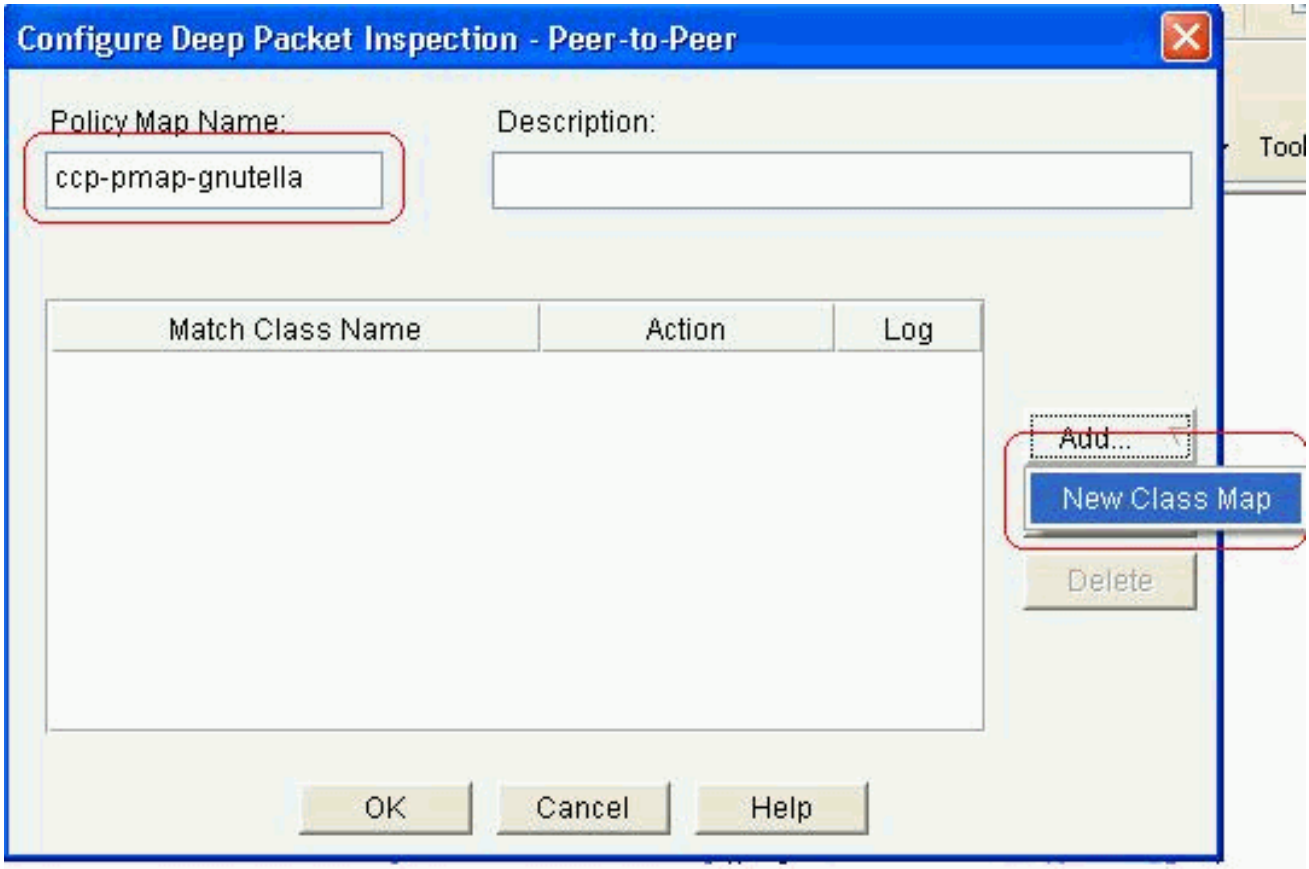


P2P检测为应用流量提供第4层和第7层策略。这意味着ZFW可以提供基本状态检测以允许或拒绝流量，以及对各种协议中特定活动的精细第7层控制，从而允许某些应用活动，而拒绝其他应用活动。在此应用检测中，您可以对P2P应用应用不同类型的特定报头级别检测。下面显示了gnutella的示例。

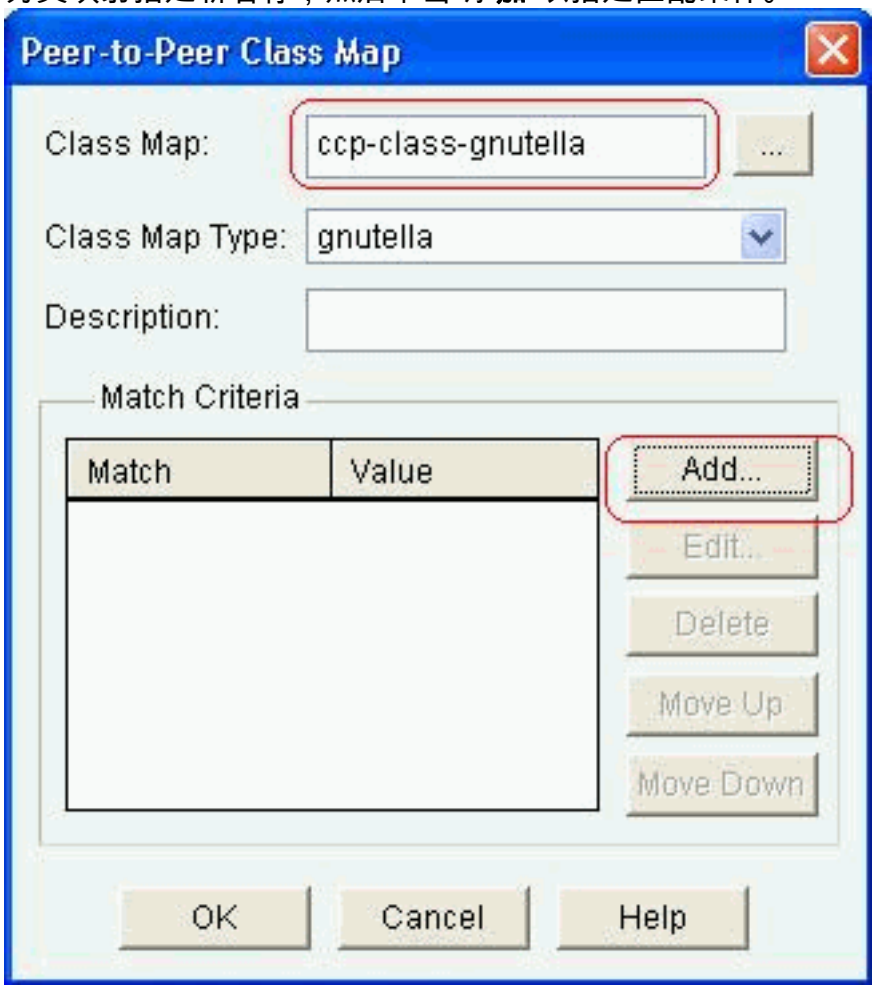
15. 选中**P2P选**项并单击**Create** 以为此创建新的策略映射。



16. 为gnutella协议创建用于深度数据包检测的新策略映射。单击**Add,然后选择New Class Map。**



17. 为类映射指定新名称，然后单击“添加”以指定匹配条件。

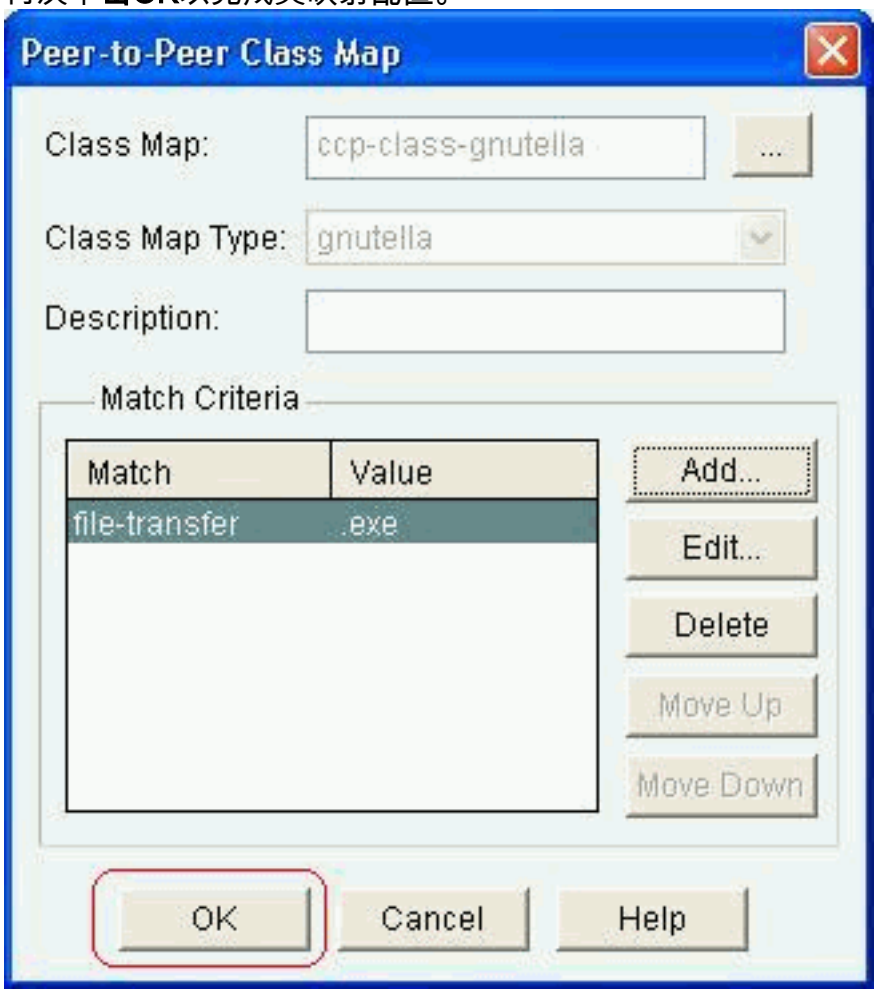


18. 使用file-transfer作为匹配条件，使用的字符串为.exe。这表示包含.exe字符串的所有gnutella文件传输连接与流量策略匹配。Click

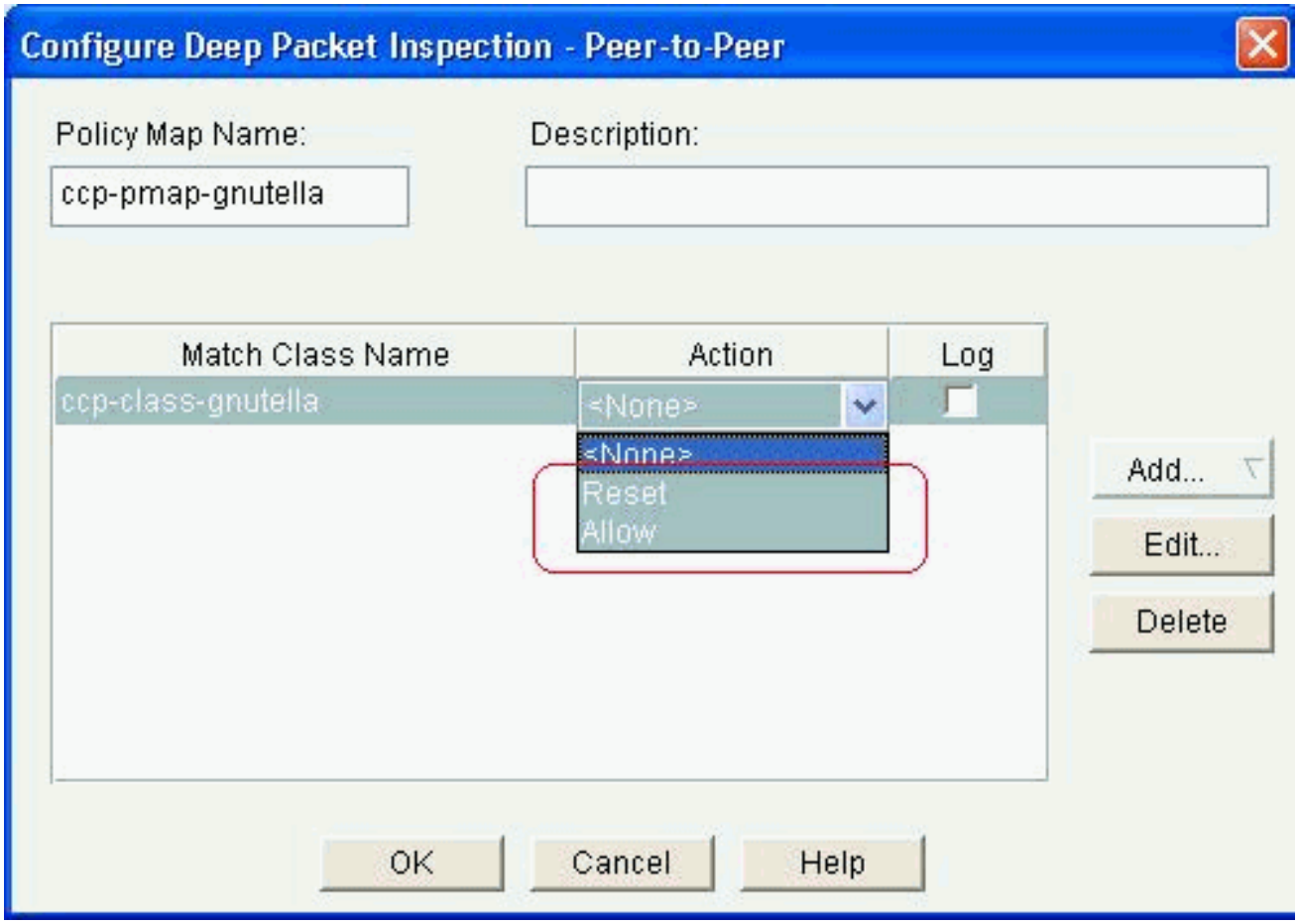


OK.

19. 再次单击**OK**以完成类映射配置。

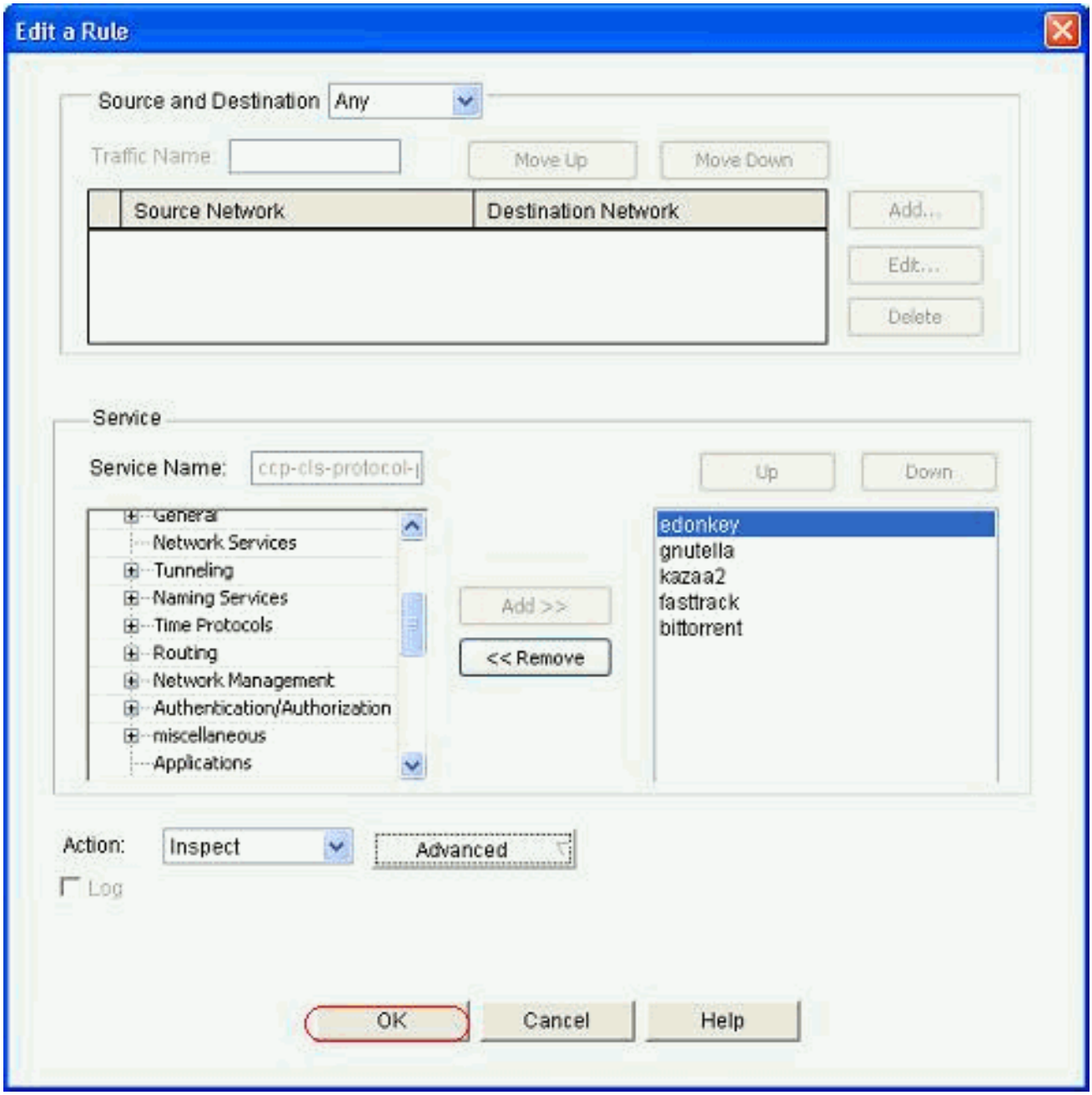


20. 选择**重置**或**允许**选项，这取决于您公司的安全策略。单击**OK**确认使用策略映射的操作。



同样，您可以通过指定不同的正则表达式作为匹配条件来添加其他策略映射，以实施其他P2P协议的深度检测功能。**注意：**P2P应用尤其难以检测，原因是“跳端口”行为和其他避免检测的伎俩，以及P2P应用频繁更改和更新导致的问题，这些应用修改了协议的行为。ZFW将本地防火墙状态检测与基于网络的应用识别(NBAR)的流量识别功能相结合，提供P2P应用控制。**注意：**P2P应用检测为第4层检测支持的应用子集提供应用特定功能：edonkeyfasttrackgnutellakazaa2**注意：**目前，ZFW没有检查“bittorrent”应用流量的选项。BitTorrent客户端通常通过在某些非标准端口上运行的HTTP与跟踪器（对等目录服务器）通信。此端口一般是 TCP 6969，但您可能需要检查 torrent 专用的 tracker 端口。如果您希望允许BitTorrent，则支持其他端口的最佳方法是将HTTP配置为匹配协议之一，并使用以下ip port-map命令将TCP 6969添加到HTTP:**ip port-map http port tcp 6969**。您需要将 http 和 bittorrent 定义为在类映射中应用的匹配条件。

21. 单击**OK**完成“Advanced Inspection（高级检查）”配置。

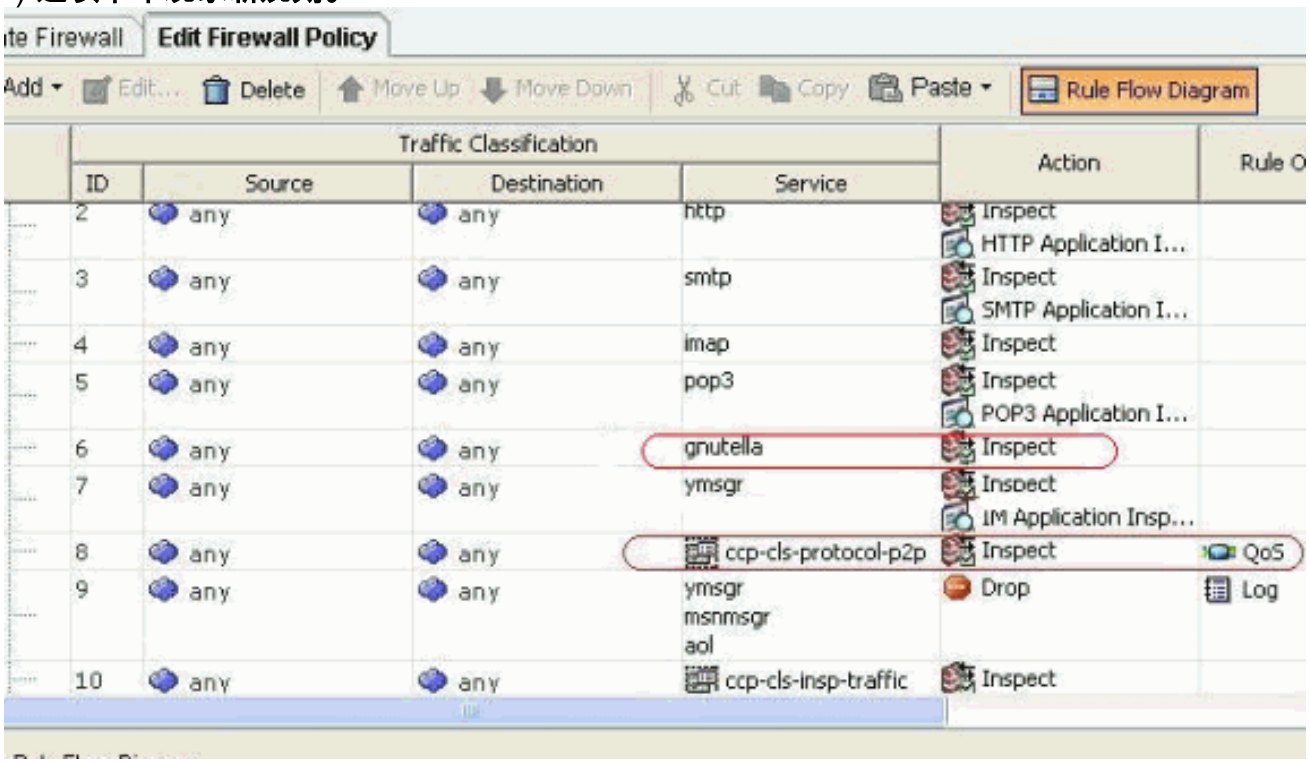


相应的一组命令将传送到路由器。

22. 单击**OK**完成命令集的复制。



23. 可以从Configure > Security > Firewall and ACL下的Edit Firewall Policy（编辑防火墙策略）选项卡中观察新规则。



ZFW路由器的命令行配置

思科CP上一节中的配置在ZFW路由器上导致以下配置：

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#
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

- ZBF-Router# **show policy-map type inspect zone-pair sessions** — 显示所有现有区域对的运行时检查类型策略映射统计信息。

相关信息

- 区域策略防火墙设计和应用指南
- Cisco IOS 防火墙传统和基于区域的虚拟防火墙应用程序配置示例
- 思科配置专业主页