Cisco CP：ピアツーピアトラフィックをブロックするためのZFWの設定

内容

概要

このドキュメントでは、Cisco Configuration Professional（Cisco CP）の [Advanced Firewall] コンフィギュレーション ウィザードを使用して Cisco IOS ルータをゾーンベース ファイアウォールとして構成し、ピアツーピア（P2P）トラフィックをブロックする手順について説明します。

ゾーンベース ポリシー ファイアウォール（または Zone-Policy Firewall（ZFW））は、以前のインターフェイスベース モデルから、より柔軟性があり、より簡単に理解できるゾーンベース モデルへとファイアウォールの設定を変更しました。インターフェイスはゾーンに割り当てられ、検査ポリシーはゾーン間を移動するトラフィックに適用されます。ゾーン間ポリシーにより、十分な柔軟性と精度が実現します。このため、同一のルータ インターフェイスに接続された複数のホスト グループにさまざまな検査ポリシーを適用できます。ゾーンは、ネットワークのセキュリティ境界を設定します。ゾーンは、トラフィックがネットワークの別の領域に移動するときにポリシーの制限の対象となる境界を定義します。ZFW のゾーン間のデフォルト ポリシーは「deny all」です。ポリシーが明示的に設定されていない場合は、ゾーン間を移動するすべてのトラフィックがブロックされます。

P2P アプリケーションは、インターネット上で最も広く利用されているアプリケーションです。P2P ネットワークは、ファイアウォールを簡単に回避する手段を提供し、プライバシーとセキュリティに関する問題の原因となって、ワームなどの悪意ある脅威を導く経路として機能する可能性があります。Cisco IOS ソフトウェア リリース 12.4(9)T では、P2P アプリケーションの ZFW サポートが導入されました。P2P 検査は、アプリケーション トラフィック用のレイヤ 4 およびレイヤ 7 ポリシーを提供します。つまり、他のアクティビティが拒否されても特定のアプリケーション アクティビティは許可されるように、ZFW が、トラフィックを許可または拒否するための基本のステートフル検査と、さまざまなプロトコルの具体的なアクティビティに対する細かいレ

イヤ 7 制御を提供できることを意味します。

Cisco CP には、[Advanced Firewall] コンフィギュレーション ウィザードを使用して IOS ルータをゾーンベース ファイアウォールとして設定する、わかりやすい手順が用意されています。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- IOS ルータのソフトウェア バージョンが 12.4(9)T 以降であること。
- Cisco CP をサポートする IOS ルータ モデルの場合は、『Cisco CP リリース ノート』を参照してください。

Cisco CP を実行するためのルータの設定

注：CiscoルータでCisco CPを実行するには、次の設定手順を実行します。

```
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
```

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- IOS ソフトウェア リリース 12.4(15)T が稼働する Cisco 1841 IOS ルータ
- Cisco Configuration Professional（Cisco CP）リリース 2.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

このドキュメントの例では、ルータをゾーンベース ファイアウォールとして設定し、P2P トラフィックをブロックしています。ZFW ルータには、ゾーン内の内部（信頼できる）インターフェイ

スと、ゾーン外の外部（信頼できない）インターフェイスの 2 つのインターフェイスがあります。ZFW ルータは、ゾーン内からゾーン外に渡されるトラフィックのロギング アクションによって、edonkey、fasttrack、gnutella、kazaa2 などの P2P アプリケーションをブロックします。

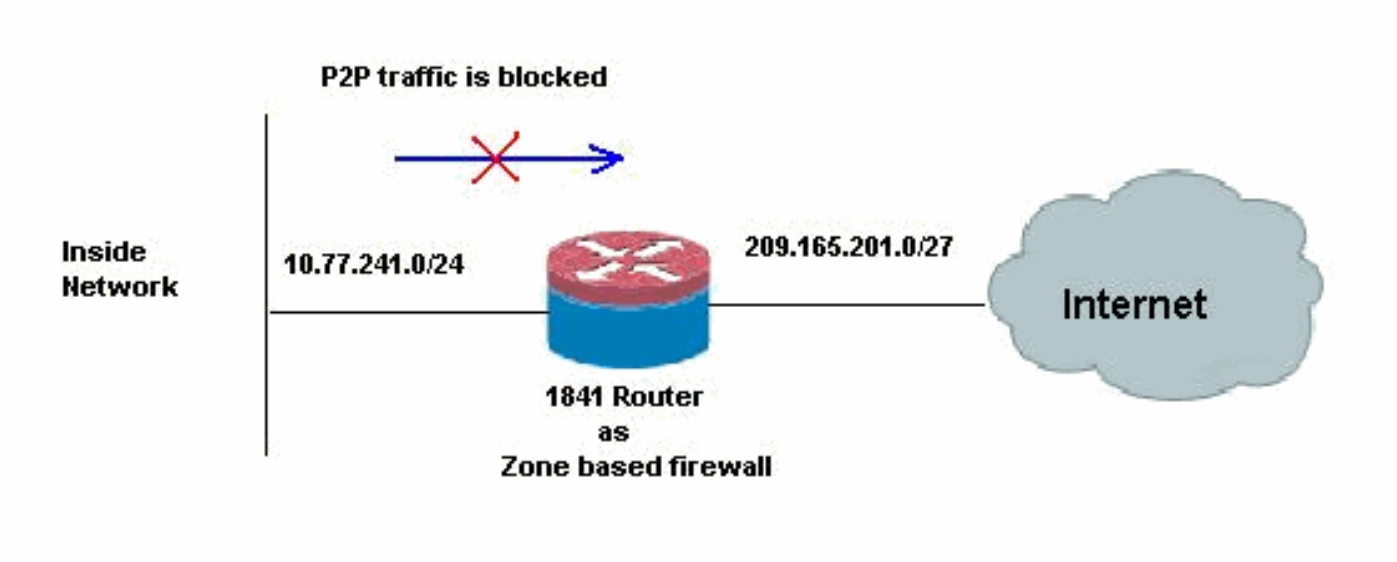
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。

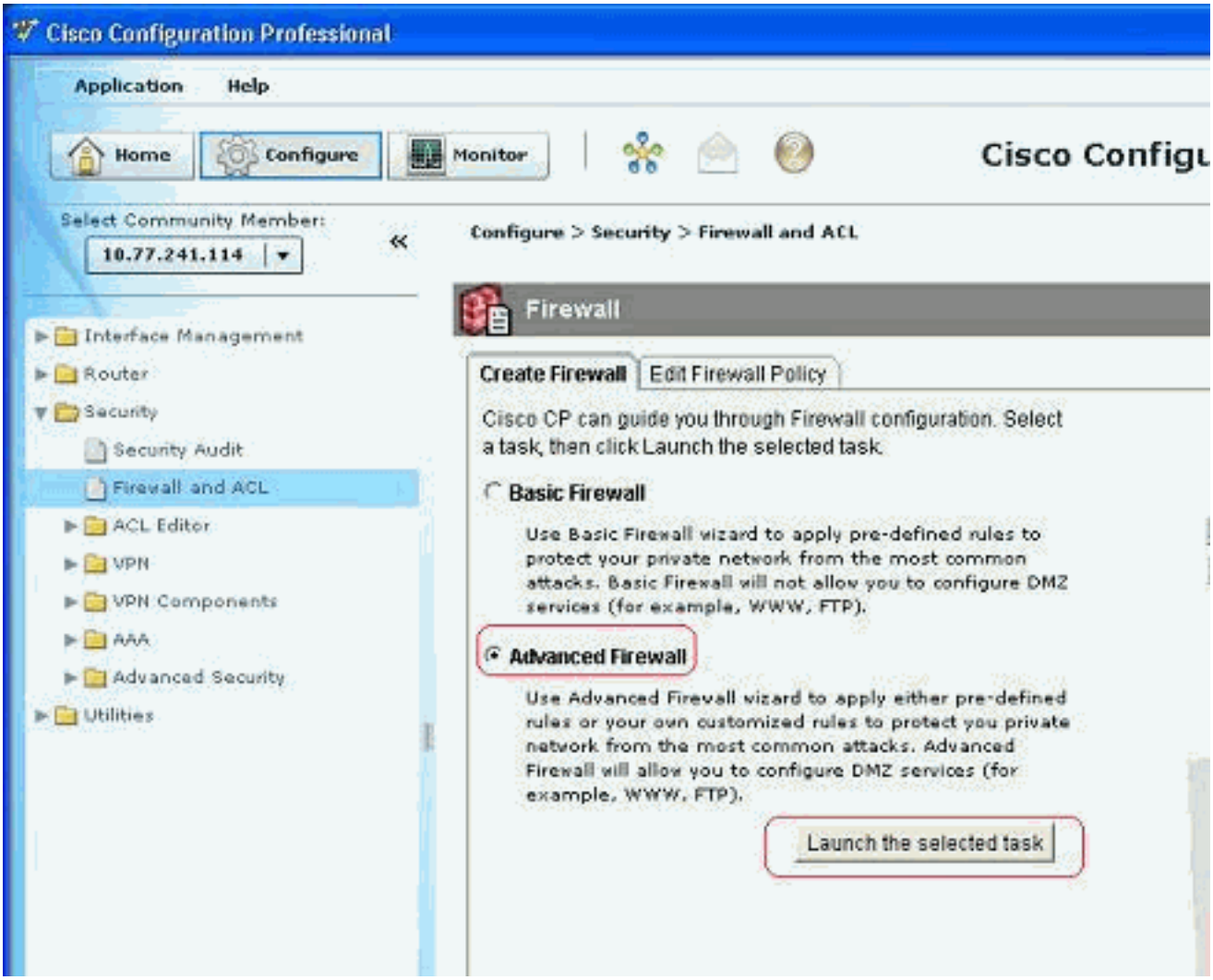


Cisco Configuration Professional を使用した設定

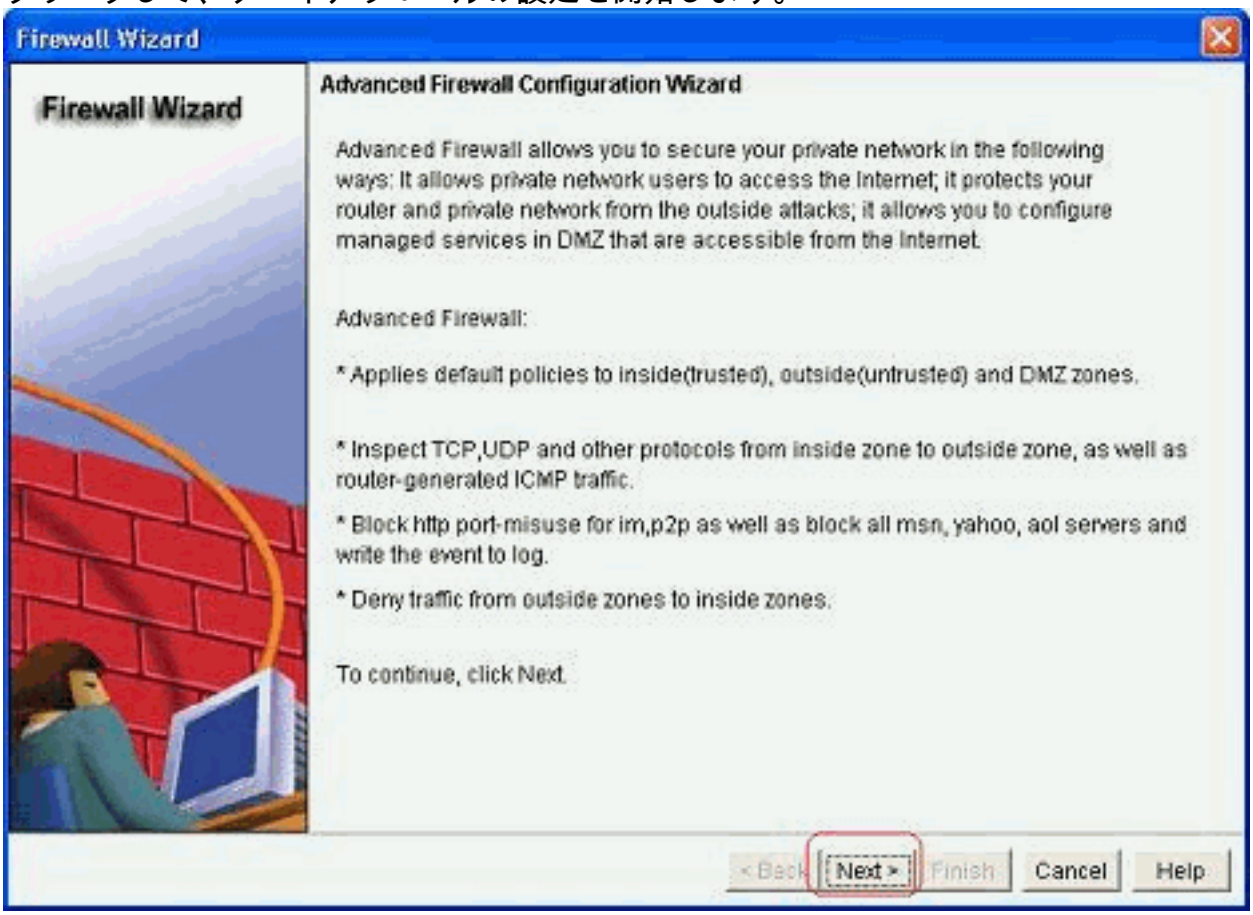
このセクションでは、ウィザードを使用して IOS ルータをゾーンベース ファイアウォールとして設定する手順を示しています。

次のステップを実行します。

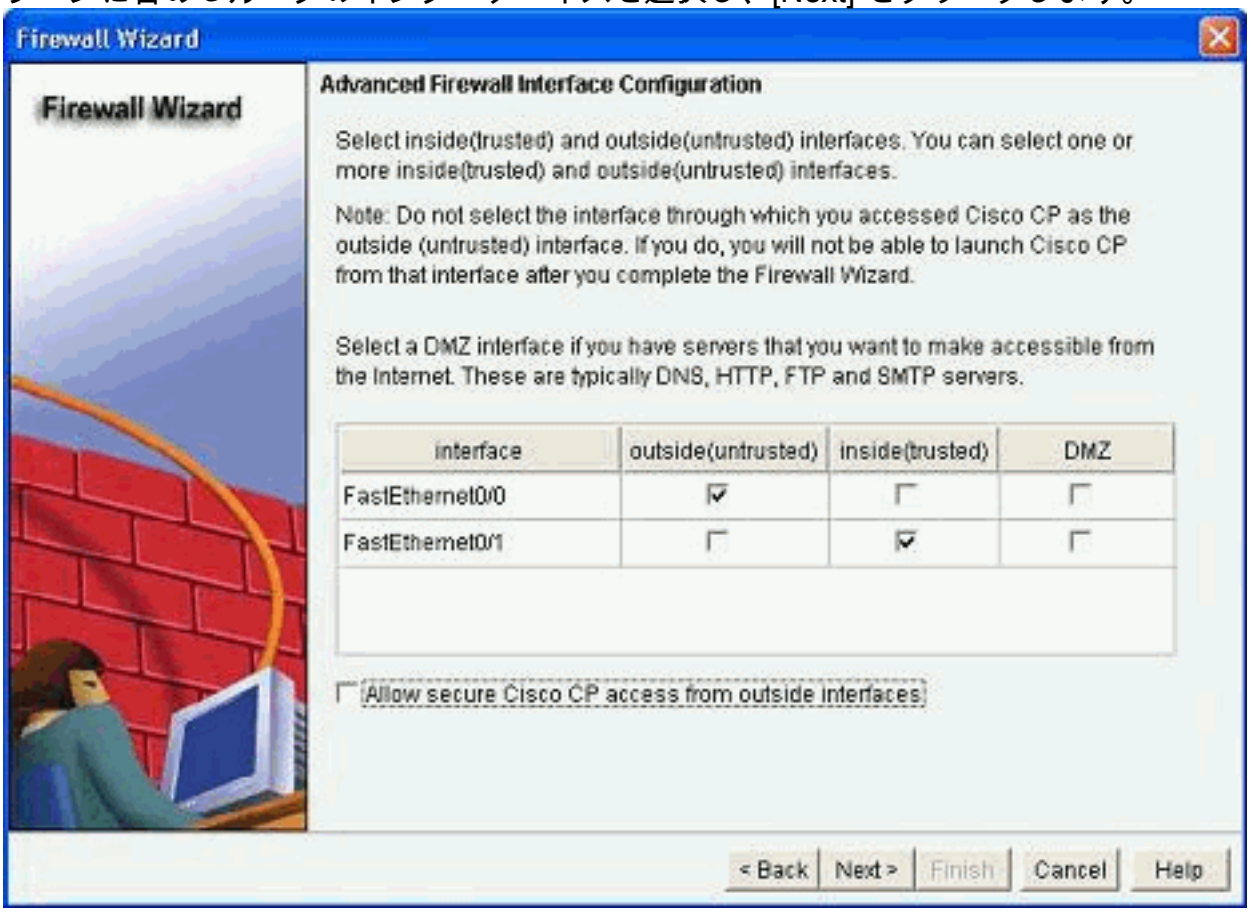
1. [Configure] > [Security] > [Firewall and ACL] の順に移動します。続いて、[Advanced Firewall] オプション ボタンを選択します。[Launch the selected task] をクリックします。



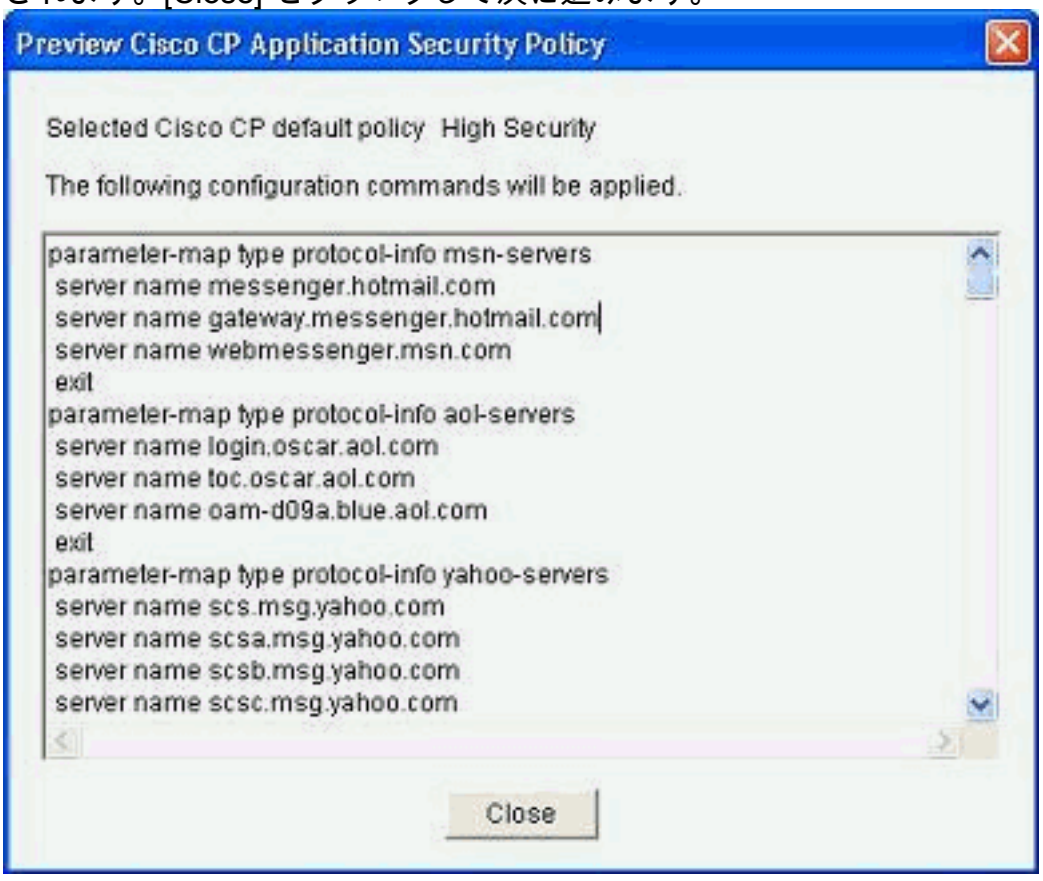
2. 次の画面には、ファイアウォール ウィザードに関する概要説明が示されています。[Next] をクリックして、ファイアウォールの設定を開始します。



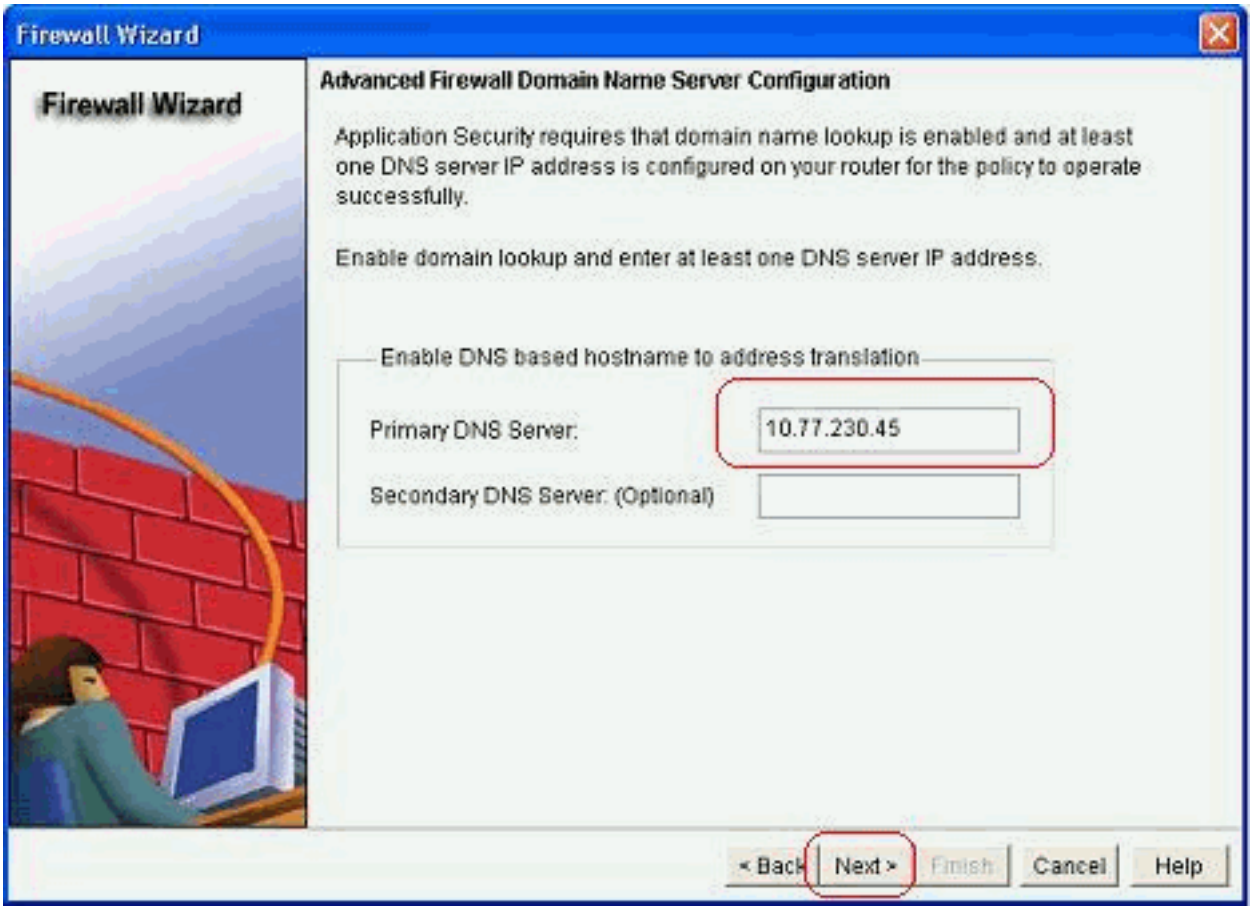
3. ゾーンに含めるルータのインターフェイスを選択し、[Next] をクリックします。



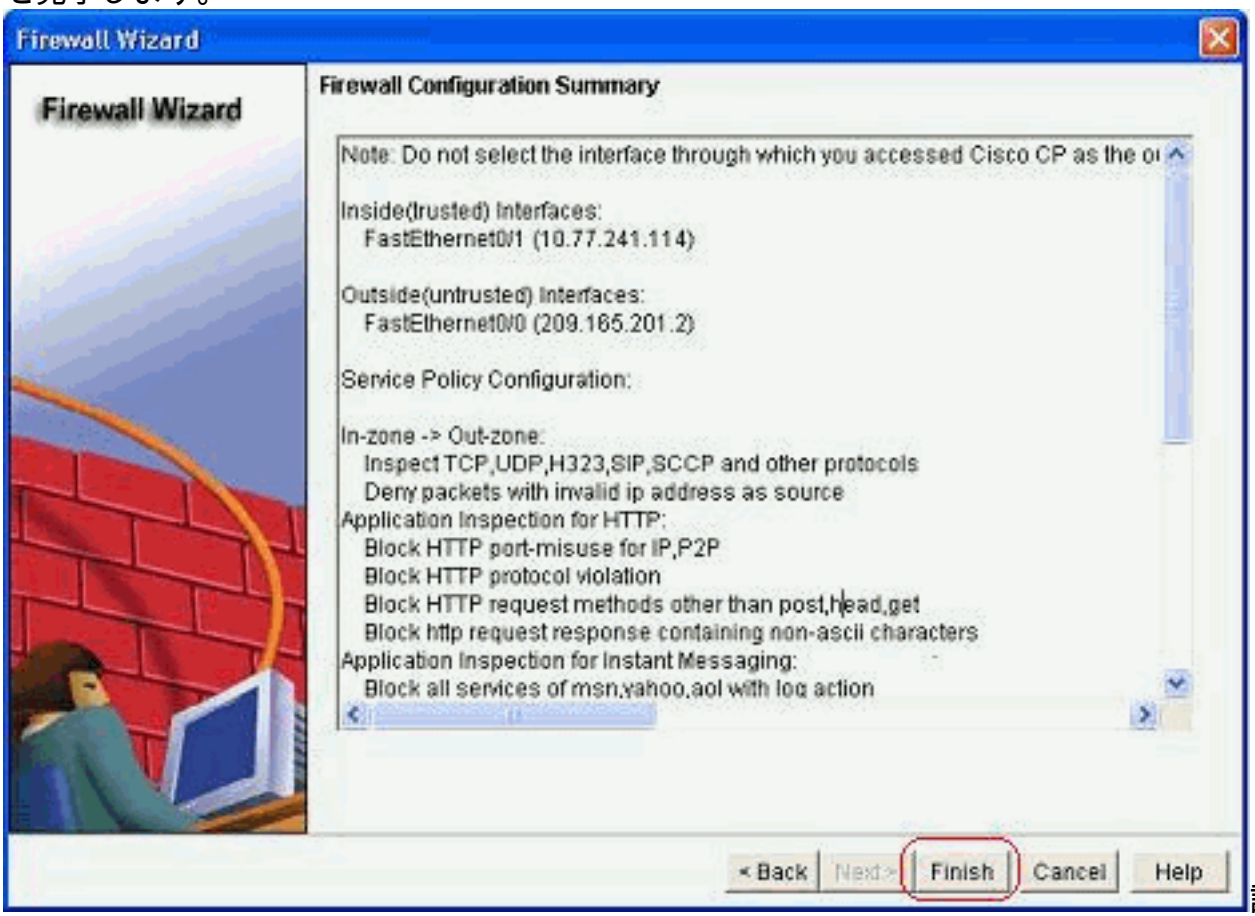
4. 高セキュリティのデフォルト ポリシーが、コマンド セットとともに次のウィンドウに表示されます。[Close] をクリックして次に進みます。



5. DNS サーバの詳細情報を入力して、[Next] をクリックします。



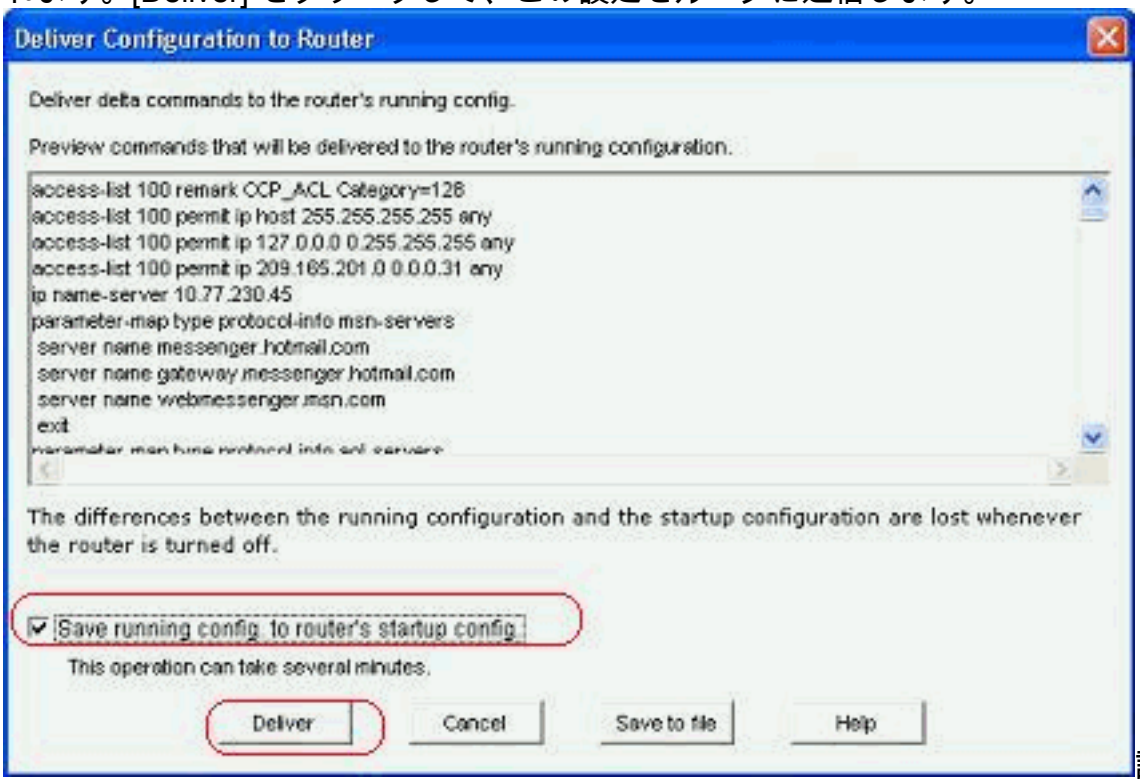
6. Cisco CP により、次に示すような設定の要約が表示されます。[Finish] をクリックして設定を完了します。



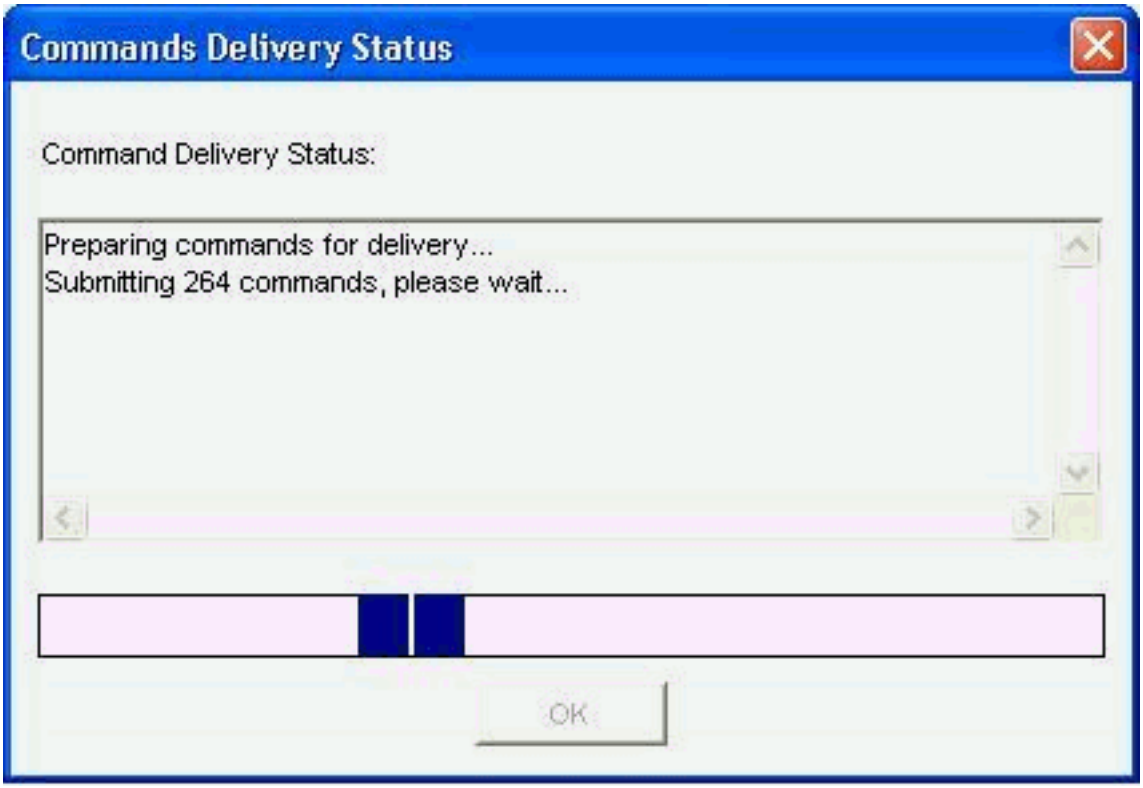
設定の要約の詳細を次の表に示します。これは、Cisco CP の高セキュリティ ポリシーによるデフォルトの設定です。

7. [Save the running config to router's startup config] チェックボックスにチェックマークを入

れます。[Deliver] をクリックして、この設定をルータに送信します。



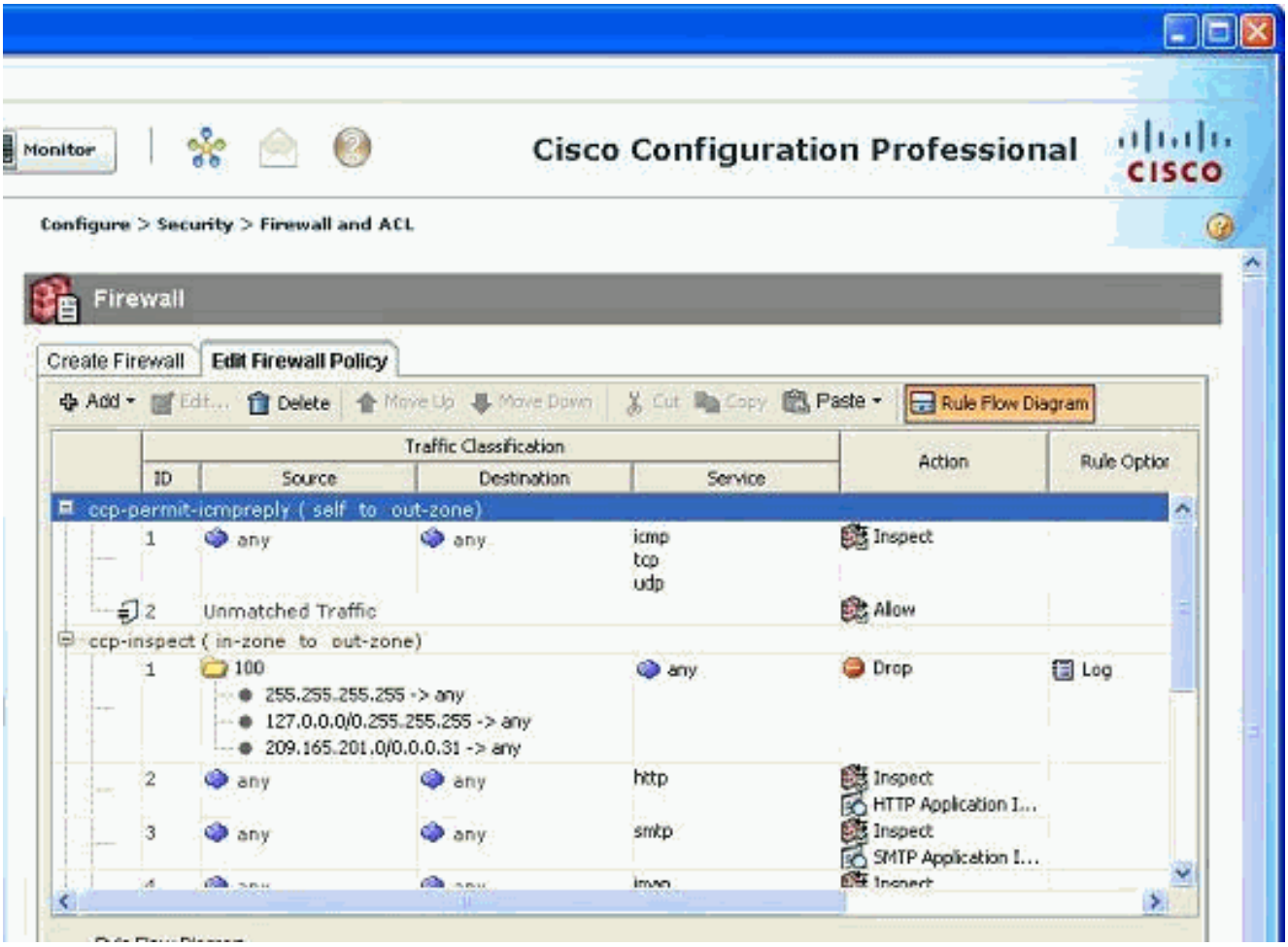
設定全体がルータに送られます。この処理には少し時間がかかります。



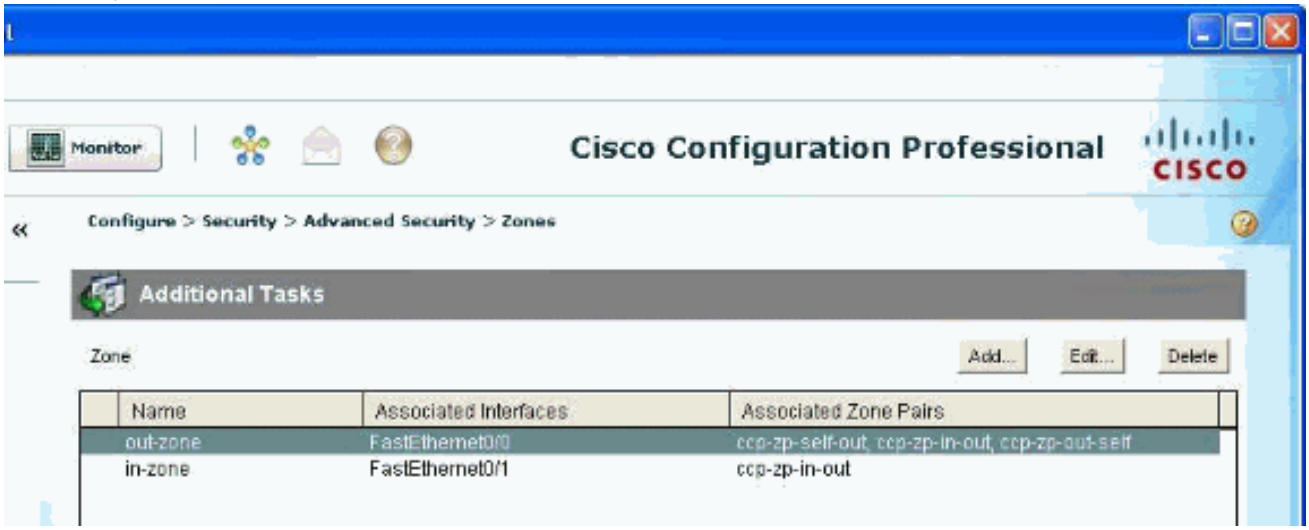
8. [OK] をクリックして続行します。

9. もう一度 [OK] をクリックします。

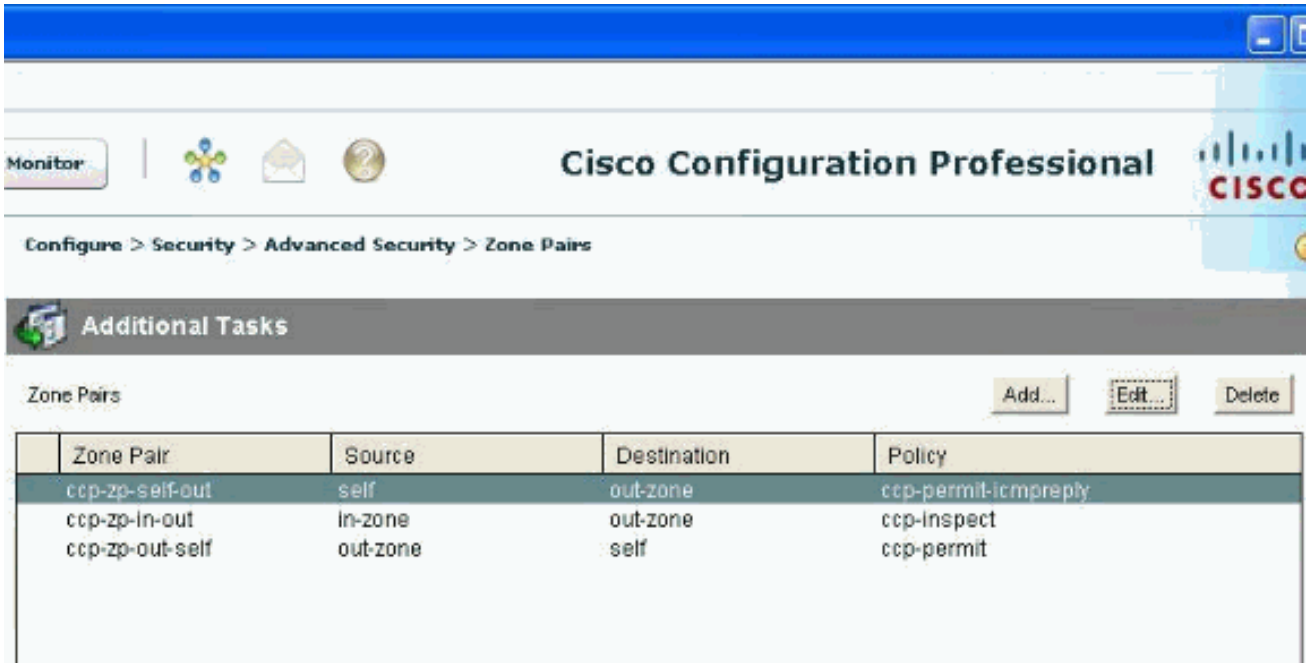
これで設定が有効になり、[Firewall Policy] タブにルールとして表示されます。



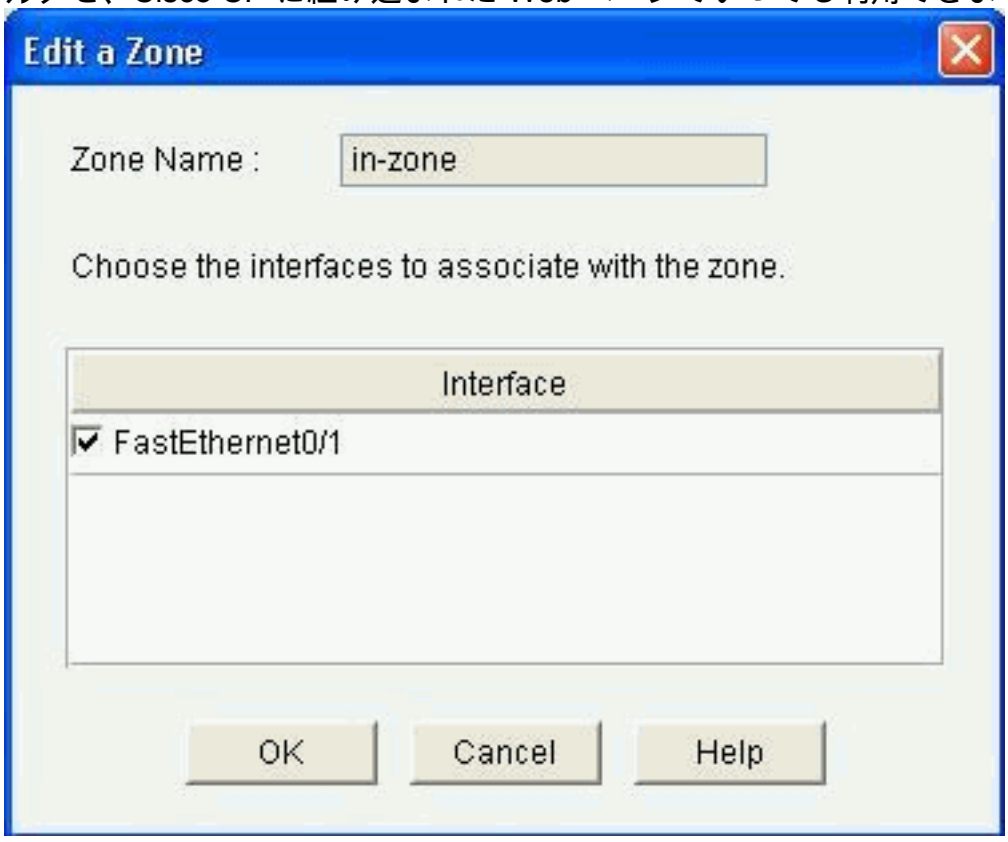
10. [Configure] > [Security] > [Advanced Security] > [Zones] の順に移動すると、ゾーン、およびそれらのゾーンが関連付けられているゾーン ペアを表示できます。また、[Add] をクリックして新しいゾーンを追加したり、[Edit] をクリックして既存のゾーンを変更することができます。

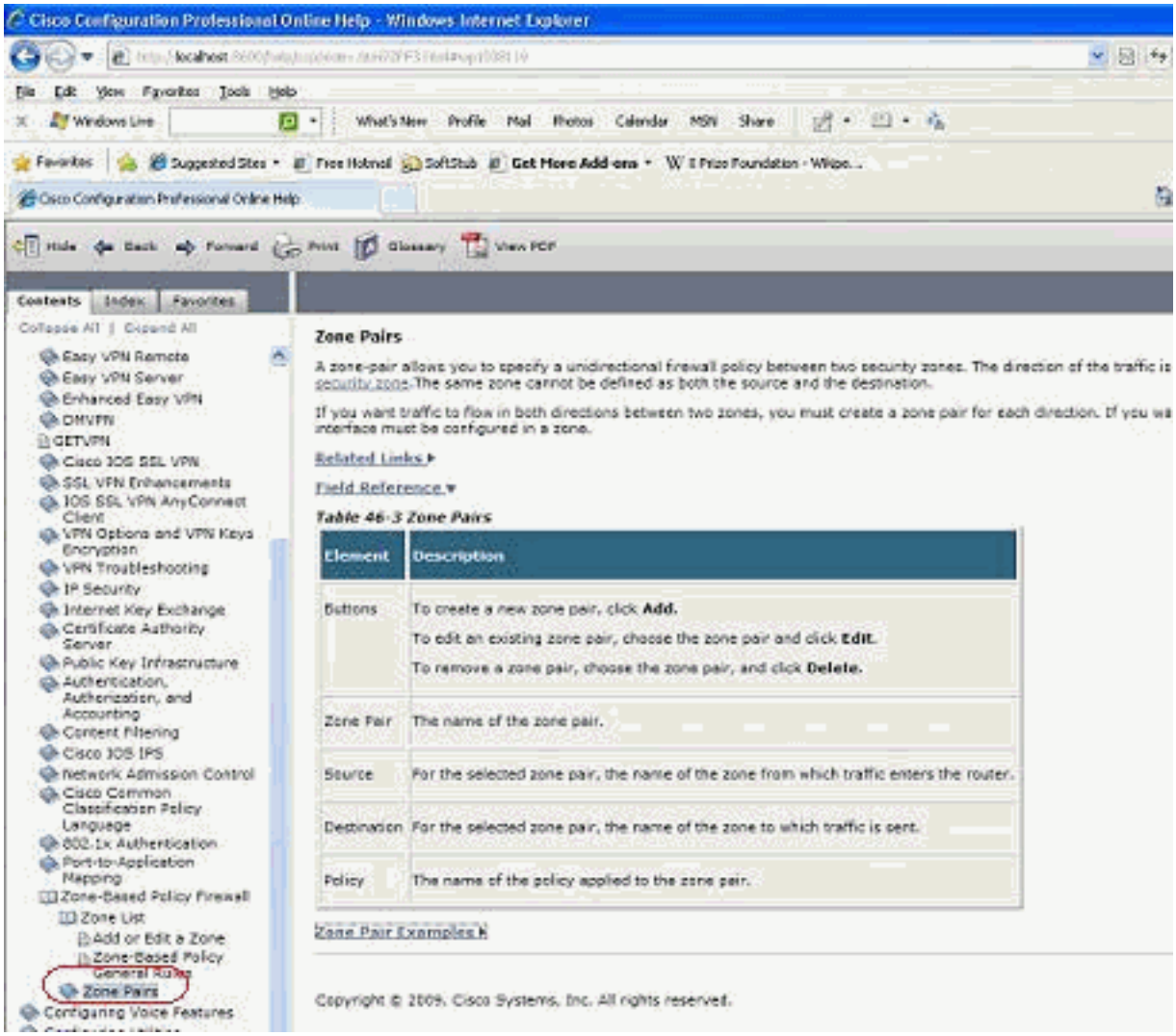


11. [Configure] > [Security] > [Advanced Security] > [Zone Pairs] の順に移動して、ゾーン ペアの詳細情報を表示します。

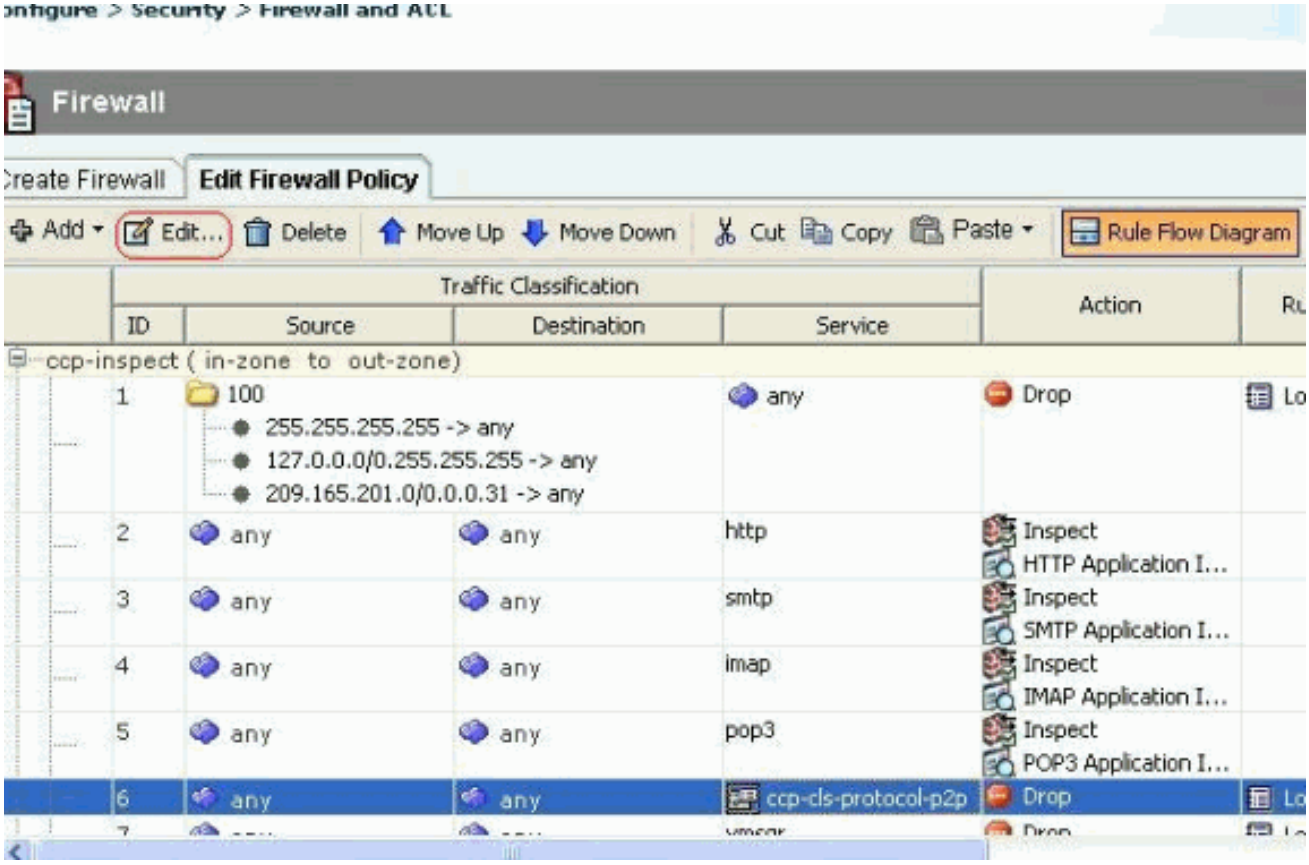


ゾーン/ゾーン ペアおよびその他の関連情報の変更/追加/削除方法に関するインスタント ヘルプを、Cisco CP に組み込まれた Web ページでいつでも利用できます。

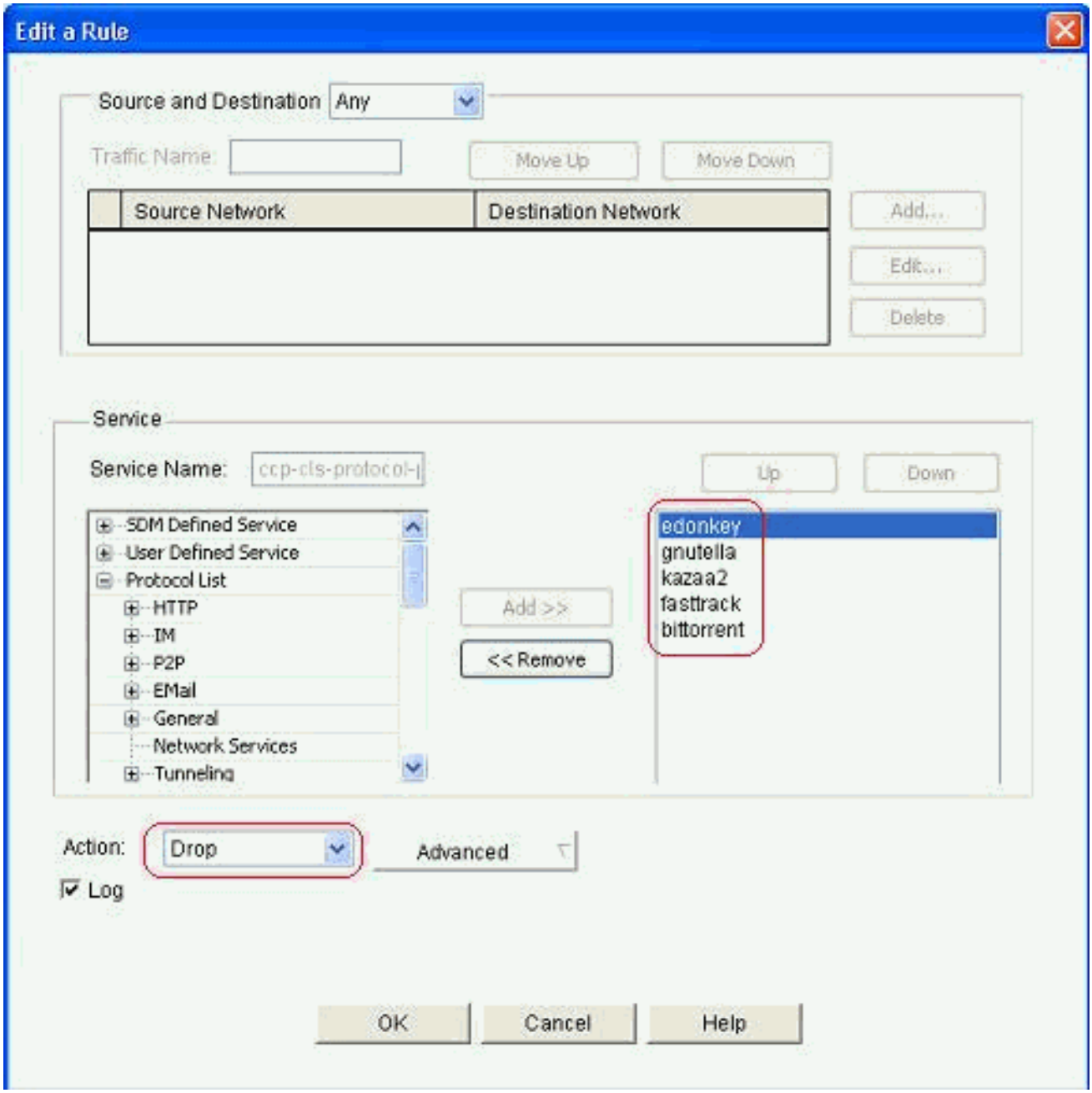




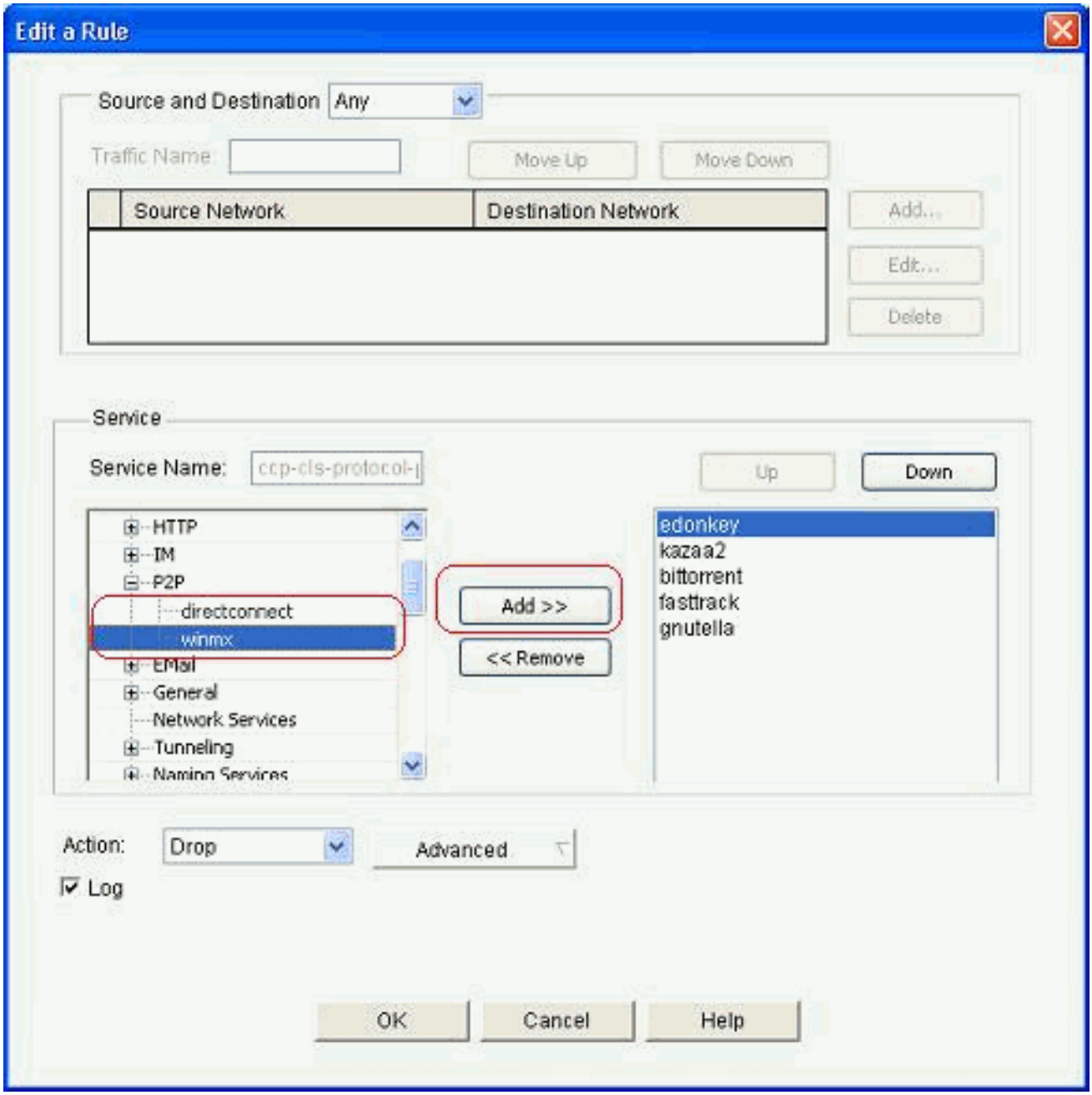
12. 特定の P2P アプリケーションについて、アプリケーション固有の検査機能を変更するには、[Configuration] > [Security] > [Firewall and ACL] の順に移動します。続いて [Edit Firewall Policy] をクリックし、ポリシー マップの個々のルールを選択します。[Edit] をクリックします。

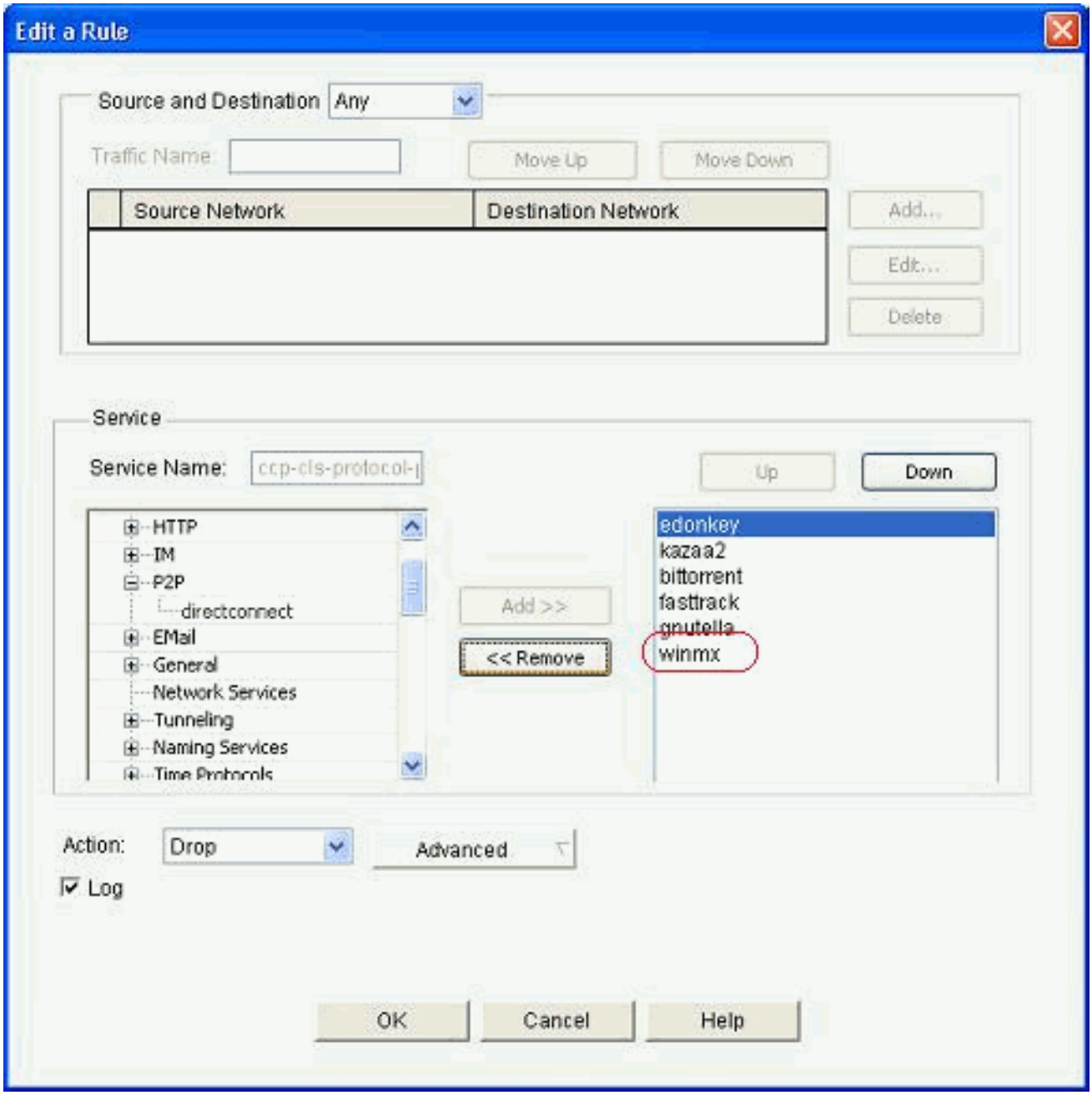


次の画面には、デフォルト設定によってブロックされる P2P アプリケーションが示されています。

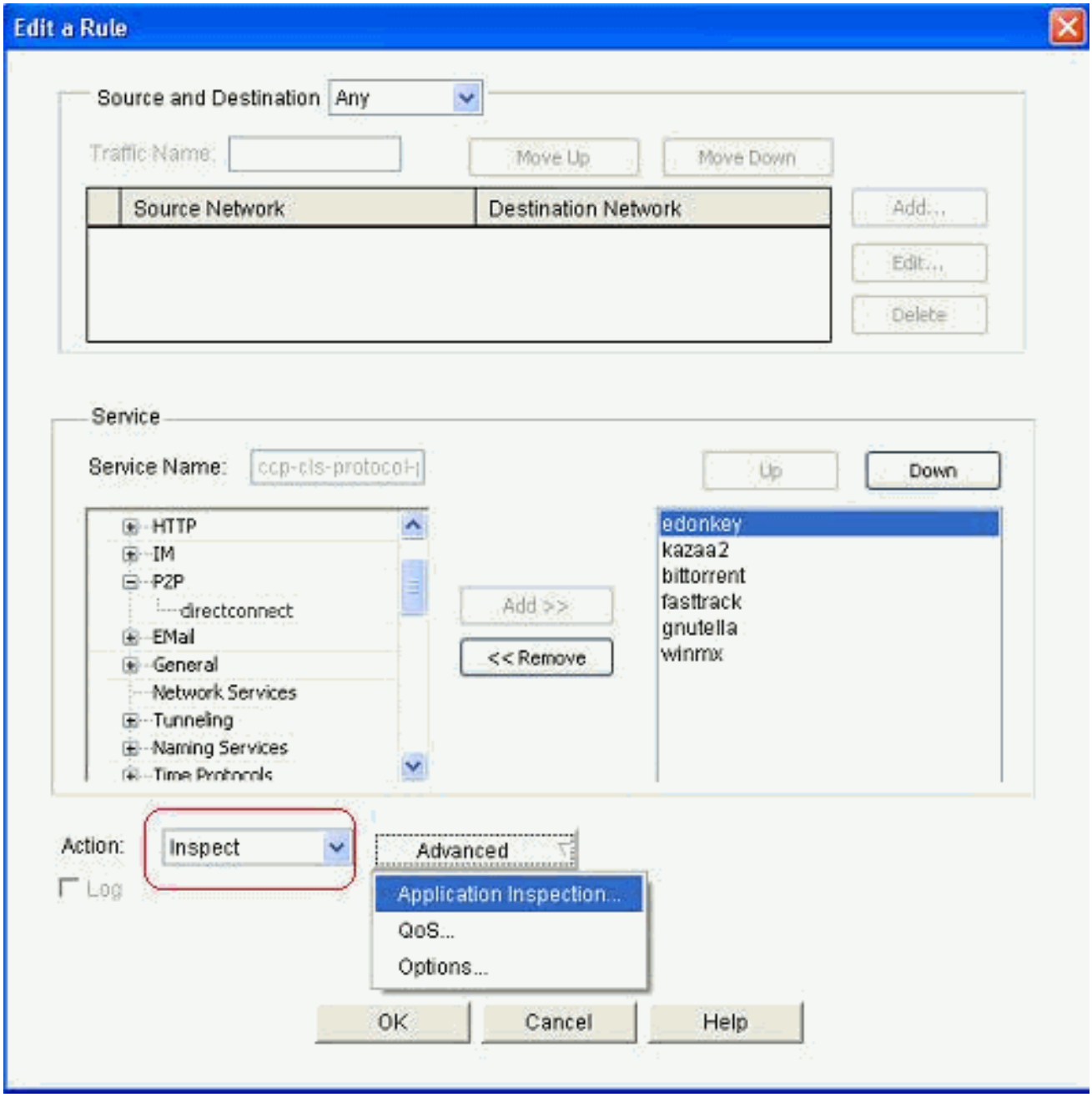


13. [Add] ボタンと [Remove] ボタンを使用して、特定のアプリケーションを追加/削除できます。次のスクリーンショットでは、winmx アプリケーションをブロックの対象として追加する方法を示しています。


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

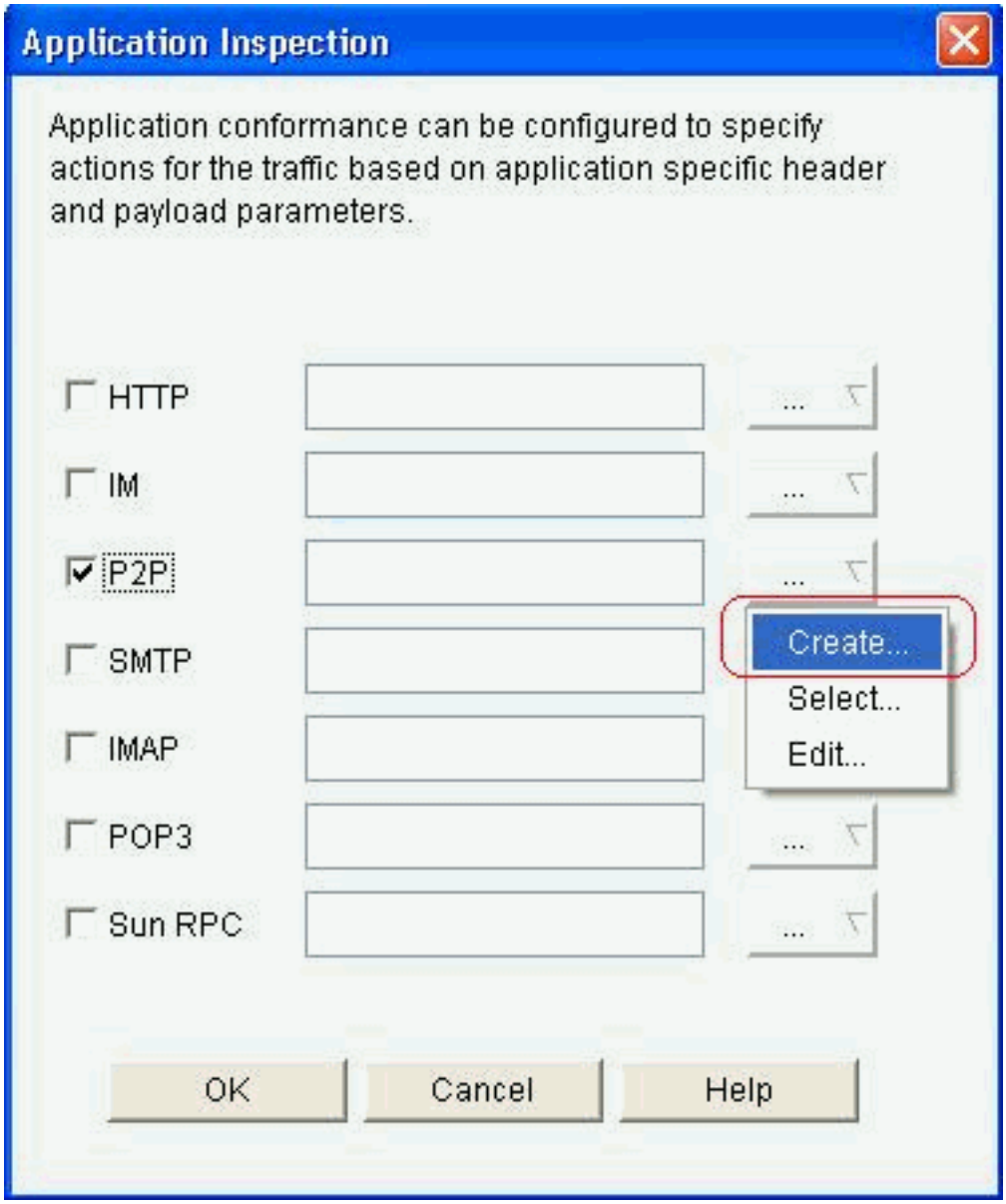


14. 廃棄アクションを選択する代わりに検査アクションを選択して、ディープ パケット インスペクションを行う別のアクションを適用することもできます。

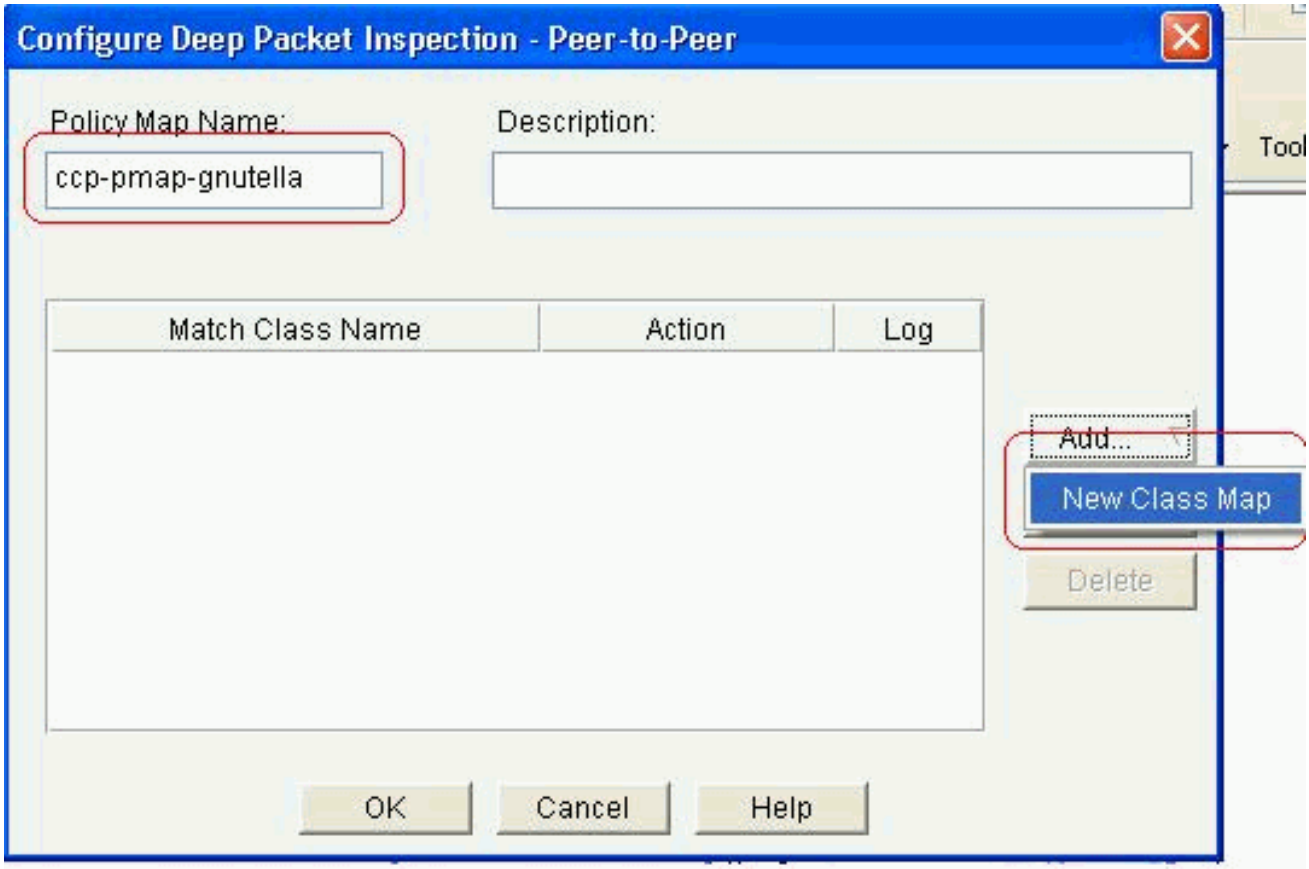


P2P 検査は、アプリケーション トラフィック用のレイヤ 4 およびレイヤ 7 ポリシーを提供します。つまり、他のアクティビティが拒否されても特定のアプリケーション アクティビティは許可されるように、ZFW が、トラフィックを許可または拒否するための基本のステートフル検査と、さまざまなプロトコルの具体的なアクティビティに対する細かいレイヤ 7 制御を提供できることを意味します。このアプリケーション検査では、P2P アプリケーションにさまざまな種類のヘッダー レベルの検査を適用できます。gnutella の例をこの後に示します。

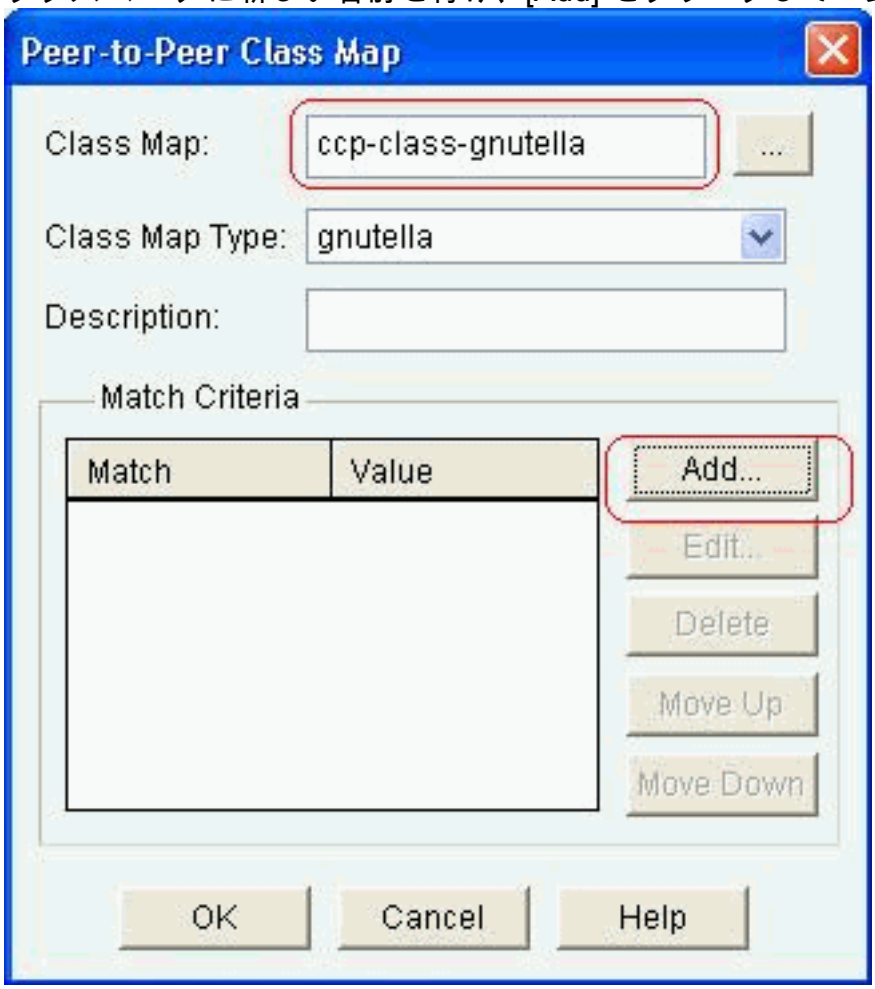
15. [P2P] オプションにチェックマークを入れ、[Create] をクリックして、このための新しいポリシー マップを作成します。



16. ディープ パケット インスペクションを行う gnutella プロトコルの新しいポリシー マップを作成します。[Add] をクリックし、[New Class Map] を選択します。

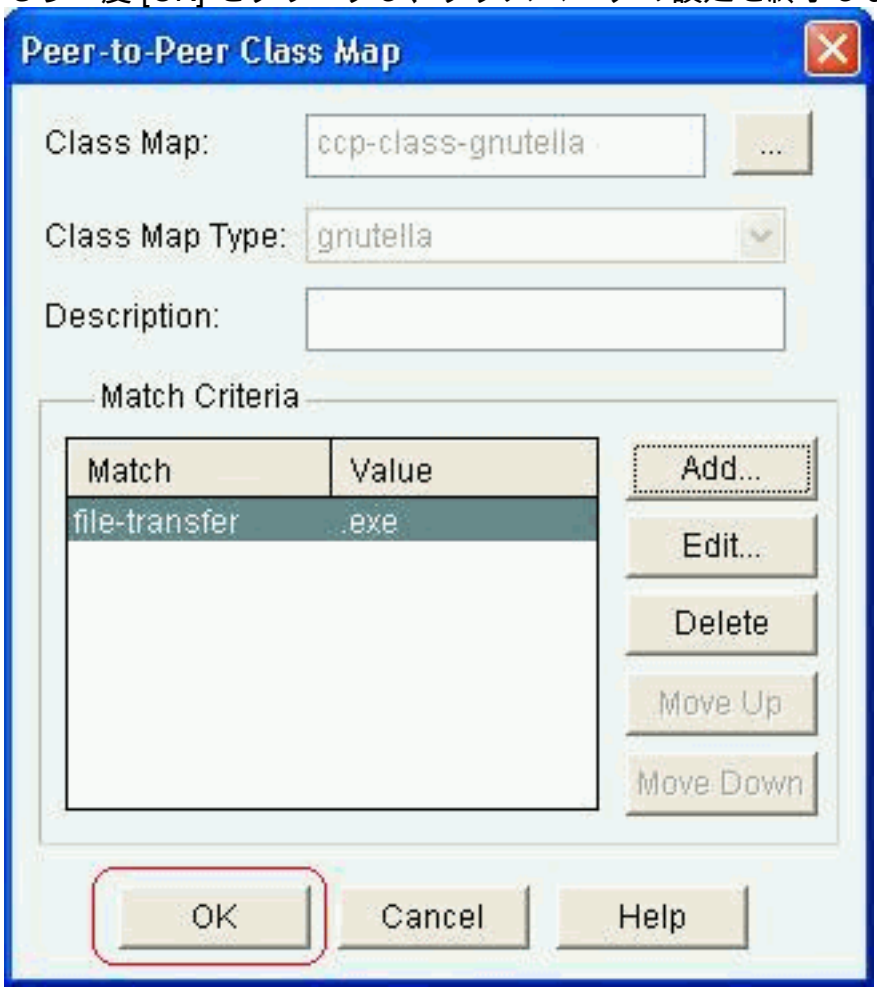


17. クラス マップに新しい名前を付け、[Add] をクリックして一致基準を指定します。

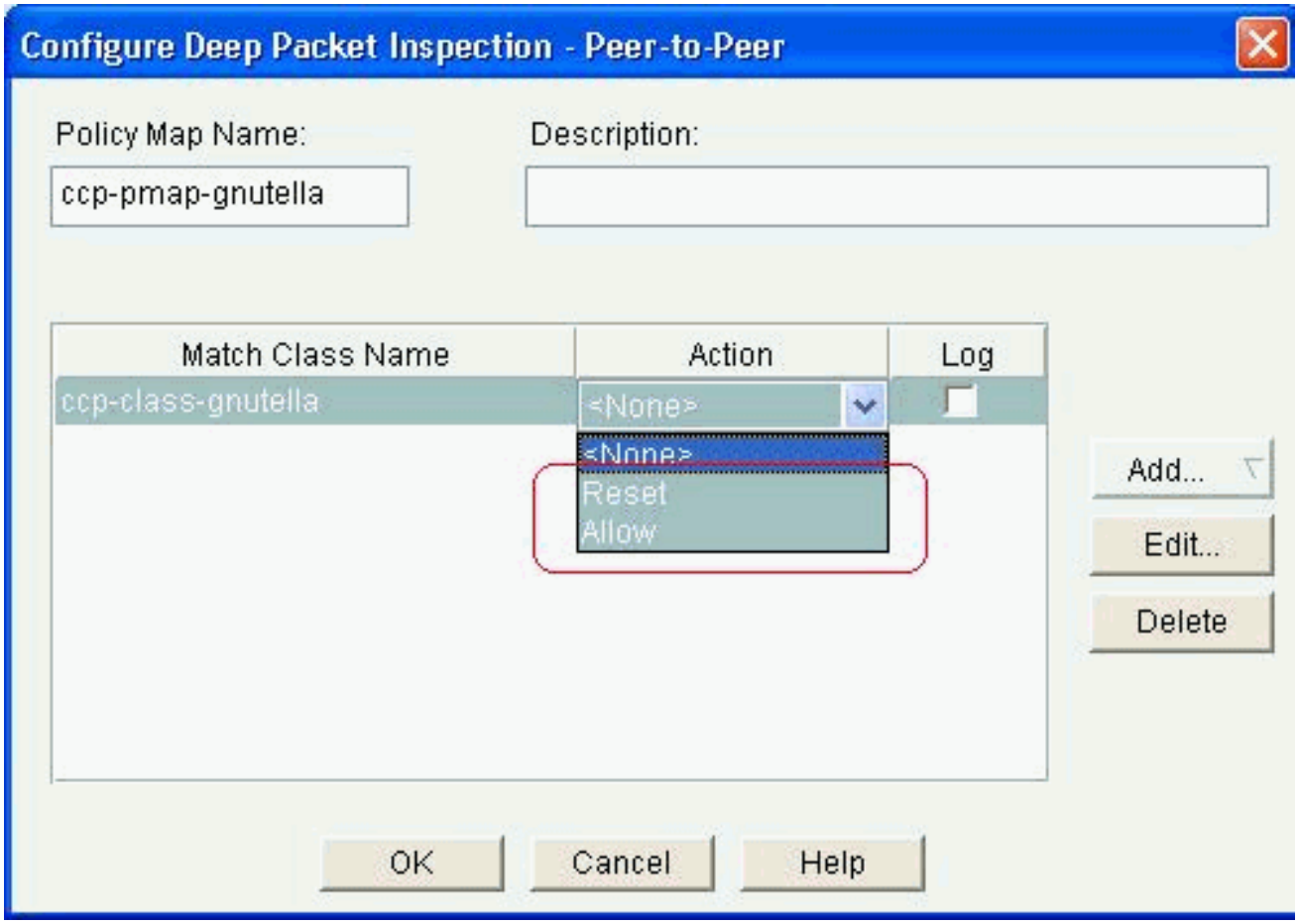


18. 一致基準として [file-transfer] を使用し、使用する文字列は「.exe」にします。「.exe」という文字列を含むすべての gnutella ファイル転送接続が、トラフィック ポリシーに一致することを意味します。[OK] をクリックします。

19. もう一度 [OK] をクリックし、クラス マップの設定を終了します。

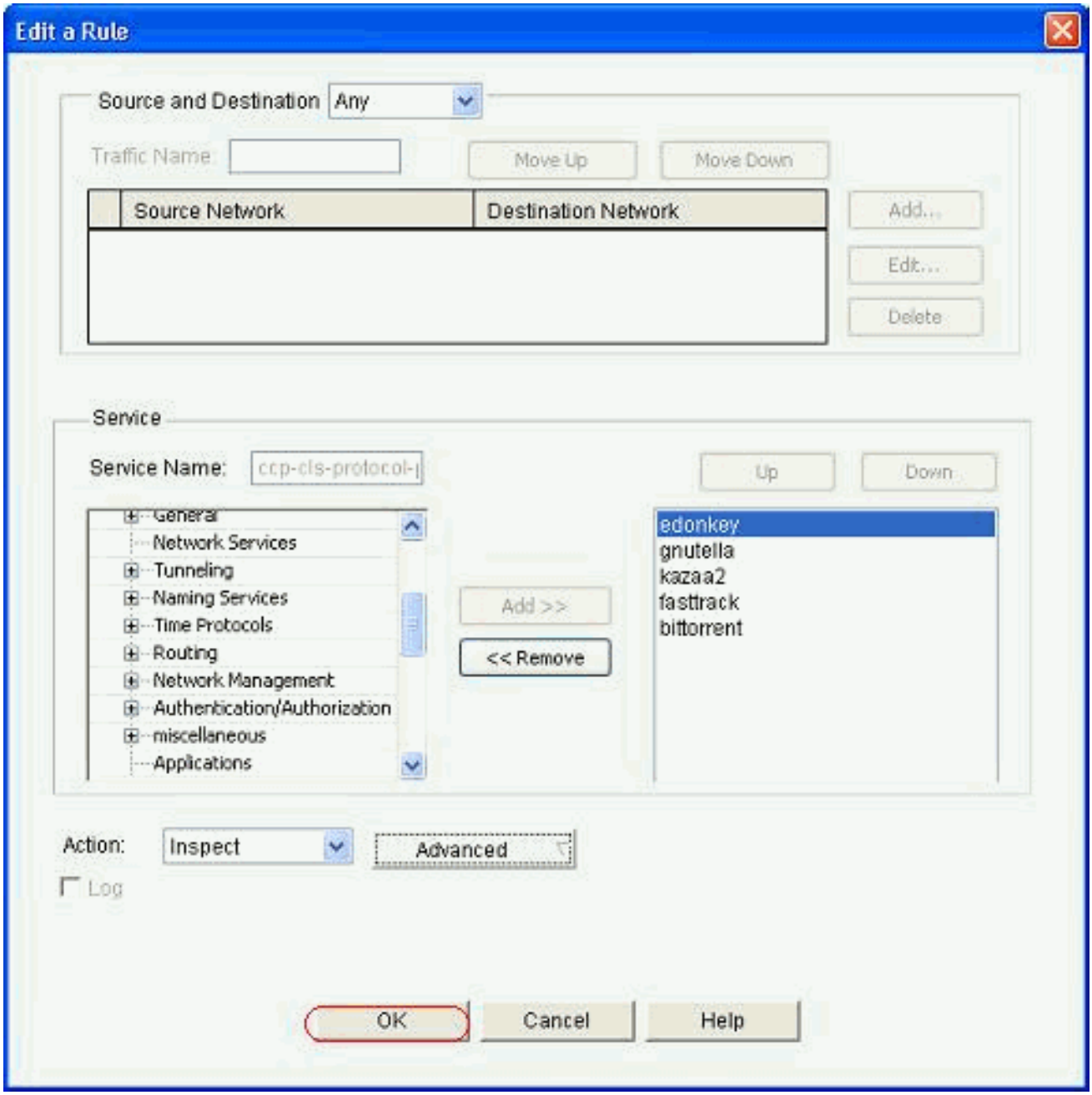


20. 会社のセキュリティ ポリシーに応じて、[Reset] または [Allow] オプションを選択します。[OK] をクリックして、ポリシー マップに設定するアクションを確認します。



以上と同じ方法で他のポリシー マップを追加し、一致基準として異なる正規表現を指定して、その他の P2P プロトコルにディープ インスペクション機能を実装できます。注：P2Pアプリケーションは、「ポートホッピング」の動作や検出を回避する他のトリックの結果、特に検出が困難です。また、プロトコルの動作を変更するP2Pアプリケーションの頻繁な変更や更新によって発生するする問題もあります。ZFW は、ネイティブのファイアウォール ステートフル検査と Network-Based Application Recognition (NBAR; ネットワークベースのアプリケーション認識) のトラフィック認識機能を組み合わせることで、P2P アプリケーション制御を提供します。**注：**P2P Application Inspectionは、レイヤ4インスペクションでサポートされるアプリケーションのサブセットに対してアプリケーション固有の機能を提供します。edonkeyfasttrackgnutellakazaa2**注：現在は**、ZFWには「bittorrent」アプリケーショントラフィックを検査するオプションはありません。BitTorrent クライアントは通常、非標準のポート上で動作している HTTP 経由でトラッカー (ピア ディレクトリ サーバ) と通信します。通常、これは TCP 6969 ですが、トレント固有のトラッカー ポートをチェックする必要があるかもしれません。BitTorrent を許可する場合、追加のポートに対処する最善の方法は、照合プロトコルの 1 つとして HTTP を設定し、次の ip port-map コマンドを使用して TCP 6969 を HTTP に追加することです：**ip port-map http port tcp 6969**。クラスマップに適用する照合基準として http と bitTorrent を定義する必要があります。

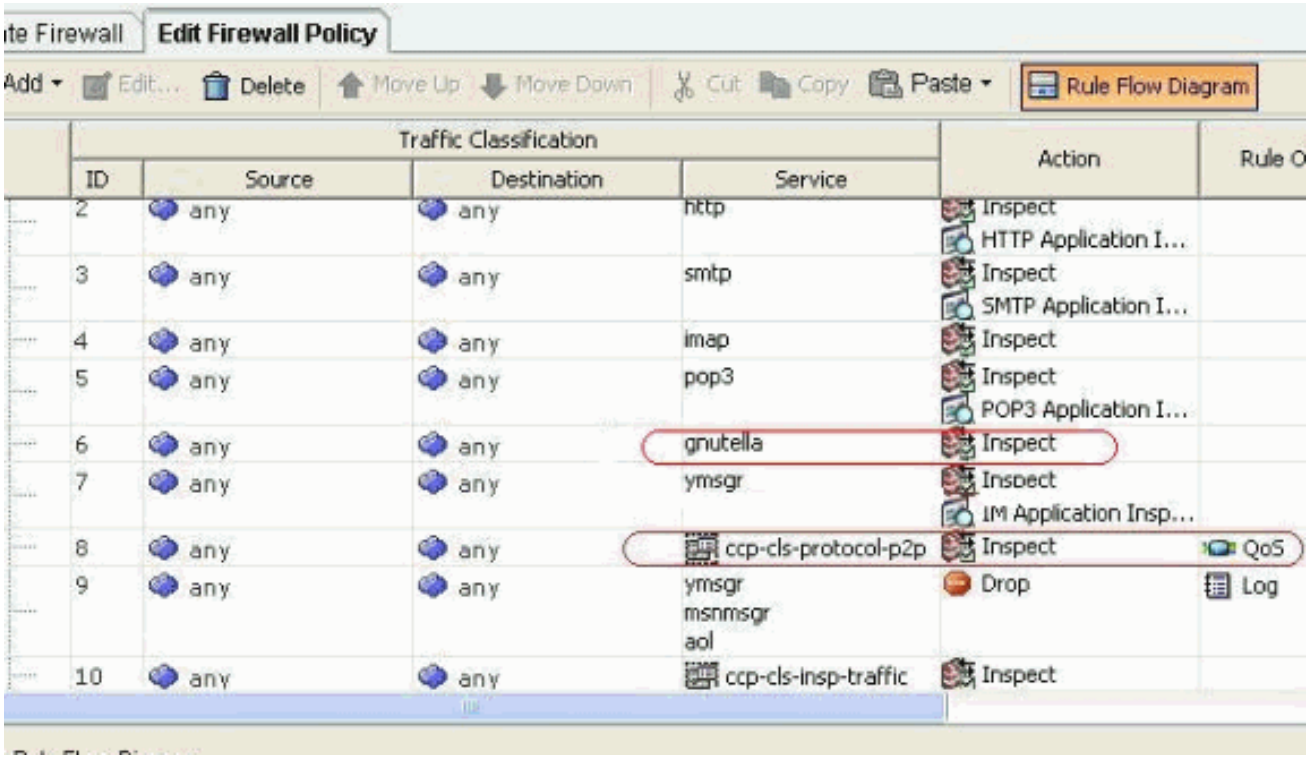
21. [OK] をクリックして、高度な検査の設定を完了します。



対応するコマンド セットがルータに送られます。

22. [OK] をクリックして、ルータへのコマンド セットのコピーを完了します。

23. [Configure] > [Security] > [Firewall and ACL] の [Edit Firewall Policy] タブから、新しいルールが実行されているのを確認できます。



ZFW ルータのコマンドライン設定

前のセクションで Cisco CP から行った設定により、ZFW ルータに次の設定が行われています。

ZBF ルータ
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#
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- ZBF-Router#**show policy-map type inspect zone-pair sessions**：既存のすべてのゾーン ペアのランタイム inspect タイプのポリシー マップ統計情報を表示します。

関連情報

- ゾーンベース ポリシー ファイアウォールの設計と適用ガイド
- Cisco IOS Firewall Classic とゾーンベースの仮想ファイアウォール アプリケーションの設定例
- Cisco Configuration Professional の [Home] ページ