Cisco Configuration Professional ：基于区域的防火墙阻塞的对等流量配置示例

目录

简介

本文提供一逐步方法配置Cisco IOS路由器作为一基于区域的防火墙阻塞对等(P2P)流量通过使用Cisco Configuration Professional的(思科CP)先进的防火墙配置向导。

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。区域之间策略提供严重的灵活性和粒度。所以，不同的检查策略可以应用到多台主机组连接对同一路由器接口。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应用程序是某些在互联网的最用途广泛的应用程序。P2P网络能作为有恶意的威胁的一conduit例如蠕虫病毒，提供一个容易路径在防火墙附近和导致关于保密性和安全的注意事项。Cisco IOS软件版本12.4(9)T介绍P2P应用程序的ZFW支持。P2P检查提供应用流量的Layer4和第七层策略。这意味着ZFW能提供基本状态检测允许或否决流量，以及在特殊活动的粒状第七层控制在多种协议，因此某些应用程序活动允许，当其他拒绝时。

思科CP提供一易执行的，逐步方法配置IOS路由器作为一基于区域的防火墙通过使用先进的防火墙配置向导。

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路由器必须有软件版本作为12.4(9)T或以后。
- 对于支持思科CP的IOS路由器型号，参考思科CP版本注释。

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Cisco 1841 IOS路由器
- Cisco Configuration Professional (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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

对于本文的示例，路由器配置作为一基于区域的防火墙阻塞P2P流量。ZFW路由器有两个接口、一个inside(trusted)接口在区域和一个外部(非受信)接口在外区域。ZFW路由器阻塞P2P申请例如edonkey、fasttrack、gnutella和kazaa2与记录日志操作对从区域通过到外区域的流量。

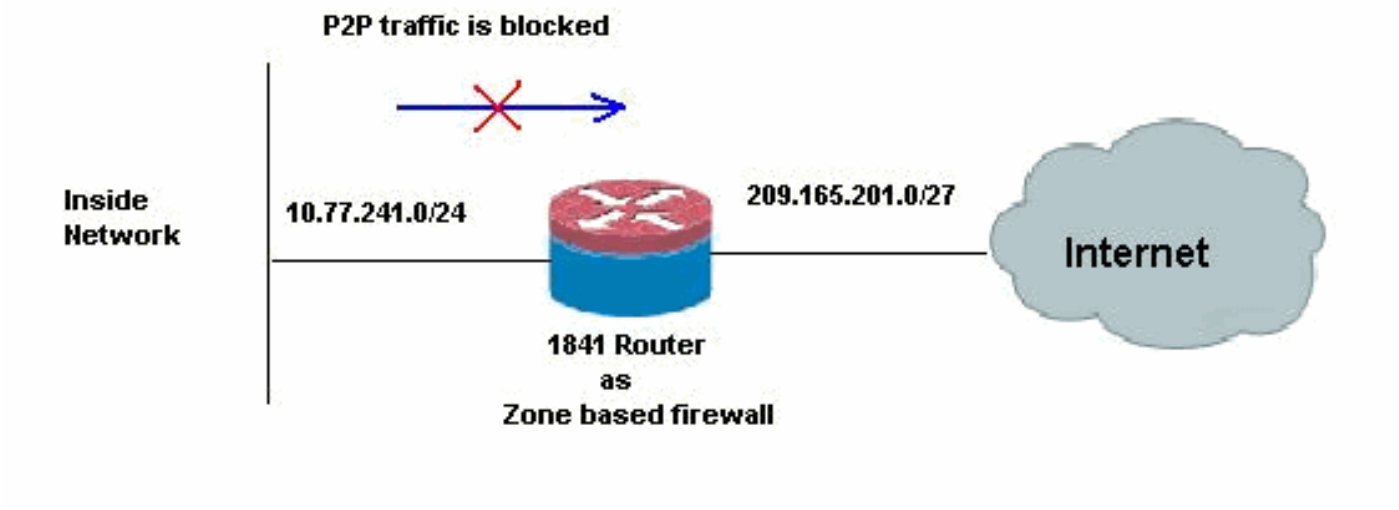
配置

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（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

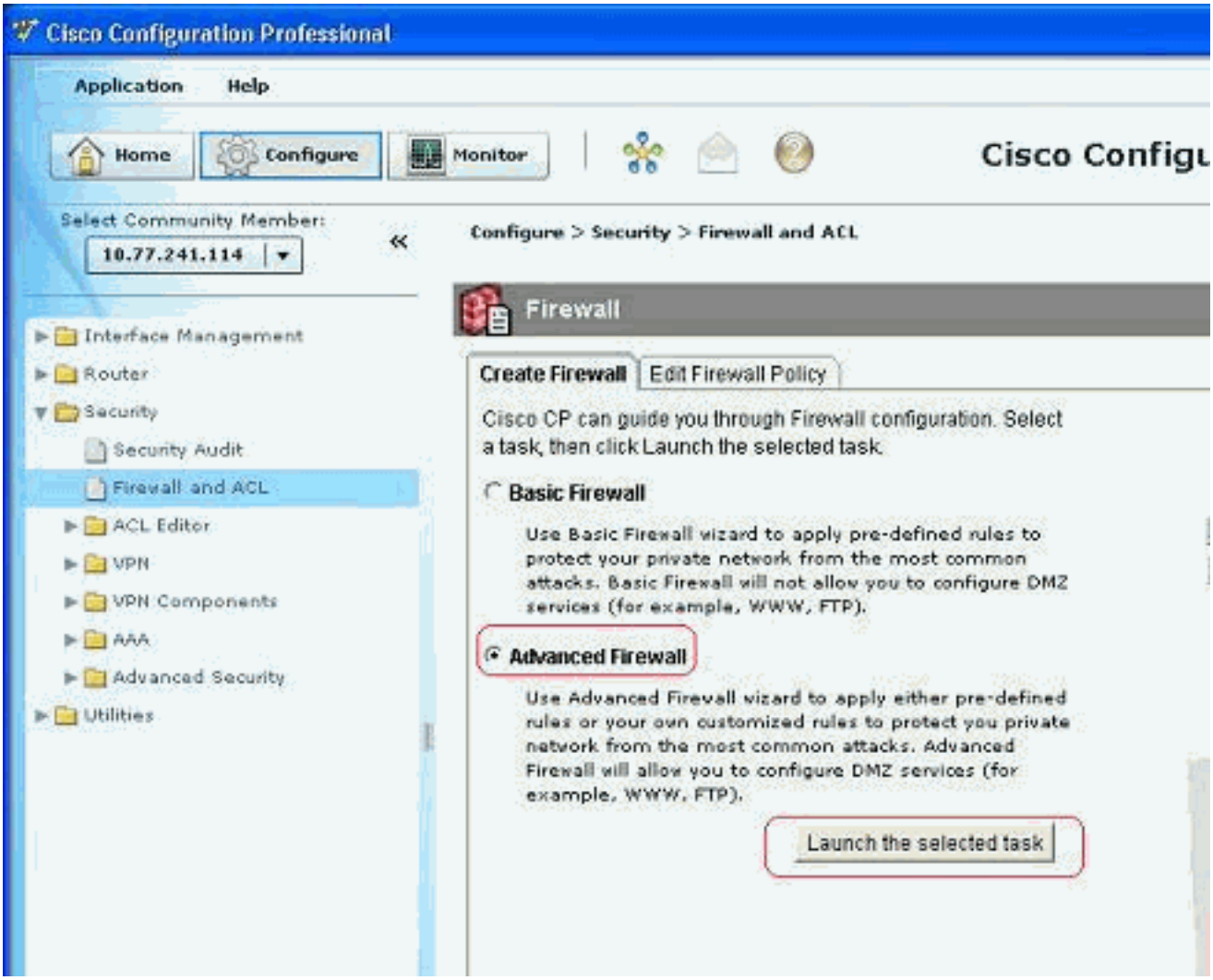


配置通过Cisco Configuration Professional

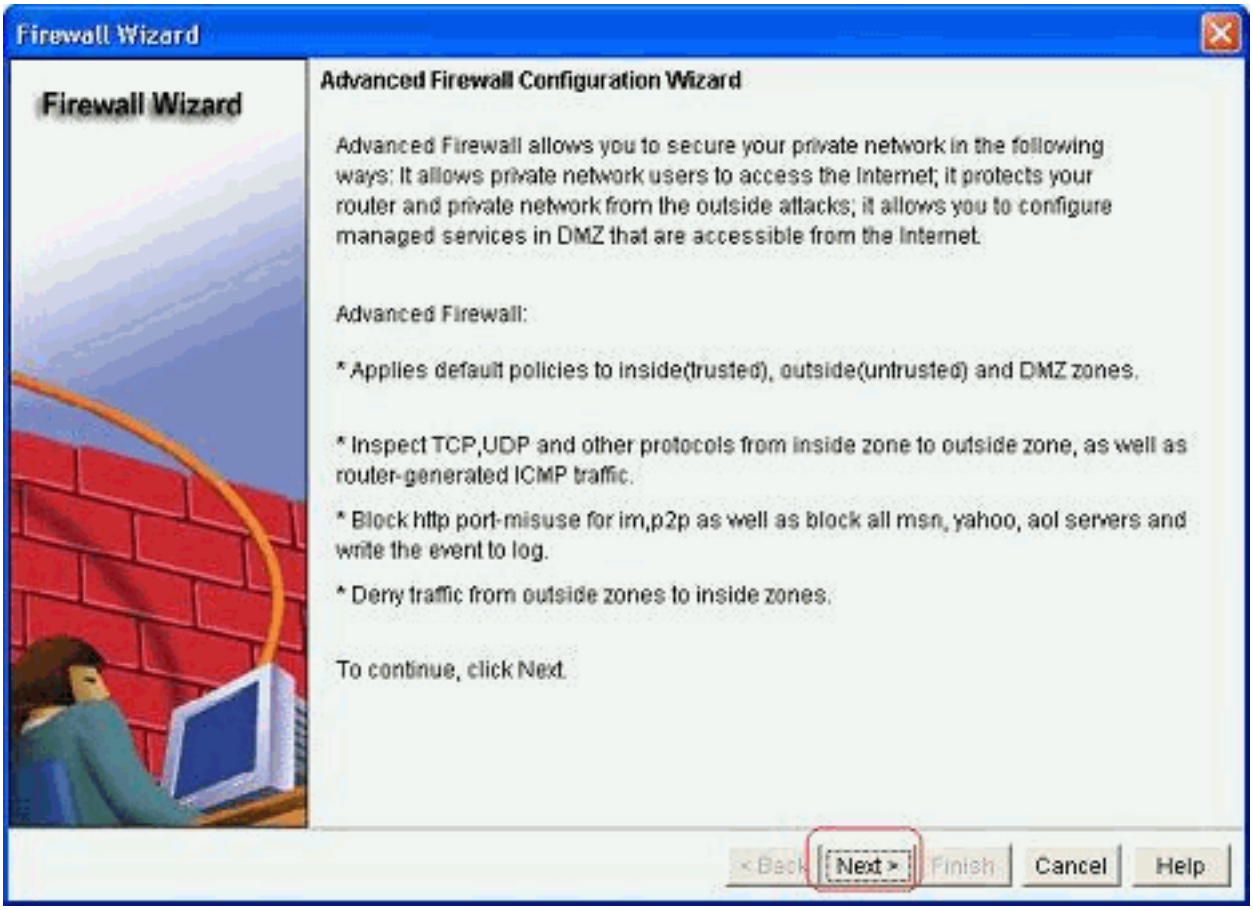
此部分包含关于怎样的逐步程序使用向导配置IOS路由器作为一基于区域的防火墙。

完成这些步骤：

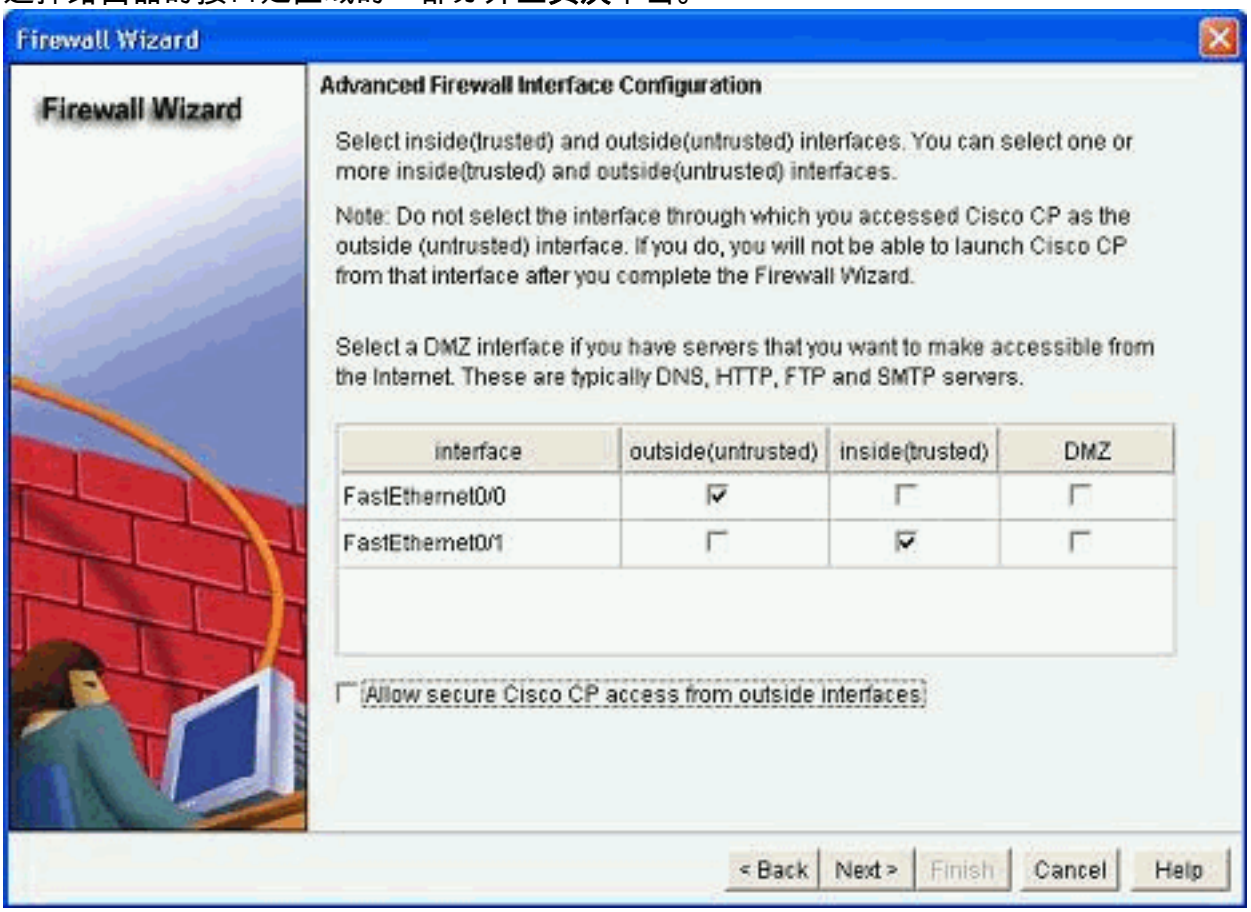
1. 去**配置> Security >防火墙和ACL**。然后，请选择**先进的防火墙**单选按钮。单击 Launch the selected task。



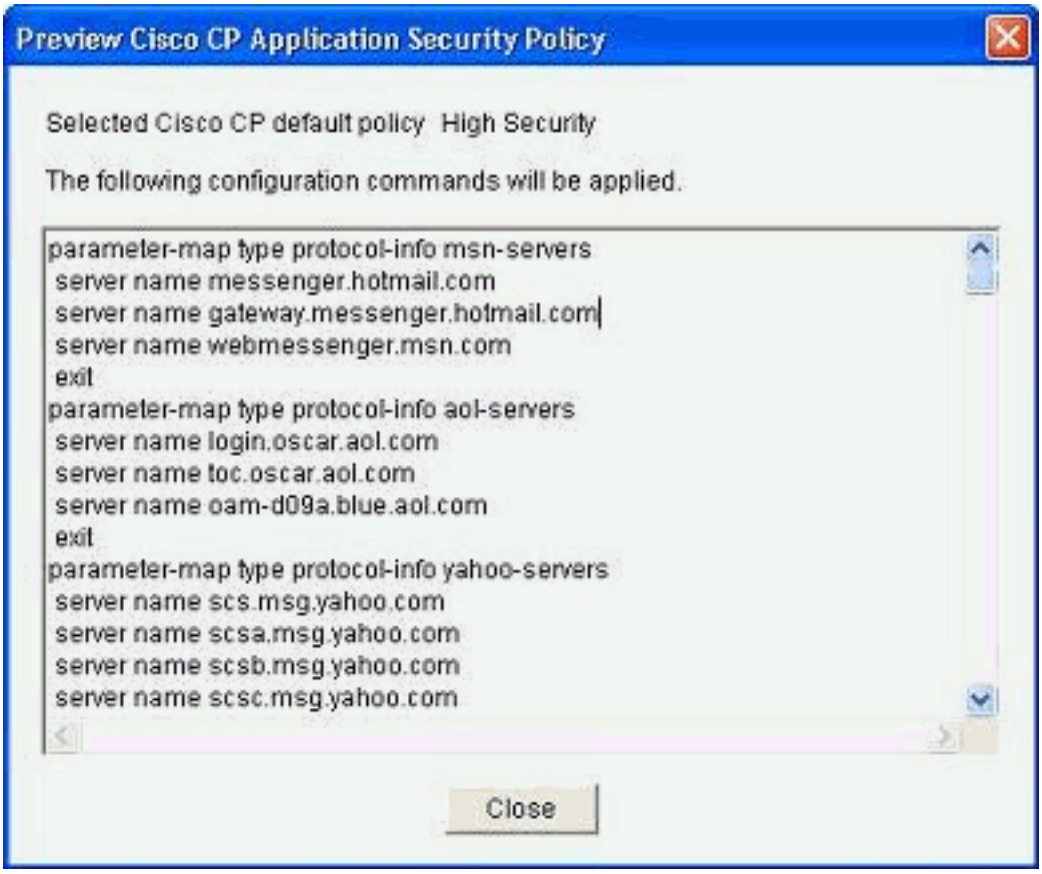
2. 此Next屏幕显示关于防火墙向导的一简要介绍。单击**在旁边**开始配置防火墙。



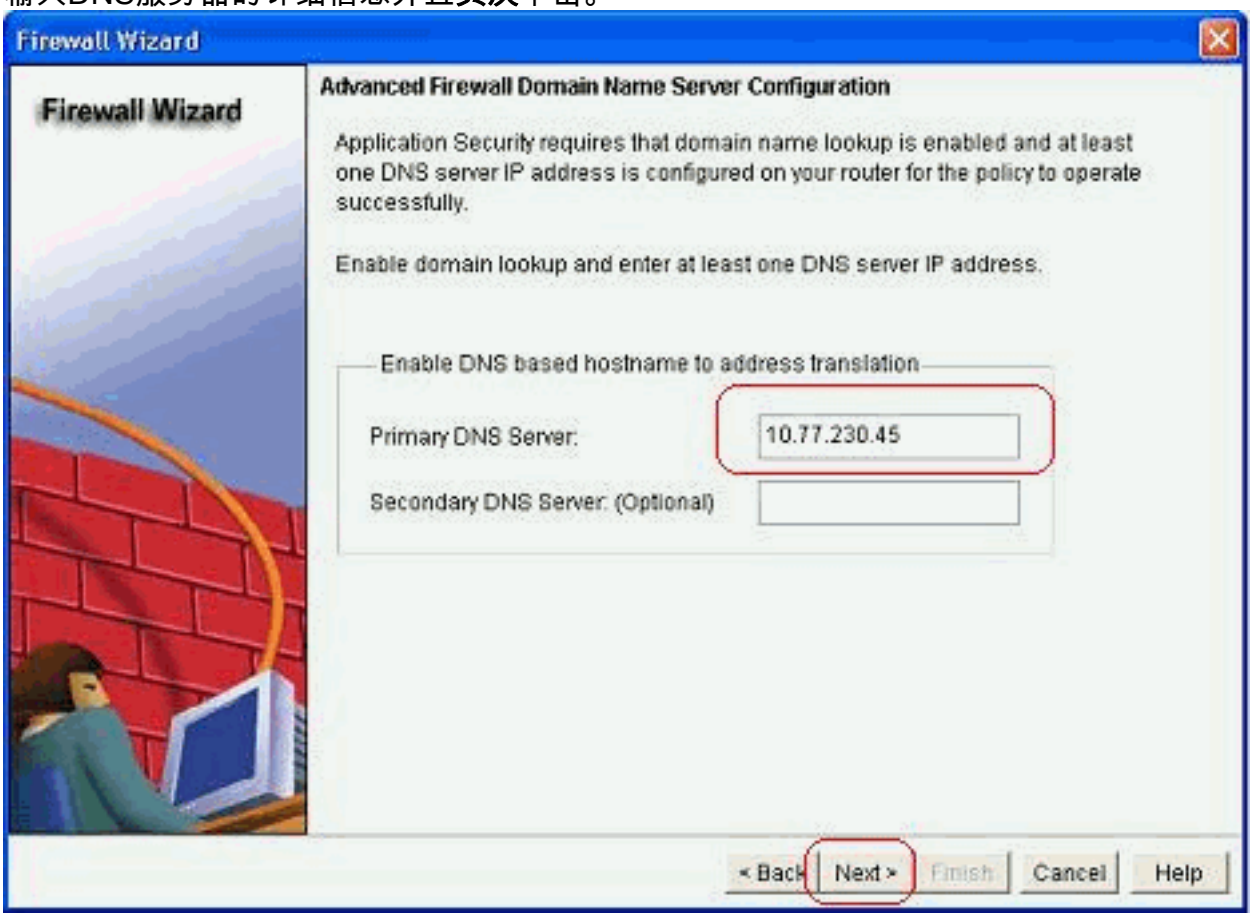
3. 选择路由器的接口是区域的一部分并且**其次**单击。



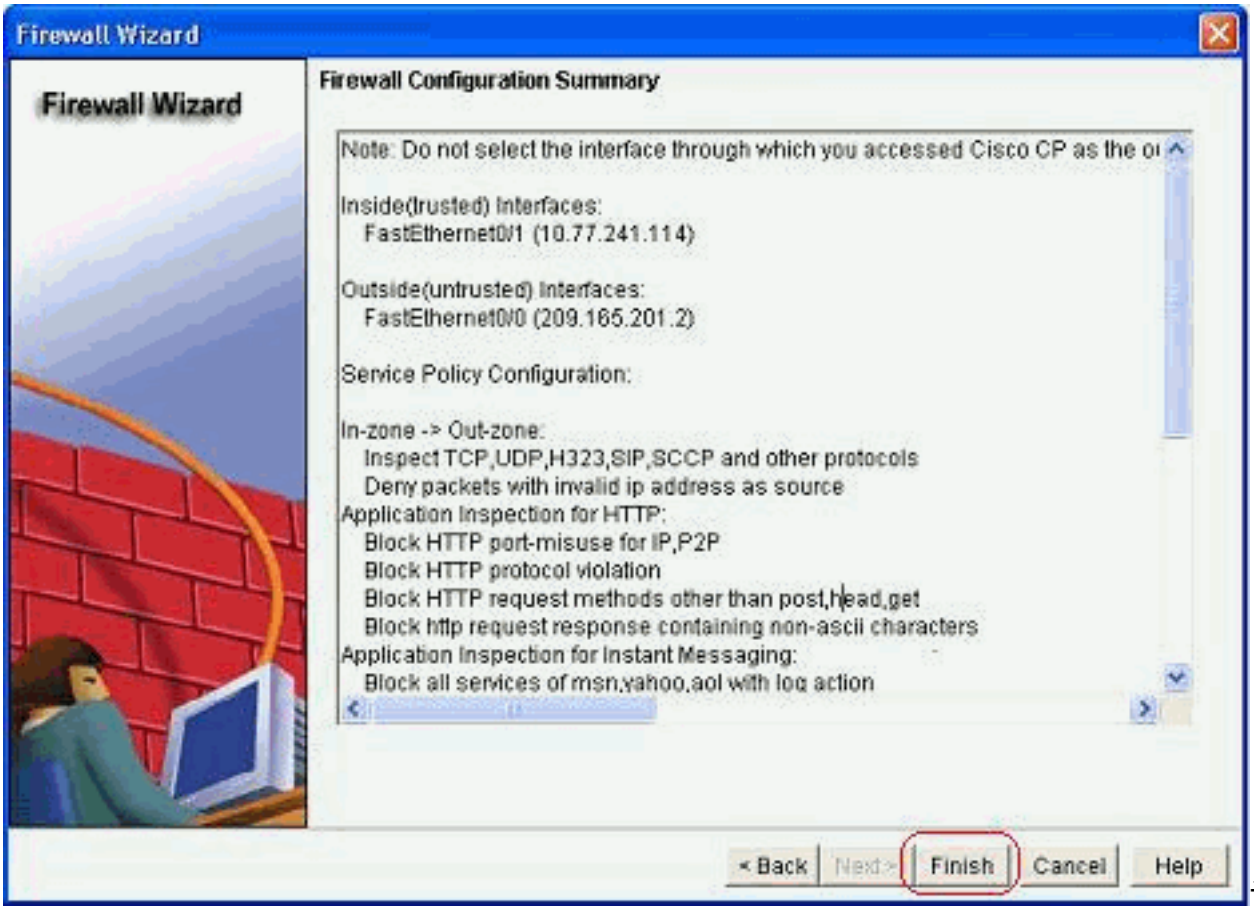
4. 默认策略以与一组命令一起的高安全性在下一个窗口显示。单击**接近**继续。



5. 输入DNS服务器的详细信息并且**其次**单击。

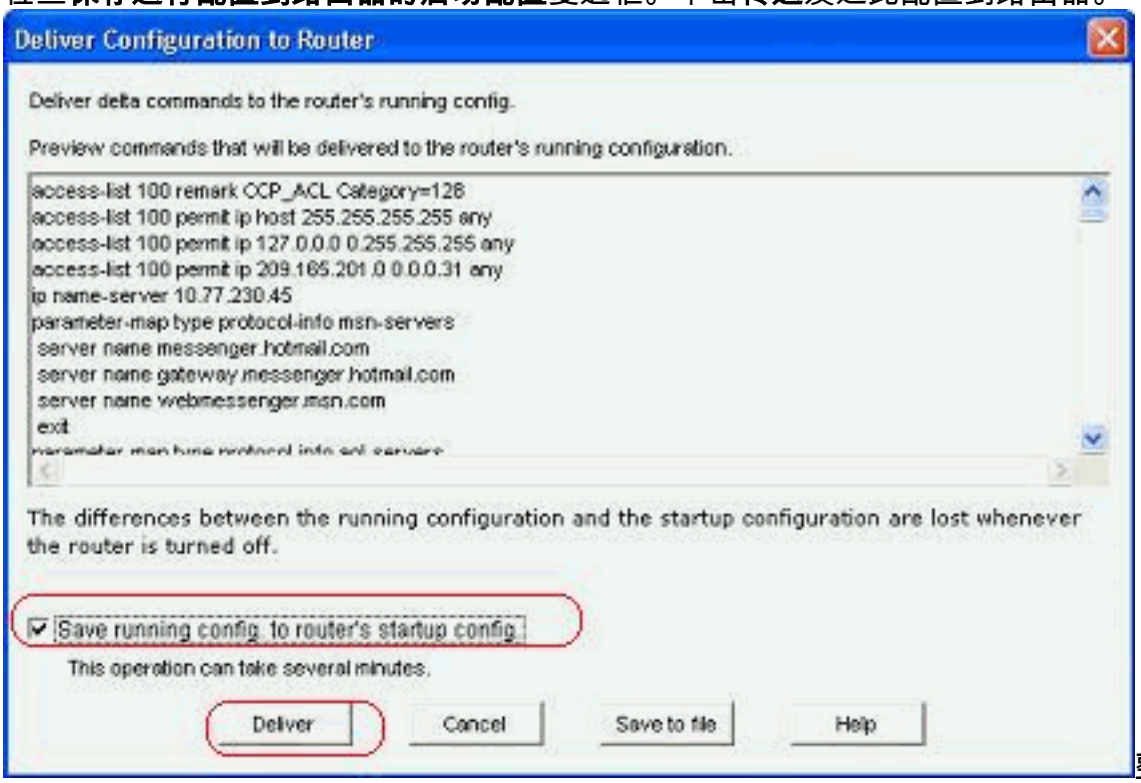


6. 思科CP提供一个配置汇总例如显示的那个此处。点击**芬通社**完成配置。

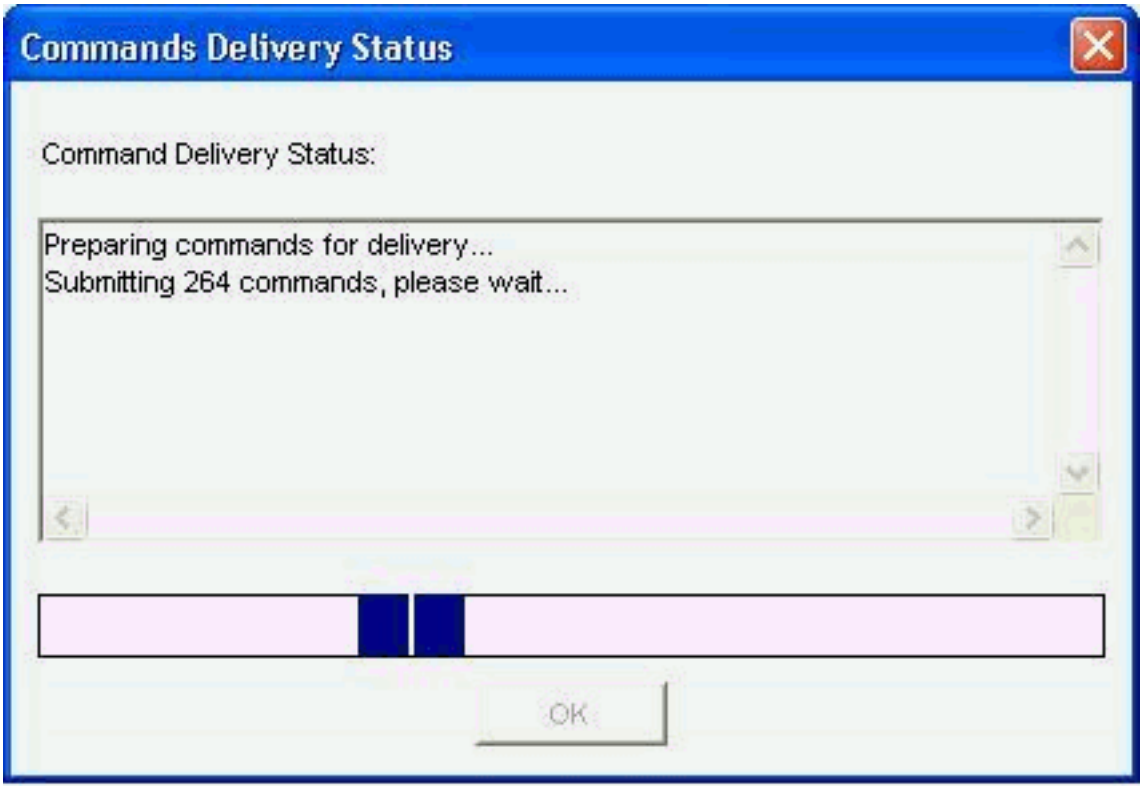


详细配置摘要在此表里提供。这是默认配置根据思科CP的高安全性策略。

7. 检查**保存运行配置到路由器的启动配置**复选框。单击**传送**发送此配置到路由器。



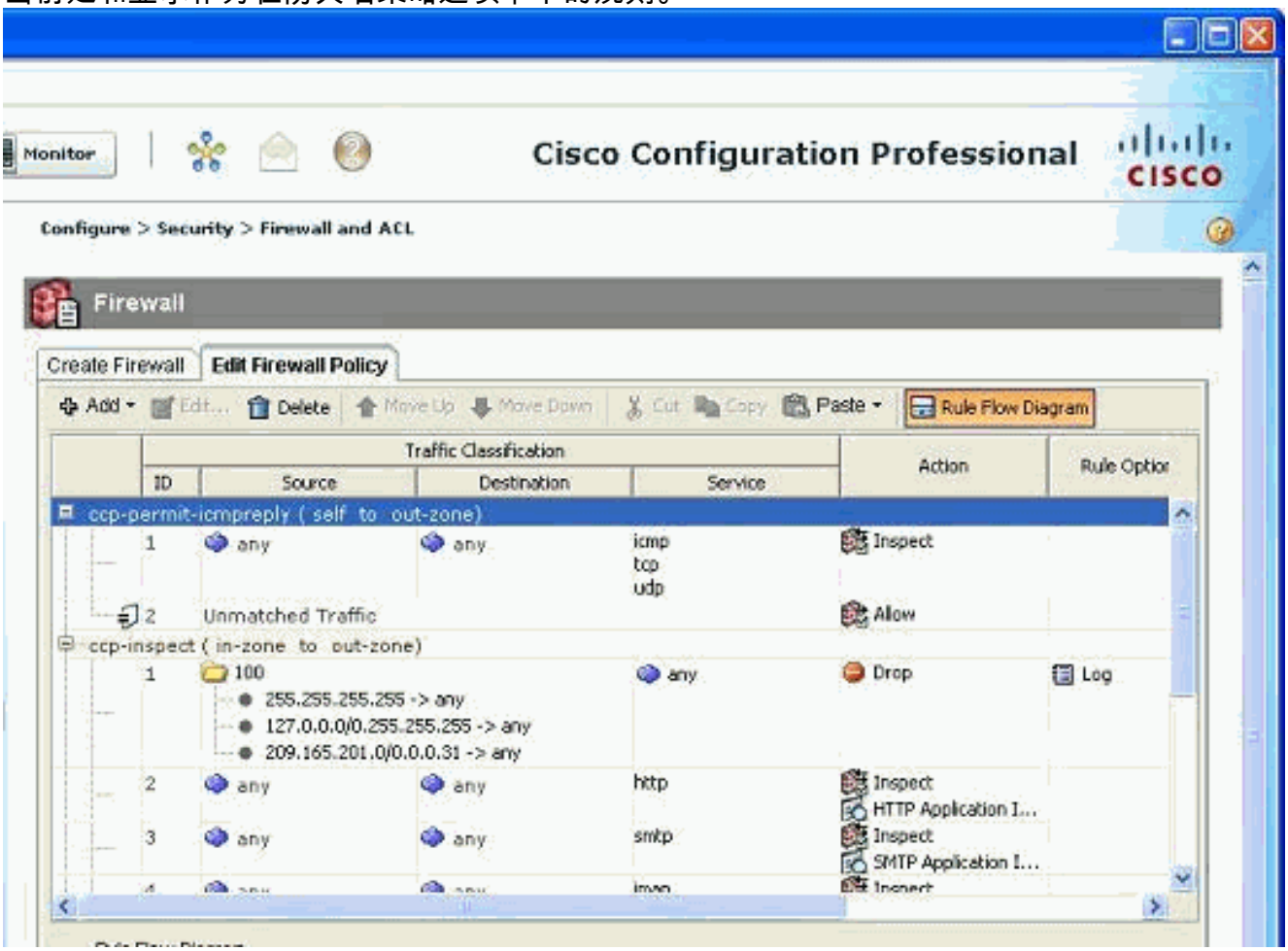
整个配置传送到路由器。这采取一些时间处理。



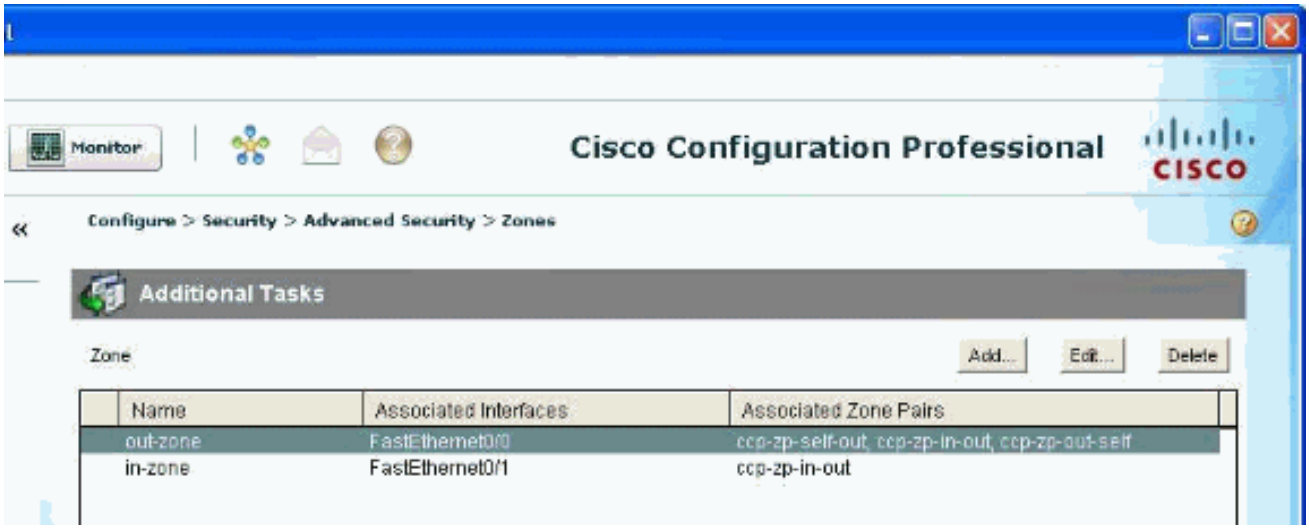
8. 点击OK键继续。

9. 再点击OK键。

配置实际上当前是和显示作为在防火墙策略选项卡下的规则。

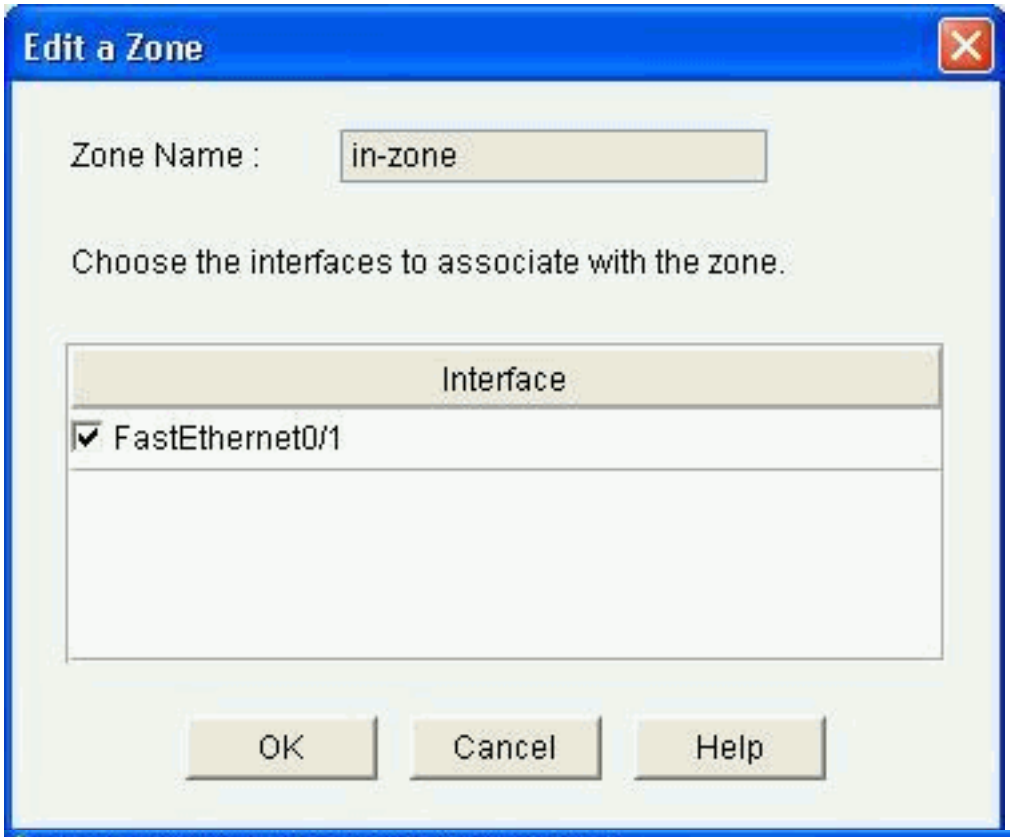


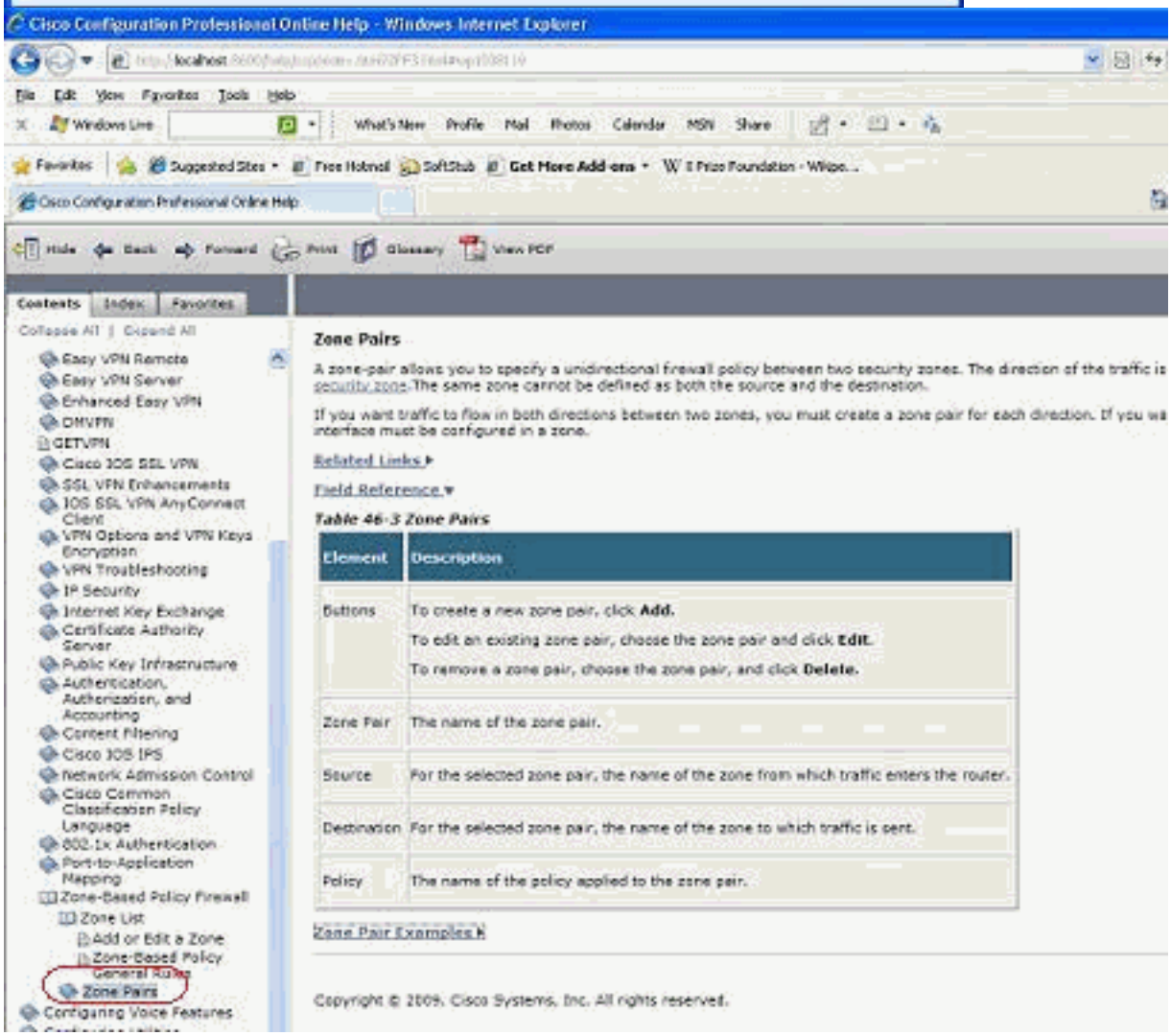
10. 他们关联与区域对一起的区域可以查看，如果去**配置> Security >Advanced安全>区域**。您能通过单击也添加新建的区域通过单击**添加**或者修改现有区域**编辑**。



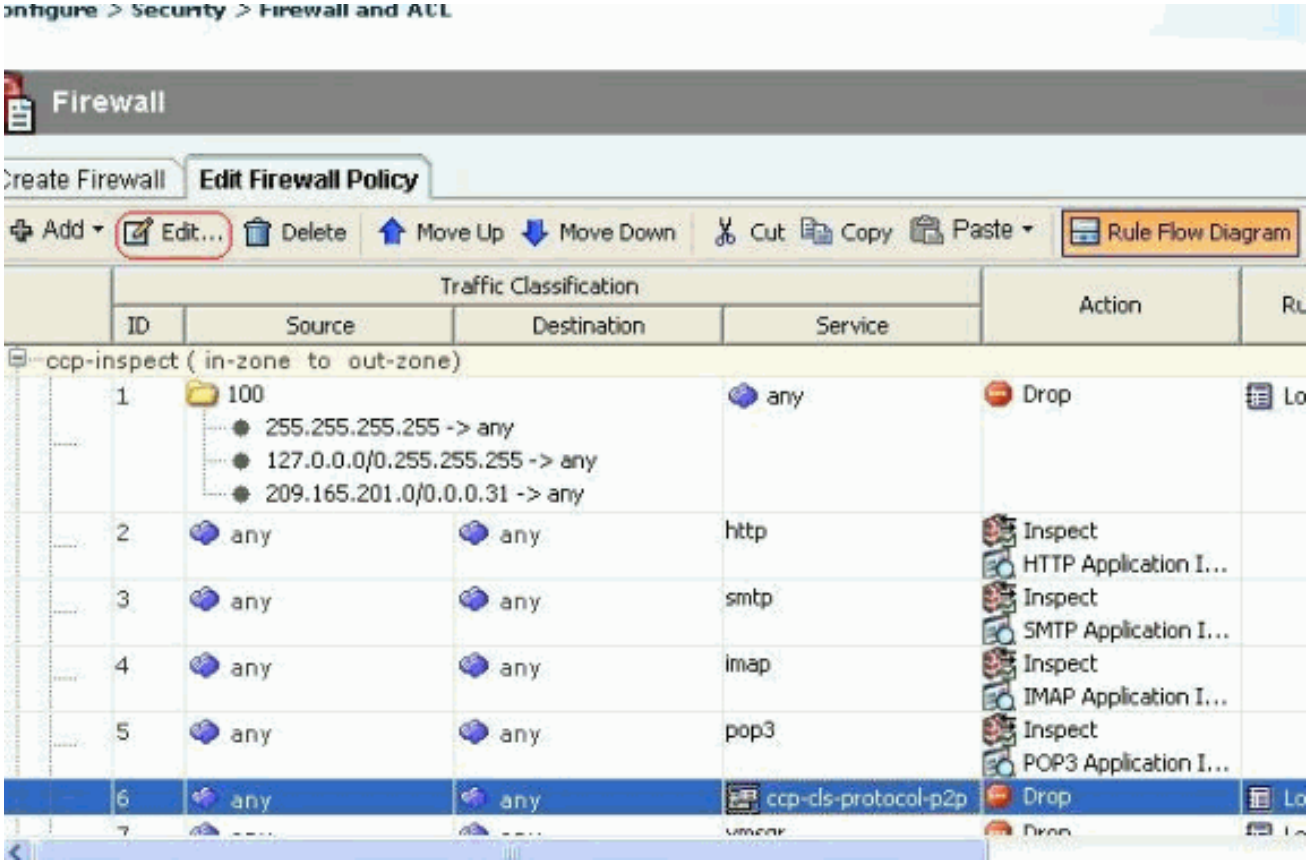
11. 去**配置> Security >Advanced**查看区域对的详细信息的**安全>区域对**。

关于怎样的即时帮助修改/添加/删除区域/区域对，并且其他相关信息是可用的与在思科CP的内置的网页。

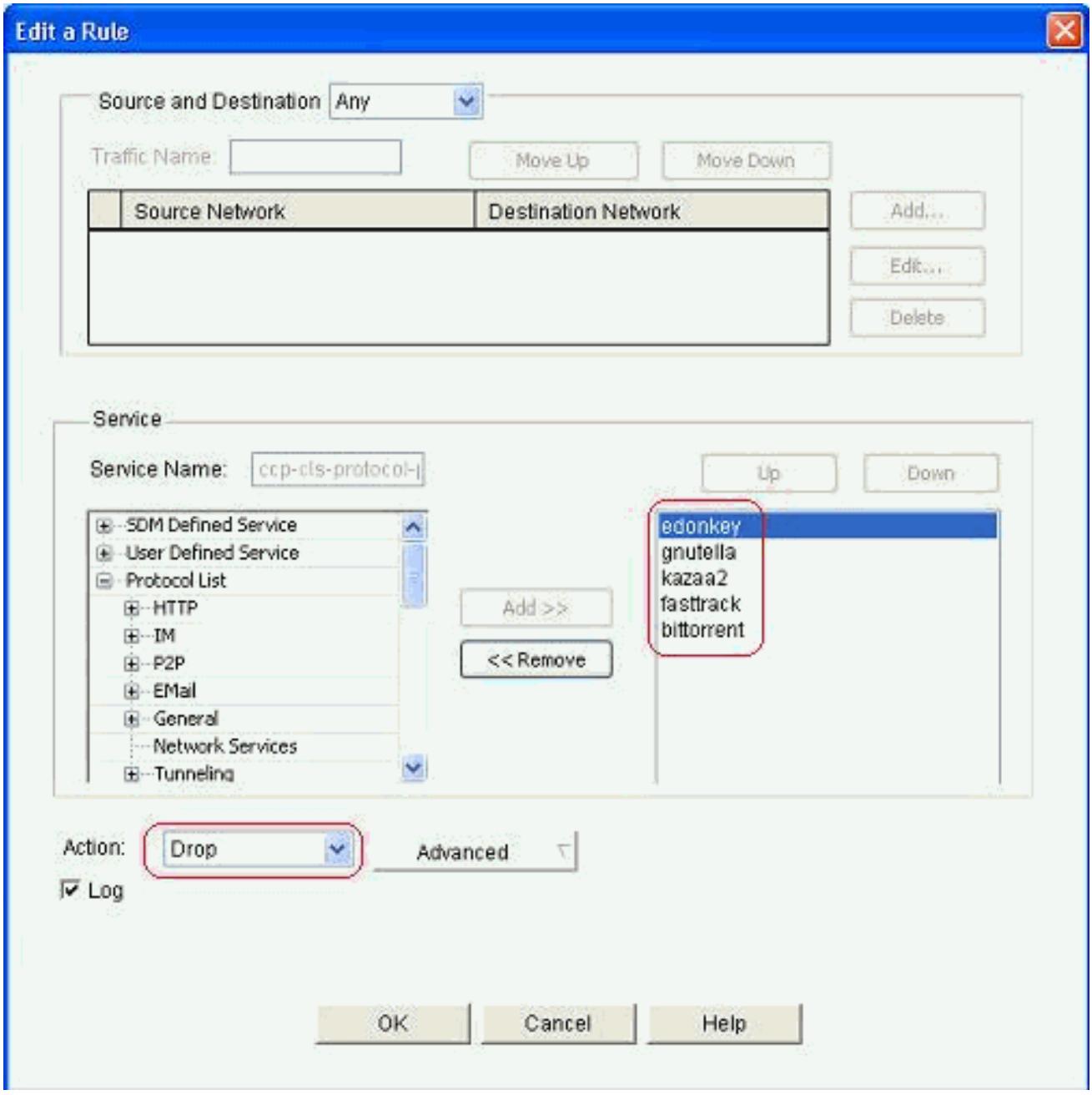




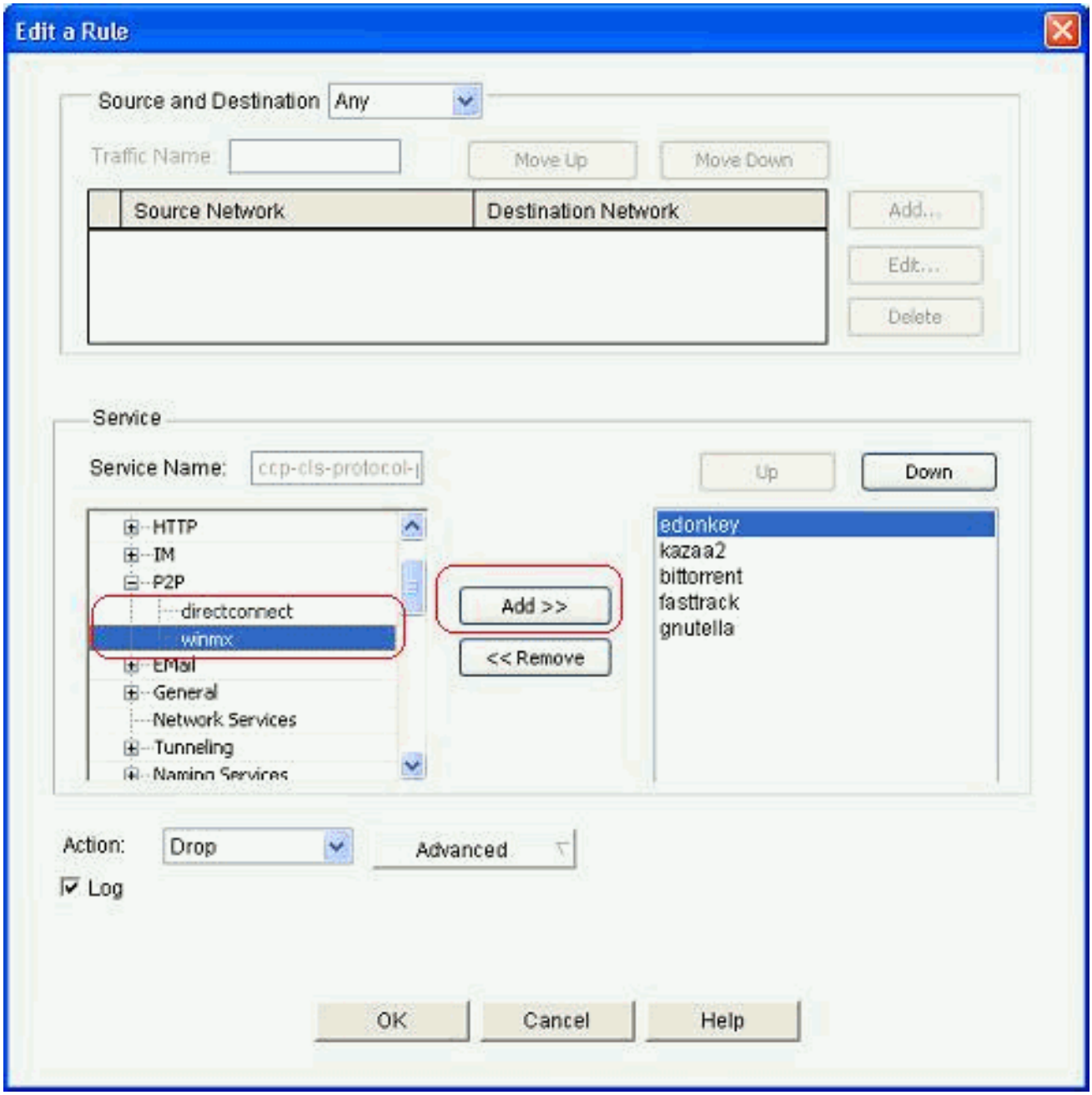
12. 为了修改某些P2P应用程序的有特殊用途的检查功能，请去**Configuration>安全>防火墙和ACL**。然后，请单击**编辑防火墙策略**并且选择在策略映射的各自规则。单击 **Edit**。

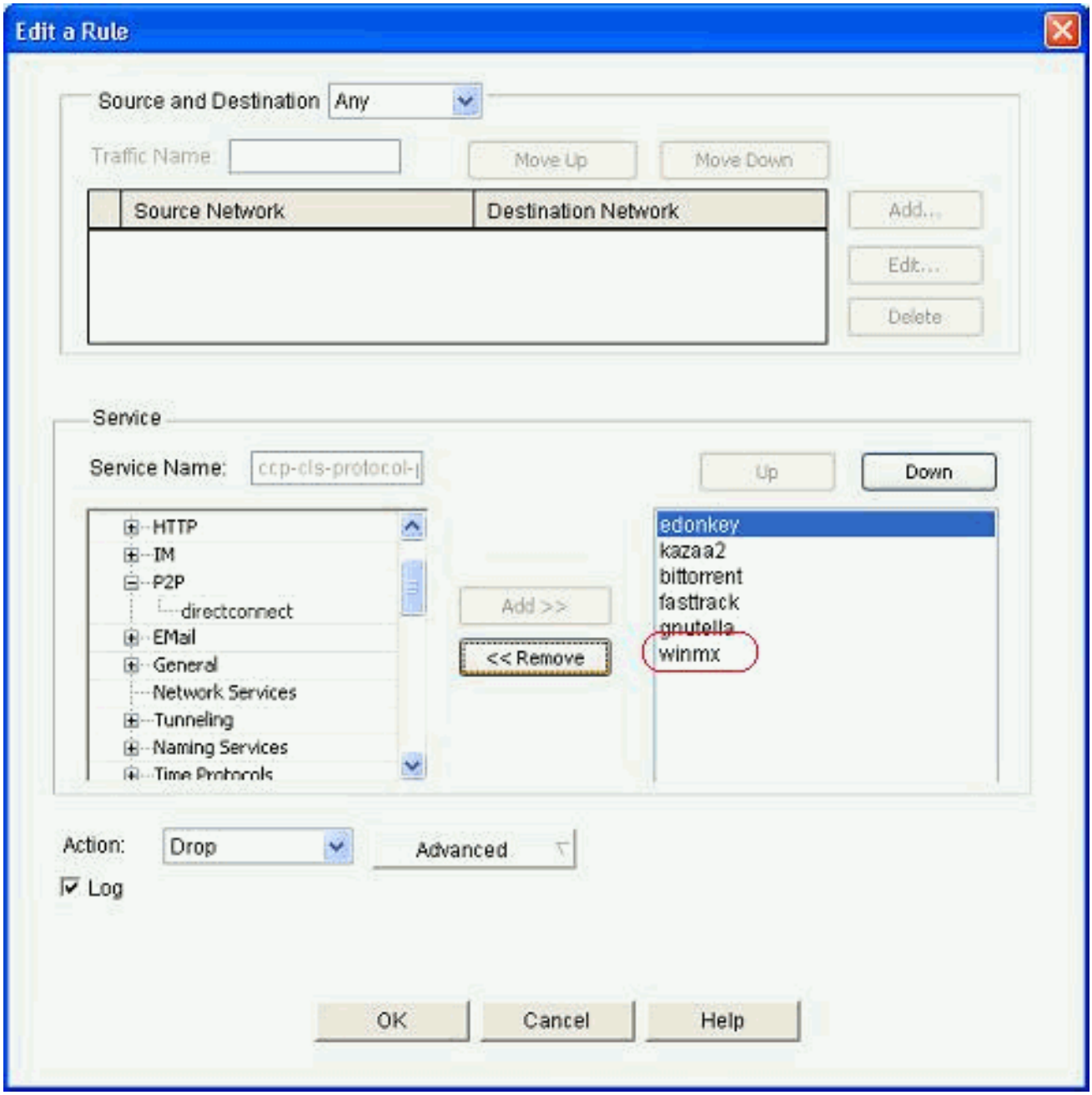


这显示默认情况下阻塞的配置的当前P2P应用程序。

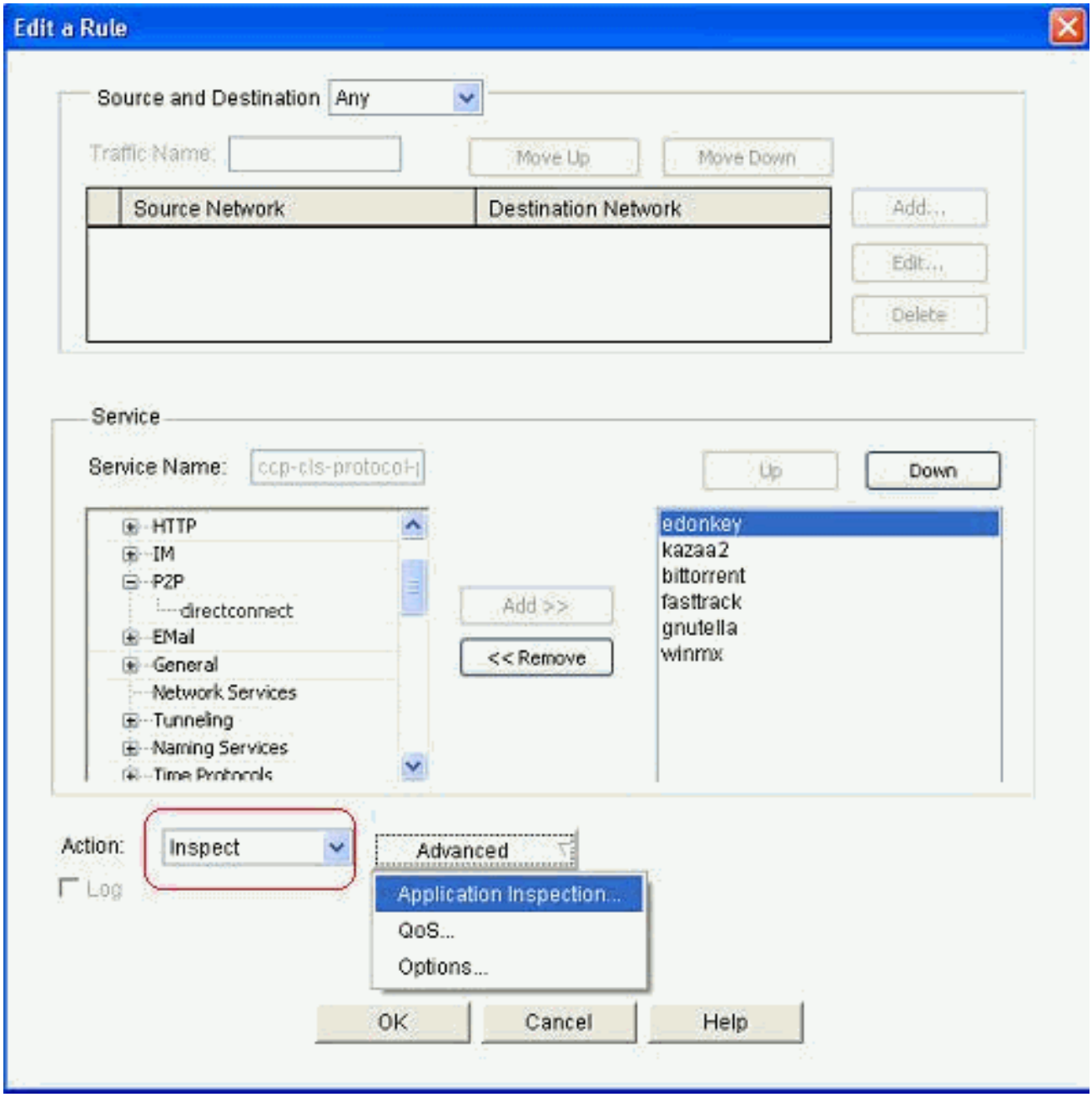


13. 您能使用添加和删除按钮添加/删除特定应用程序。此屏幕画面如何显示添加winmx应用程序阻塞那。


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

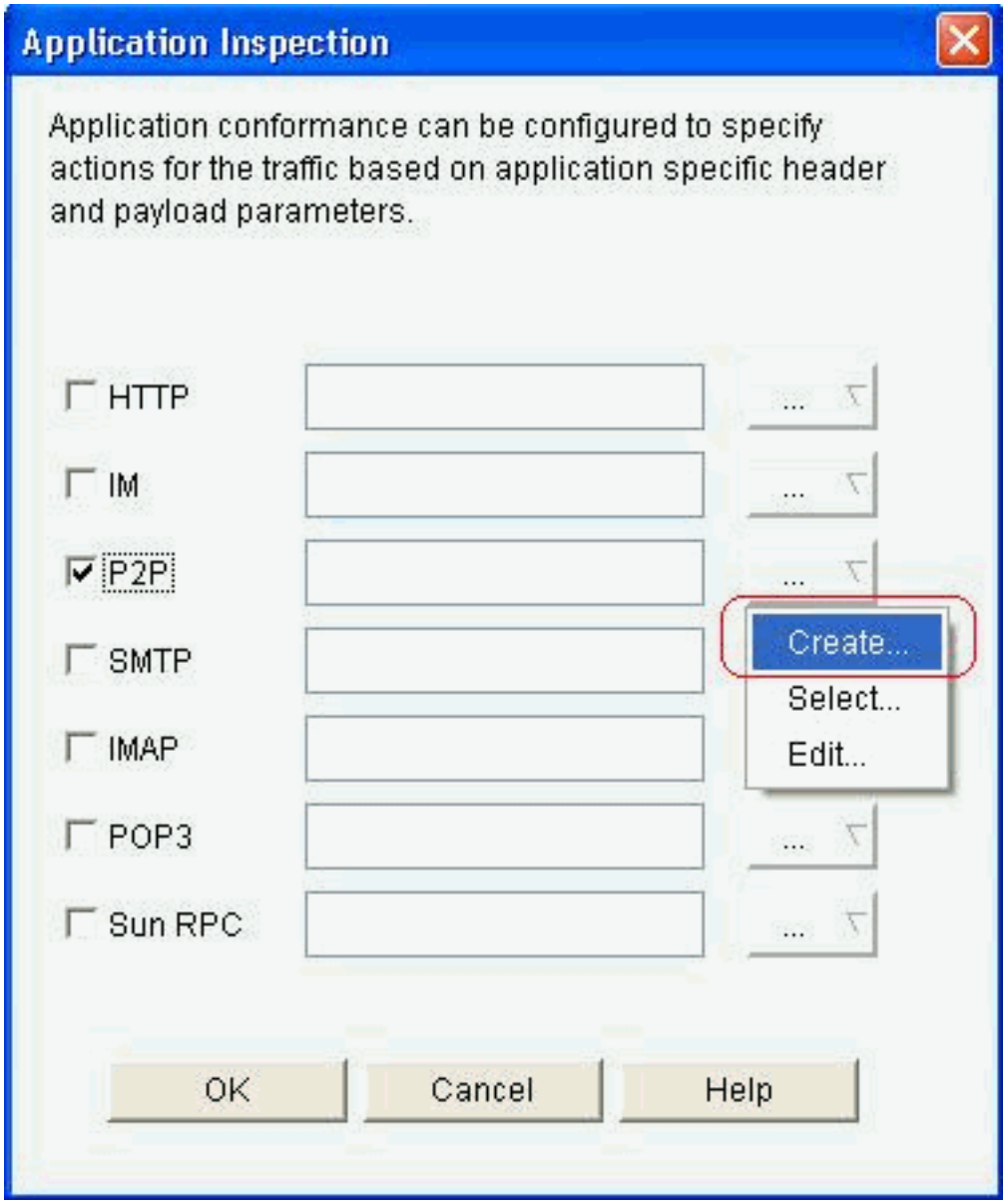


14. 而不是选择丢弃操作，您能也选择检查操作申请不同的选项深度信息包检验。

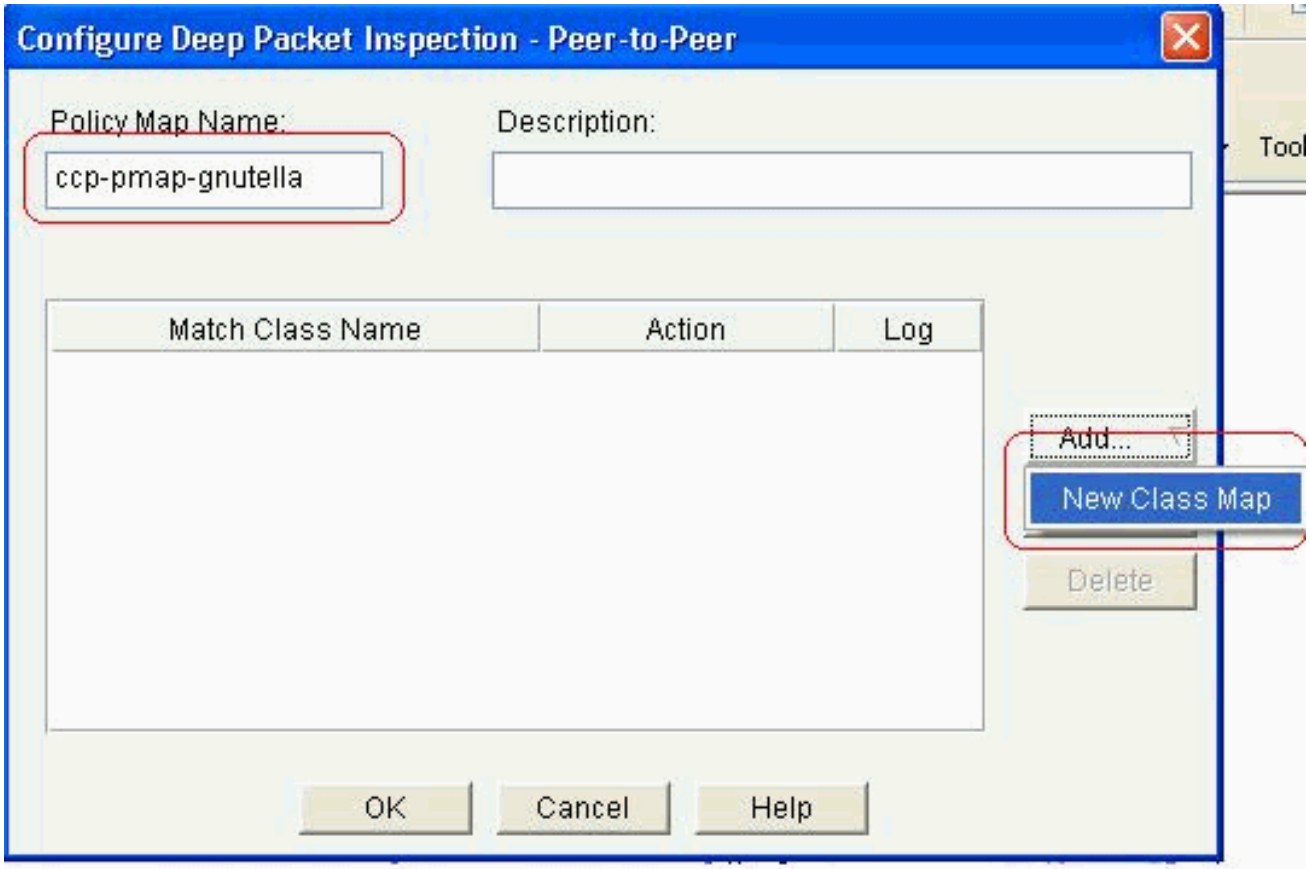


P2P检查提供应用流量的Layer4和第七层策略。这意味着ZFW能提供基本状态检测允许或否决流量，以及在特殊活动的粒状第七层控制在多种协议，因此某些应用程序活动允许，当其他拒绝时。在此应用检查，您能申请不同种类的特定报头级别检验P2P应用程序。gnutella的一示例其次显示。

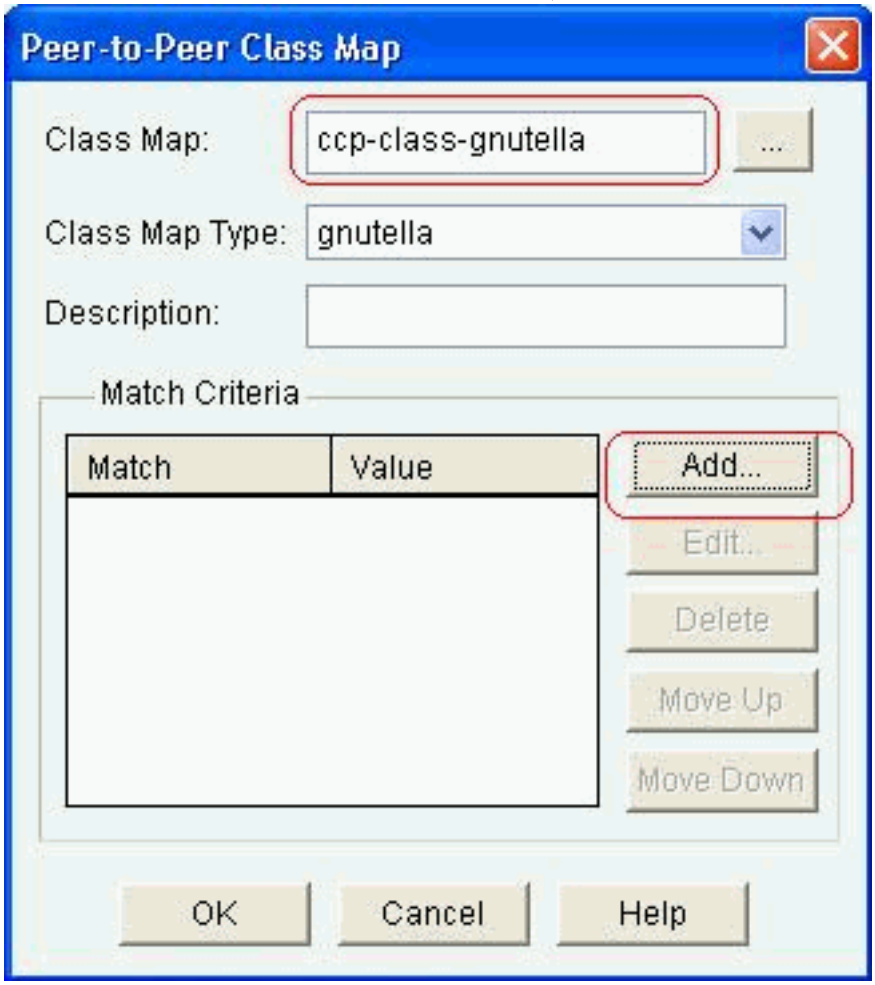
15. 检查**P2P**选项并且单击**创建**为了创建此的一新的策略映射。



16. 创建深度信息包检验的一新的策略映射gnutella协议的。单击**添加**然后选择**新的类映射**。

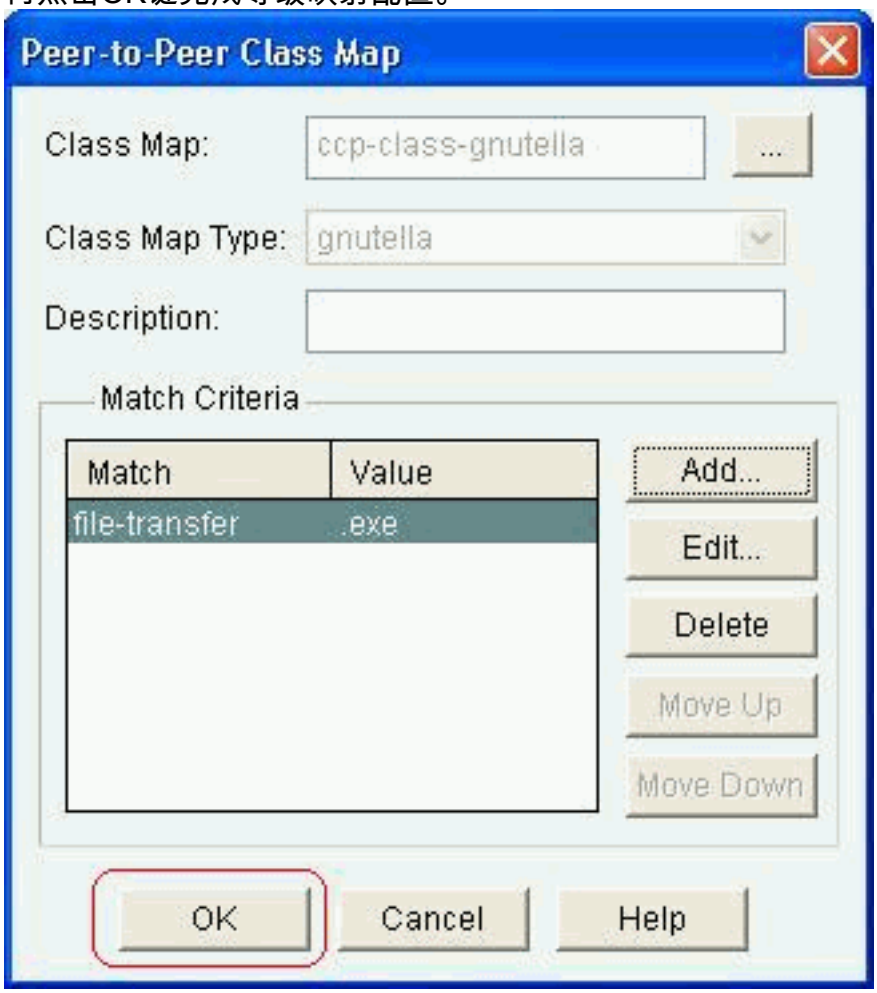


17. 给予一个新名字对于类映射并且单击**添加**指定匹配标准。

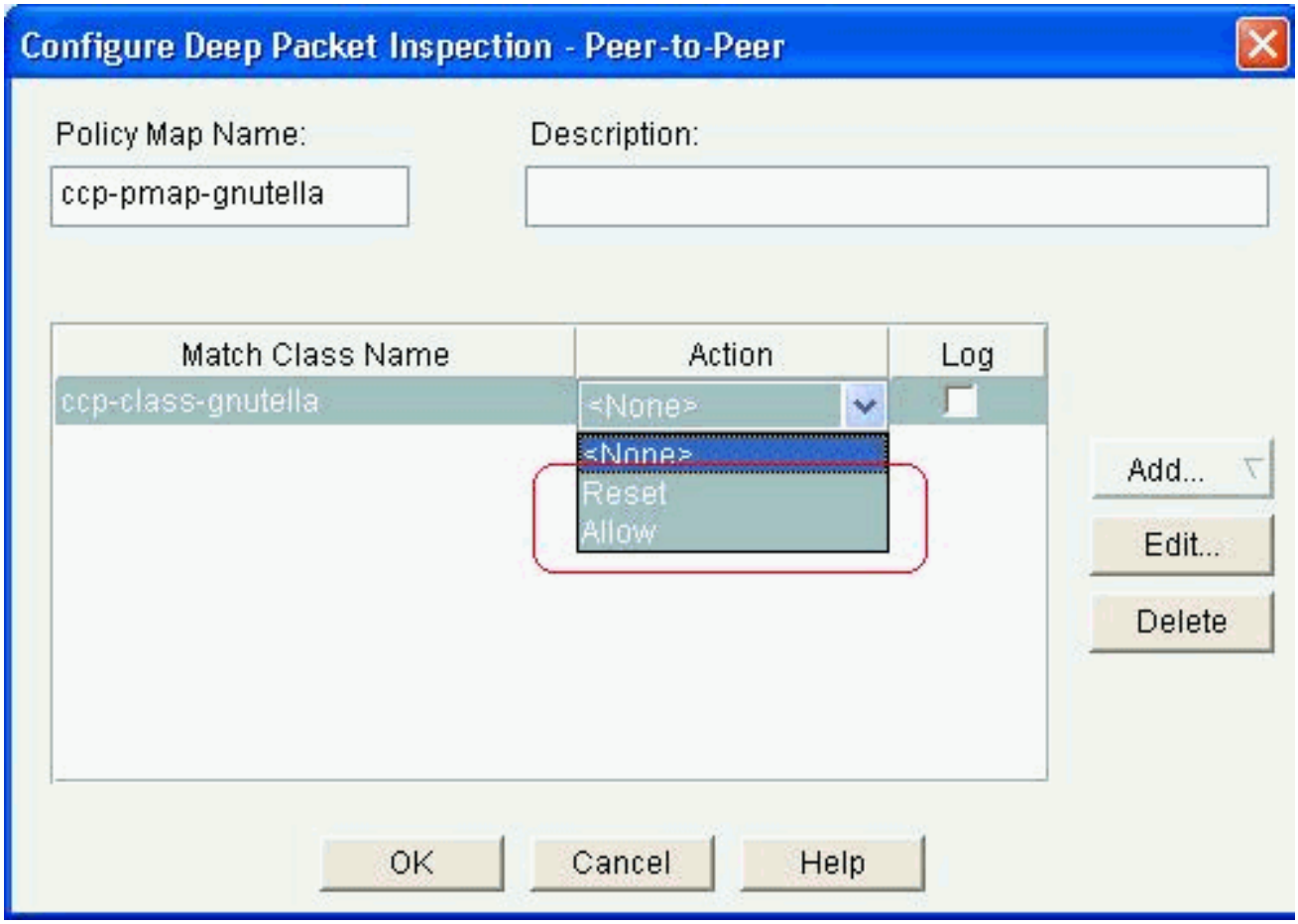


18. 因为使用的匹配标准和字符串是.exe，请使用文件传输。这表明包含数据流策略的所有gnutella文件传输连接.exe字符串匹配。单击 **Ok**。

19. 再点击OK键完成等级映射配置。

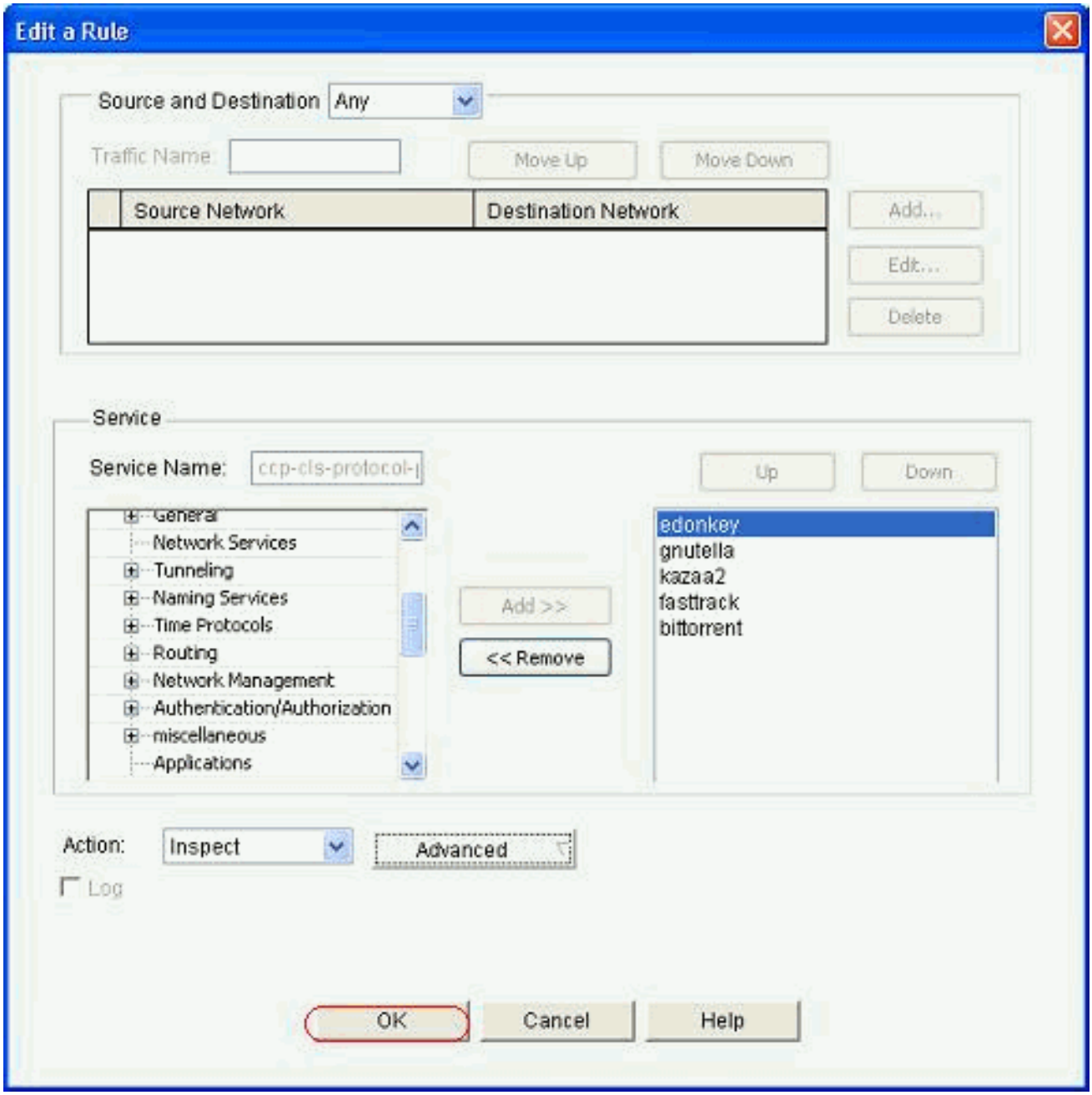


20. 选择**重置**或**允许**选项，取决于您的公司安全策略。点击OK键确认与策略映射的操作。



用同样这样您能添加其他策略映射通过指定不同的常规表达式实现其他P2P协议的深刻的检查功能作为匹配标准。**注意：** P2P 应用程序很难检测到，这是因为它们采用了“端口跳变”以及其他一些技巧以避免检测，同时 P2P 应用程序的频繁更改和更新也引入了一些问题，因为它们会修改协议的行为。ZFW与基于网络应用的识别(NBAR) ‘s结合本地防火墙状态检测流量识别功能提供P2P应用程序控制。**注意：** P2P 应用程序检查为第 4 层检查支持的部分应用程序提供了特定于应用程序的功能：edonkeyfasttrackgnutellakazaa2**注意：** 目前，ZFW没有一个选项检查“bittorrent”应用流量。BitTorrent客户端通常通信与跟踪仪(对等体目录服务器)通过在一些非标准端口的HTTP运行。此端口一般是 TCP 6969，但您可能需要检查 torrent 专用的 tracker 端口。如果希望允许BitTorrent，适应额外端口的佳方法是配置HTTP作为其中一match protocol和添加TCP 6969到HTTP使用此ip port-map命令：**port-map ip HTTP端口tcp 6969**。您需要将 http 和 bittorrent 定义为在类映射中应用的匹配条件。

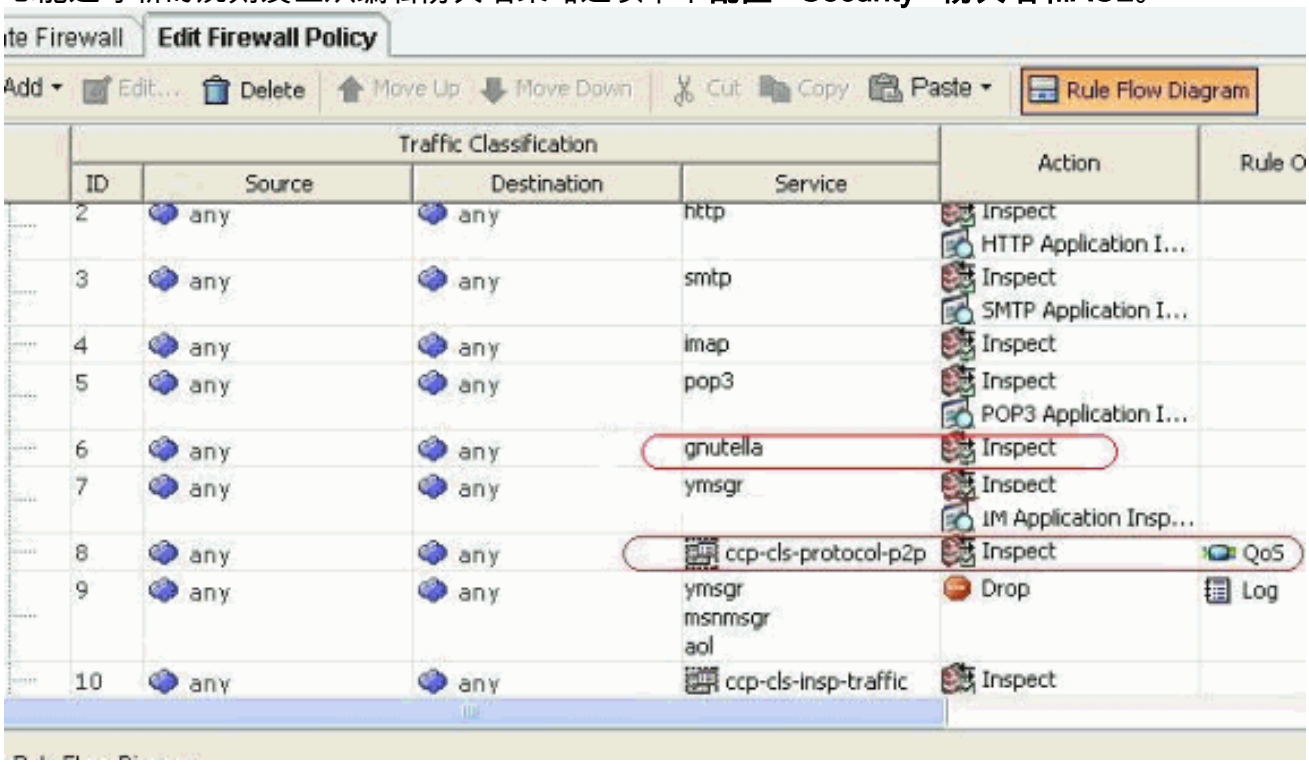
21. 点击OK键完成先进的检查配置。



对应的一组命令传送到路由器。

22. 点击OK键完成复制一组命令对路由器。

23. 您能遵守新的规则发生从编辑防火墙策略选项卡下**配置> Security >防火墙和ACL**。



ZFW路由器命令行配置

在前面部分的配置从思科CP导致在ZFW路由器的此配置：

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**策略映射类型Inspect区域对会话**—显示所有现有区域对的运行时Inspect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
- Cisco Configuration Professional主页
- Cisco Configuration Professional用户指南
- 技术支持和文档 - Cisco Systems