Cisco CP - Configurer ZFW pour bloquer le trafic homologue à homologue

Contenu

Introduction
Conditions préalables
Conditions requises
Configuration du routeur pour exécuter Cisco CP
Components Used
Conventions
Informations générales
Configuration
Diagramme du réseau
Configuration via Cisco Configuration Professional
Configuration en ligne de commande du routeur ZFW
Vérification
Informations connexes

Introduction

Ce document fournit une approche pas à pas pour configurer un routeur Cisco IOS en tant que pare-feu basé sur une zone pour bloquer le trafic P2P (Peer-to-Peer) à l'aide de l'assistant de configuration Advanced Firewall dans Cisco Configuration Professional (Cisco CP).

Le pare-feu de la politique selon les zones (également connu sous le nom de pare-feu de zone politique ou ZFW) change la configuration du pare-feu de l'ancien modèle basé sur l'interface pour un modèle plus souple et plus facilement compréhensible basé sur des zones. Des interfaces sont affectées aux zones et la politique d'inspection est appliquée au trafic qui se déplace entre les zones. Les politiques interzones offrent une flexibilité et une granularité considérables. Par conséquent, différentes stratégies d'inspection peuvent être appliquées à plusieurs groupes d'hôtes connectés à la même interface de routeur. Les zones établissent les frontières de sécurité de votre réseau. Une zone définit une borne où le trafic est soumis aux restrictions politiques à mesure qu'elle se dirige vers une autre region de votre réseau. La politique par défaut de ZFW entre les zones est tout refuser. Si aucune politique n'est explicitement configurée, tout le trafic qui se déplace entre les zones est bloqué.

Les applications P2P sont parmi les applications les plus utilisées sur Internet. Les réseaux P2P peuvent servir de conduits pour les menaces malveillantes telles que les vers, offrir un chemin facile autour des pare-feu et susciter des préoccupations en matière de confidentialité et de sécurité. La version 12.4(9)T du logiciel Cisco IOS a introduit la prise en charge de ZFW pour les applications P2P. L'inspection P2P offre des politiques de couches 4 et 7 pour le trafic d'applications. Cela signifie que ZFW peut fournir une inspection dynamique de base pour autoriser ou refuser le trafic, ainsi qu'un contrôle granulaire de couche 7 sur des activités

spécifiques dans les différents protocoles, de sorte que certaines activités d'application soient autorisées alors que d'autres sont refusées.

Cisco CP propose une approche étape par étape et simple à suivre pour configurer le routeur IOS en tant que pare-feu basé sur une zone à l'aide de l'assistant de configuration Advanced Firewall.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- La version du logiciel du routeur IOS doit être 12.4(9)T ou ultérieure.
- Pour les modèles de routeur IOS qui prennent en charge Cisco CP, reportez-vous aux notes de version de Cisco CP.

Configuration du routeur pour exécuter Cisco CP

Remarque : Procédez comme suit pour exécuter Cisco CP sur un routeur Cisco :

```
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
```

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur Cisco 1841 IOS qui exécute le logiciel IOS Version 12.4(15)T
- Cisco Configuration Professional (Cisco CP) version 2.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Dans l'exemple de ce document, le routeur est configuré comme un pare-feu basé sur une zone

pour bloquer le trafic P2P. Le routeur ZFW comporte deux interfaces, une interface interne (approuvée) dans la zone d'entrée et une interface externe (non approuvée) dans la zone de sortie. Le routeur ZFW bloque les applications P2P telles que edonkey, fasttrack, gnutella et kazaa2 avec une action de journalisation pour le trafic qui passe de la zone d'entrée à la zone de sortie.

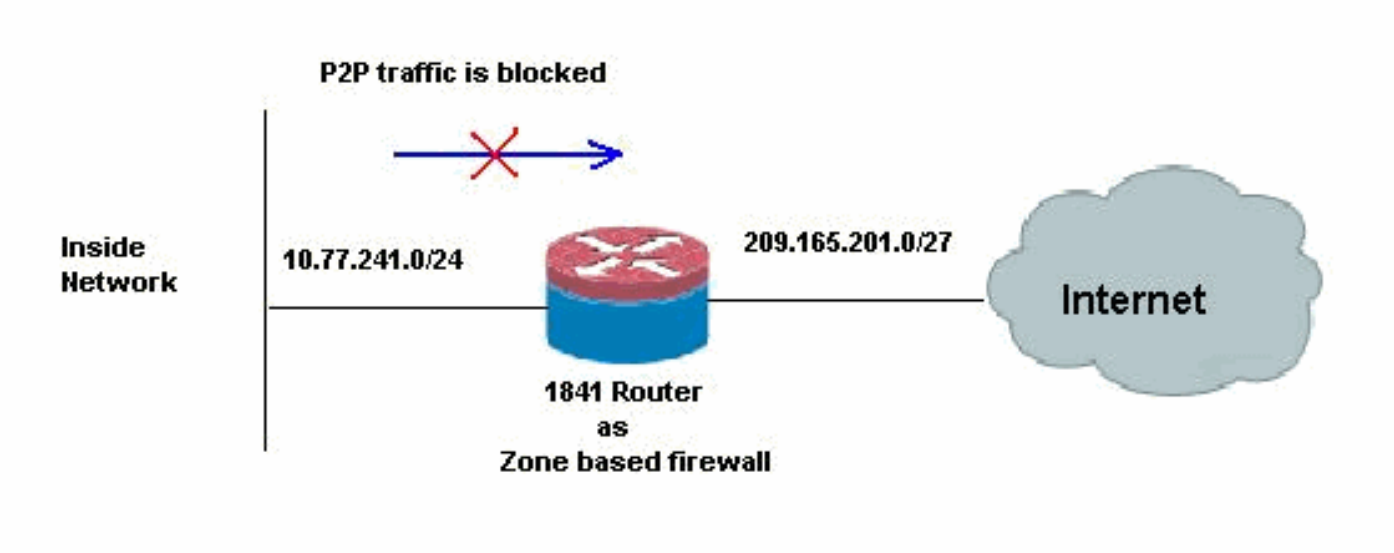
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

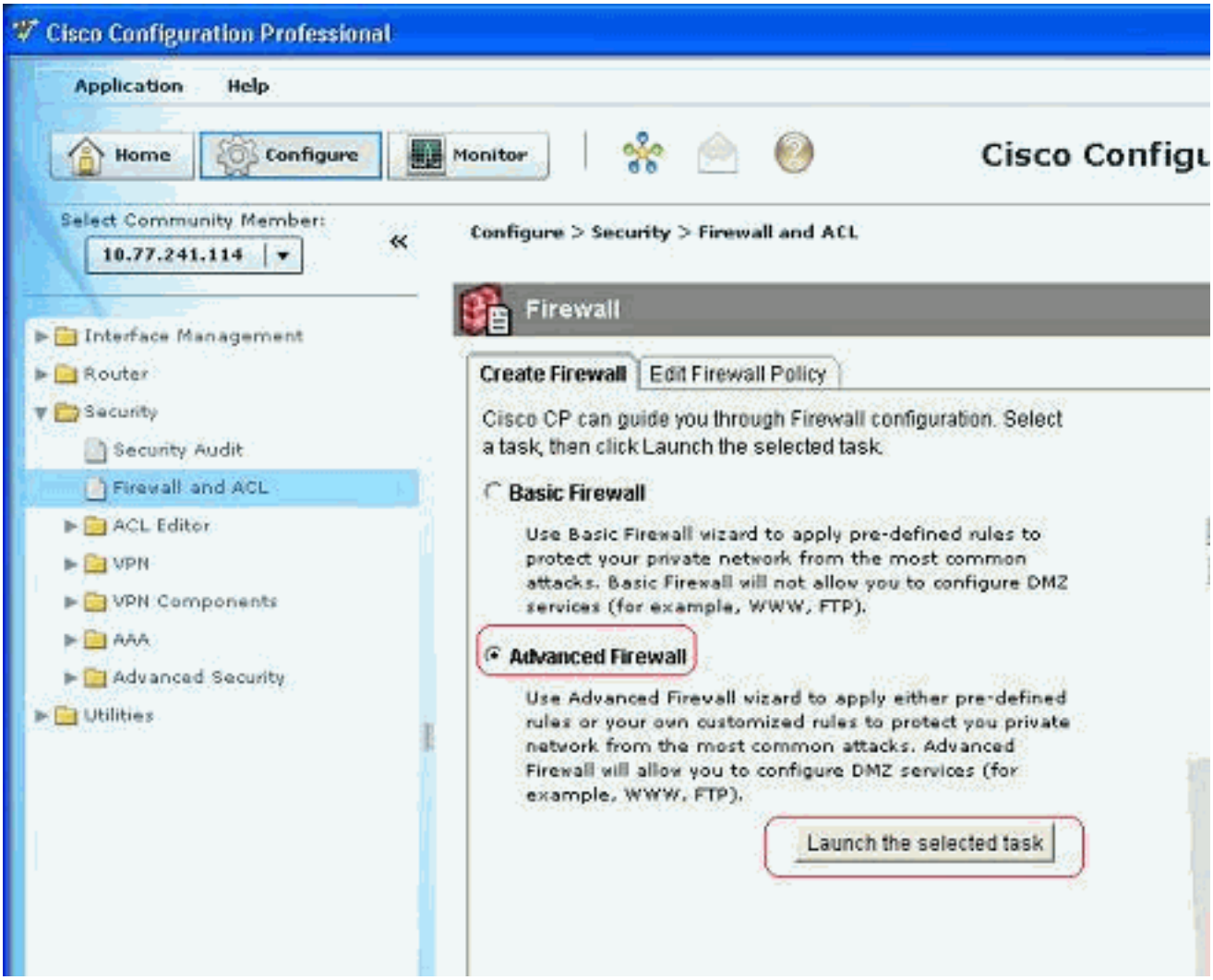


Configuration via Cisco Configuration Professional

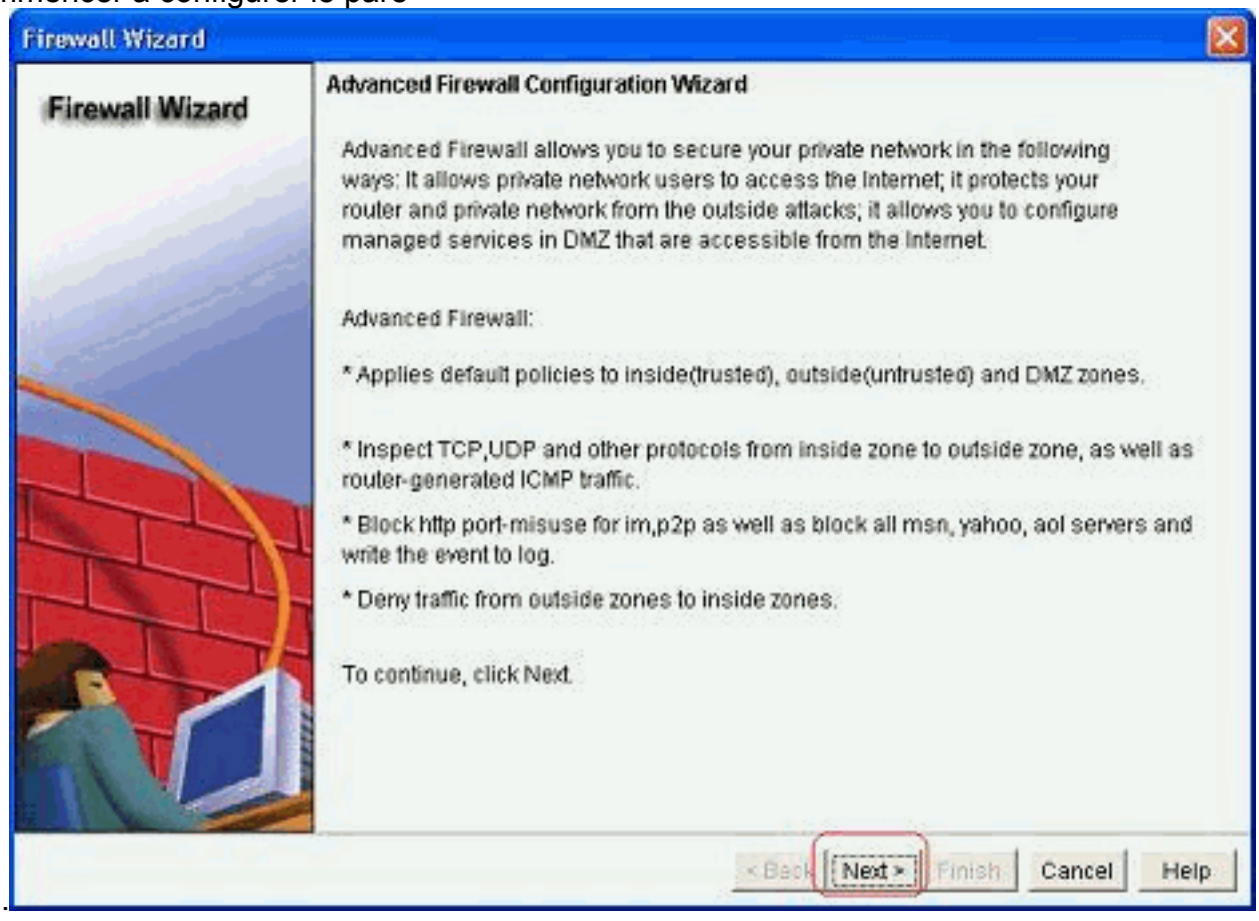
Cette section contient la procédure pas à pas pour utiliser l'assistant de configuration du routeur IOS en tant que pare-feu basé sur une zone.

Procédez comme suit :

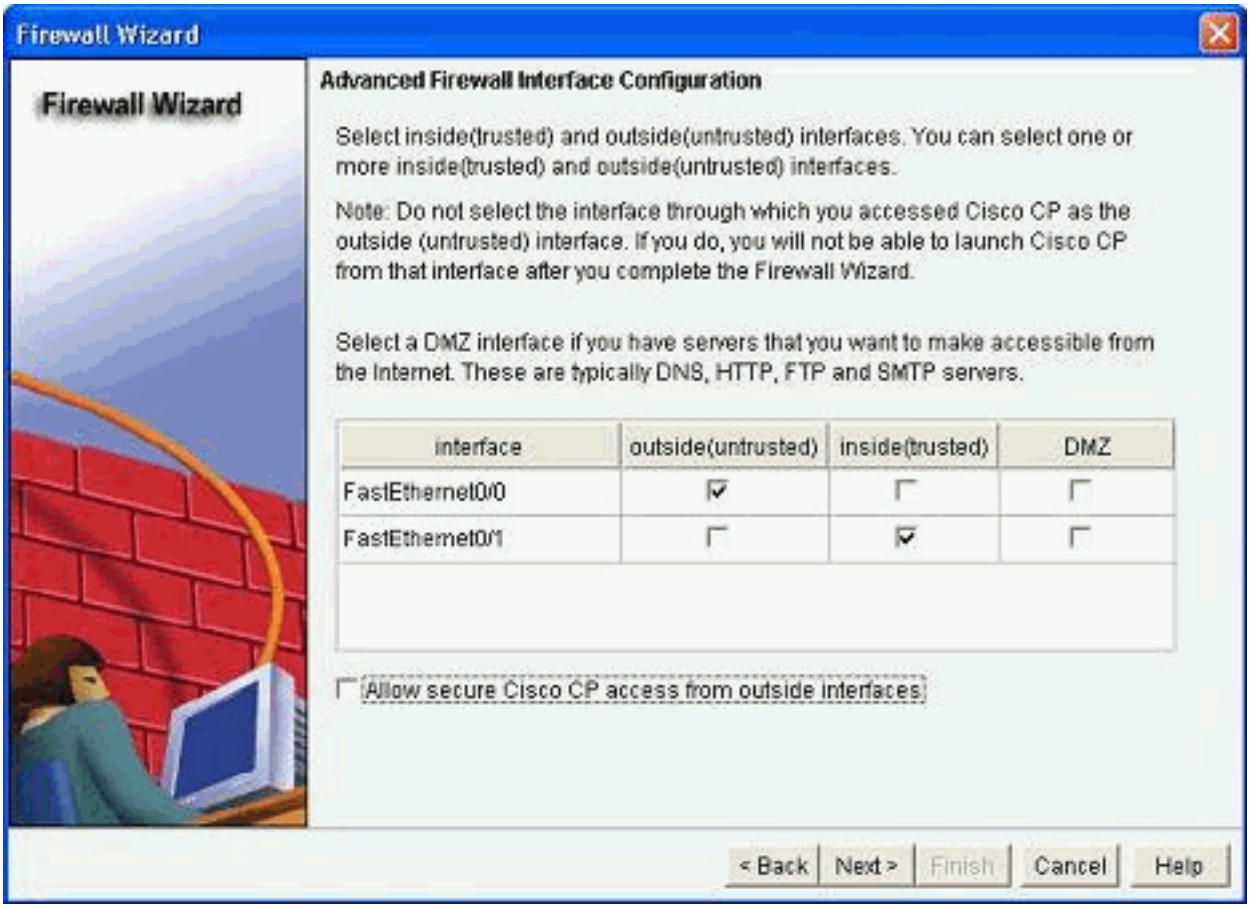
1. Accédez à **Configure > Security > Firewall and ACL**. Sélectionnez ensuite la case d'option **Advanced Firewall**. Cliquez sur **Lancer la tâche sélectionnée**.



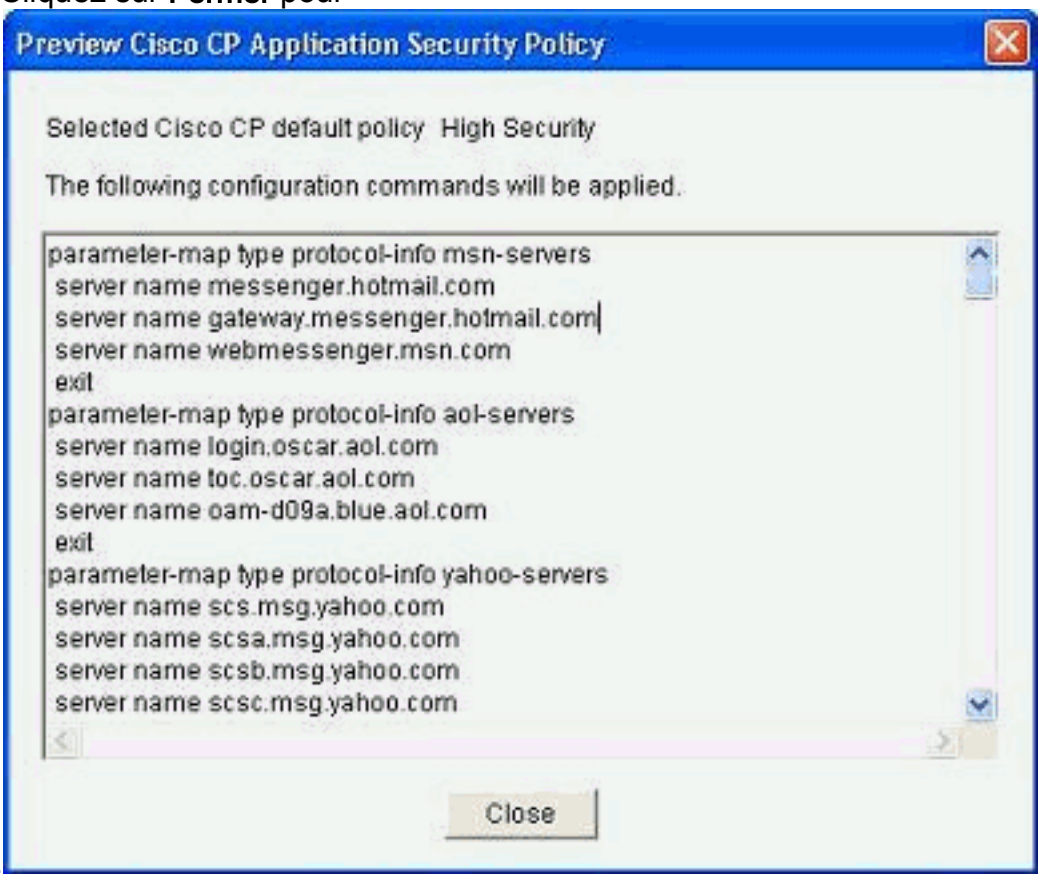
2. L'écran suivant présente brièvement l'Assistant Pare-feu. Cliquez sur **Suivant** pour commencer à configurer le pare-feu.



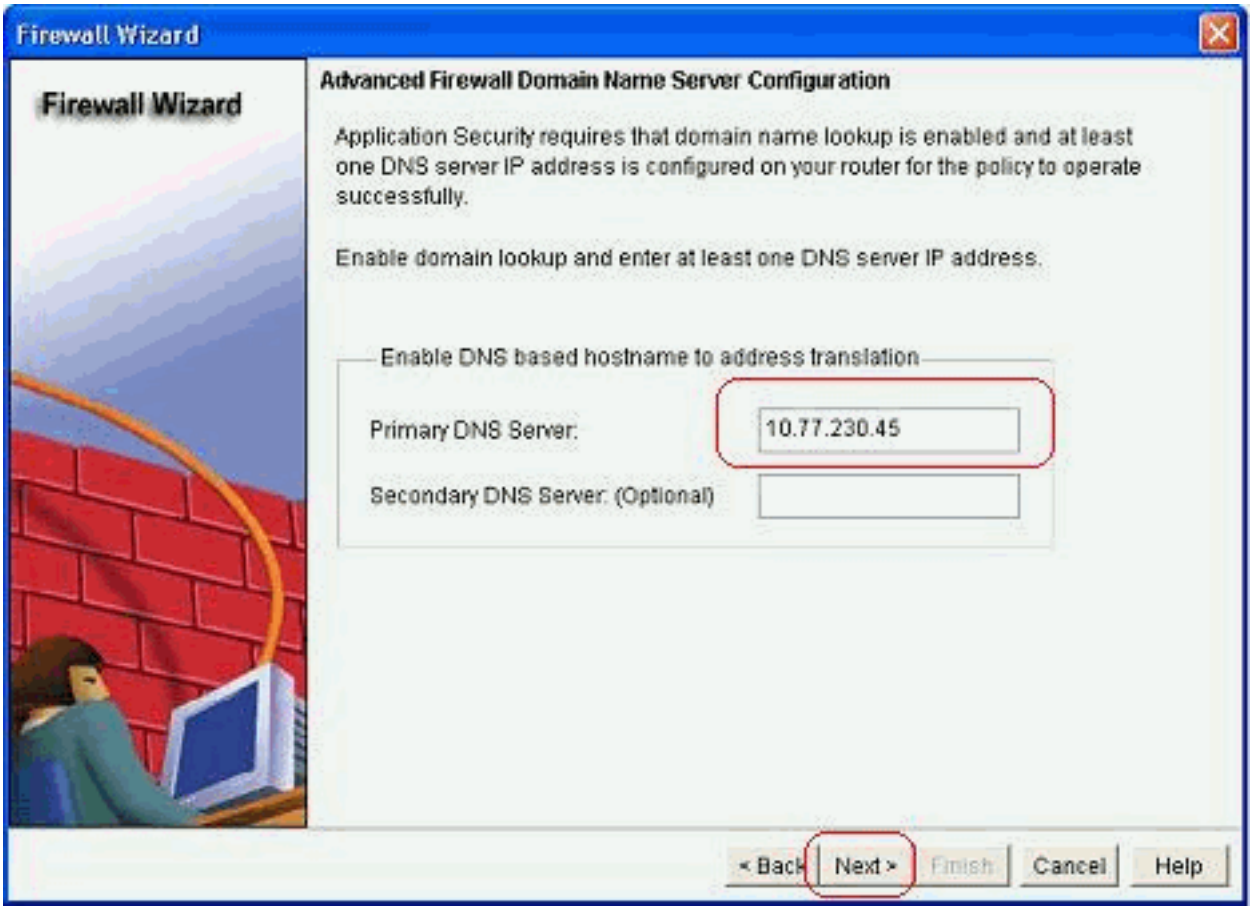
3. Sélectionnez les interfaces du routeur à inclure dans les zones et cliquez sur **Suivant**.



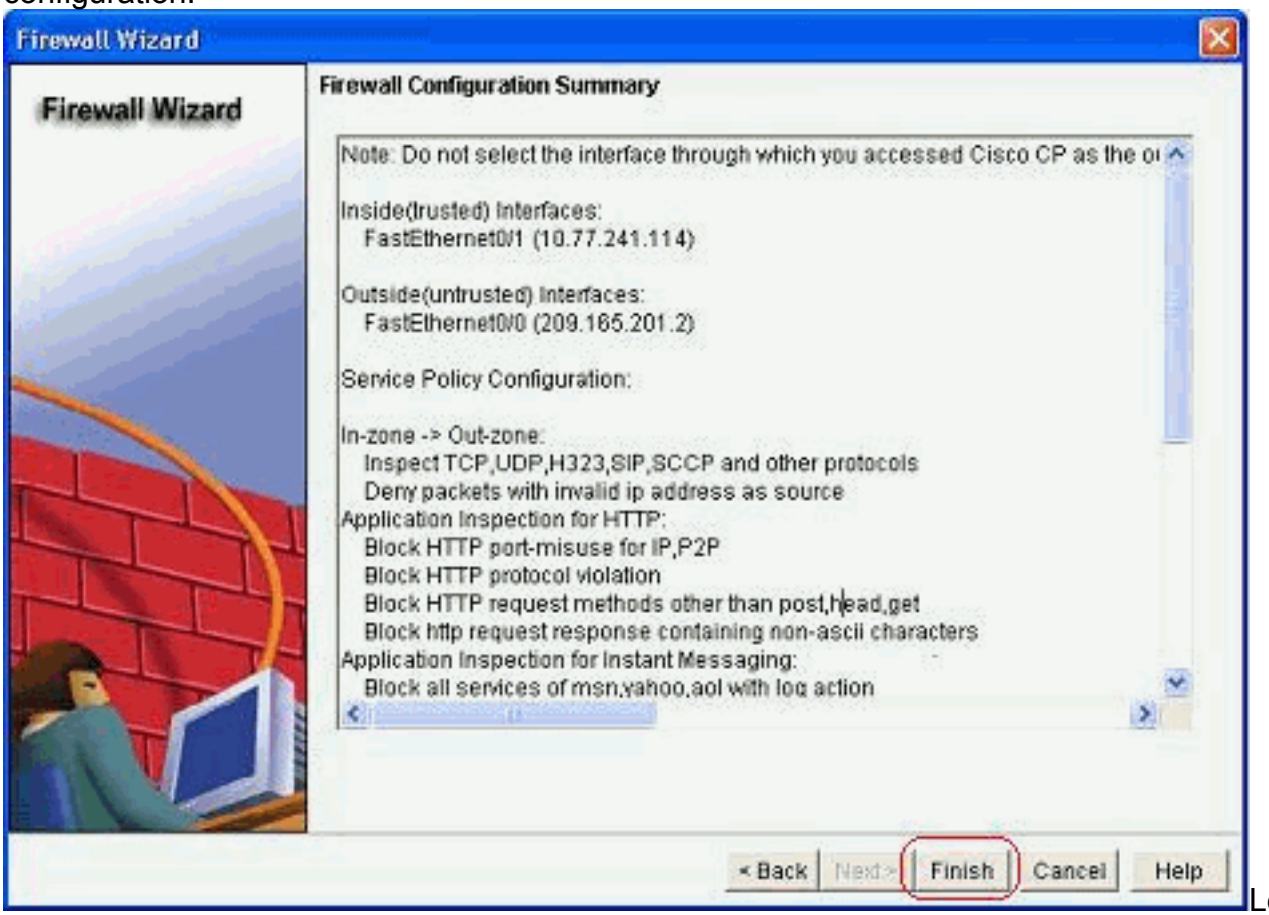
4. La stratégie par défaut avec haute sécurité et le jeu de commandes s'affiche dans la fenêtre suivante. Cliquez sur **Fermer** pour continuer.



5. Entrez les détails du serveur DNS et cliquez sur **Suivant**.

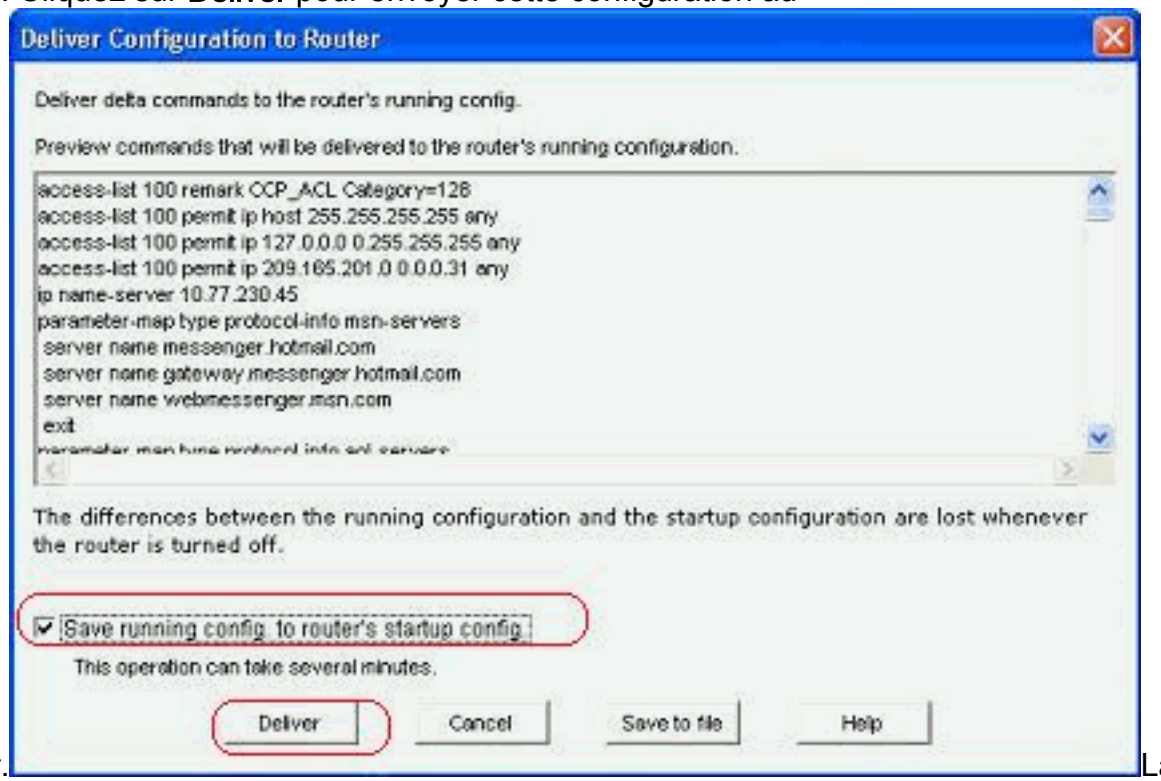


6. Cisco CP fournit un résumé de configuration tel que celui présenté ici. Cliquez sur **Terminer** pour terminer la configuration.

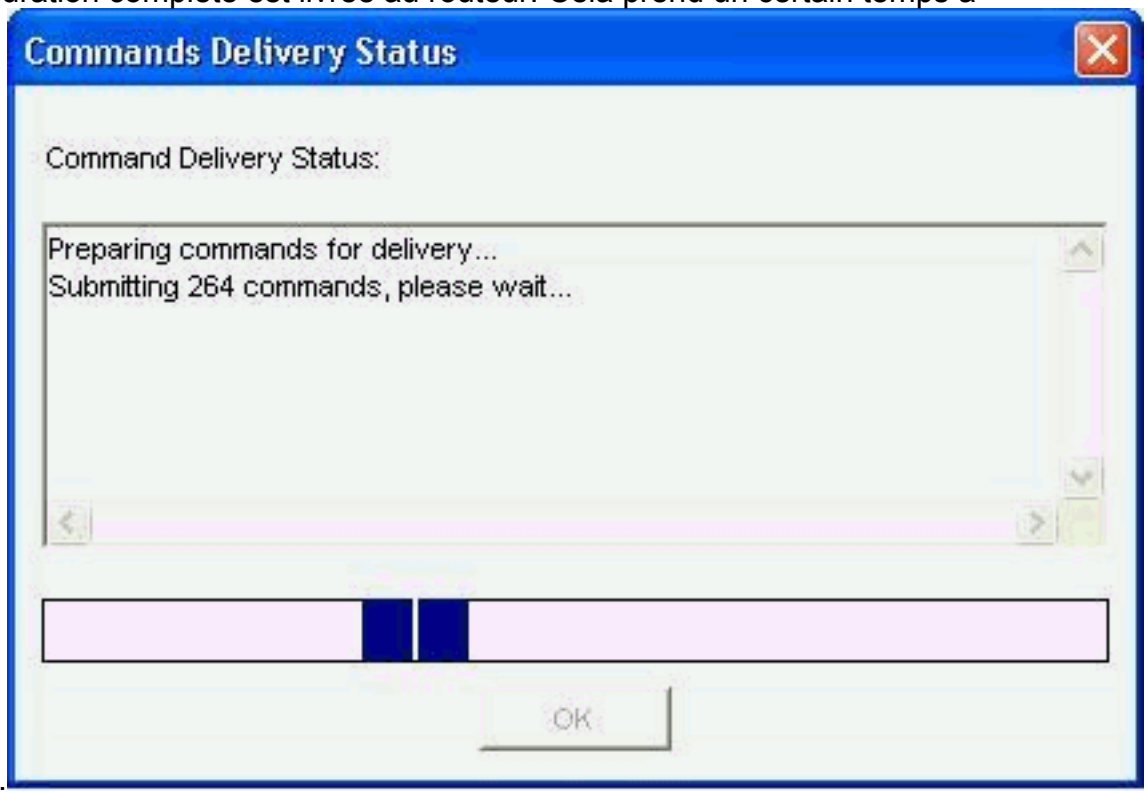


Le résumé détaillé de la configuration est fourni dans ce tableau. Il s'agit de la configuration par défaut conformément à la politique de sécurité élevée de Cisco CP.

7. Cochez la case **Enregistrer la configuration en cours dans la configuration de démarrage du routeur**. Cliquez sur **Deliver** pour envoyer cette configuration au routeur.



La configuration complète est livrée au routeur. Cela prend un certain temps à traiter.



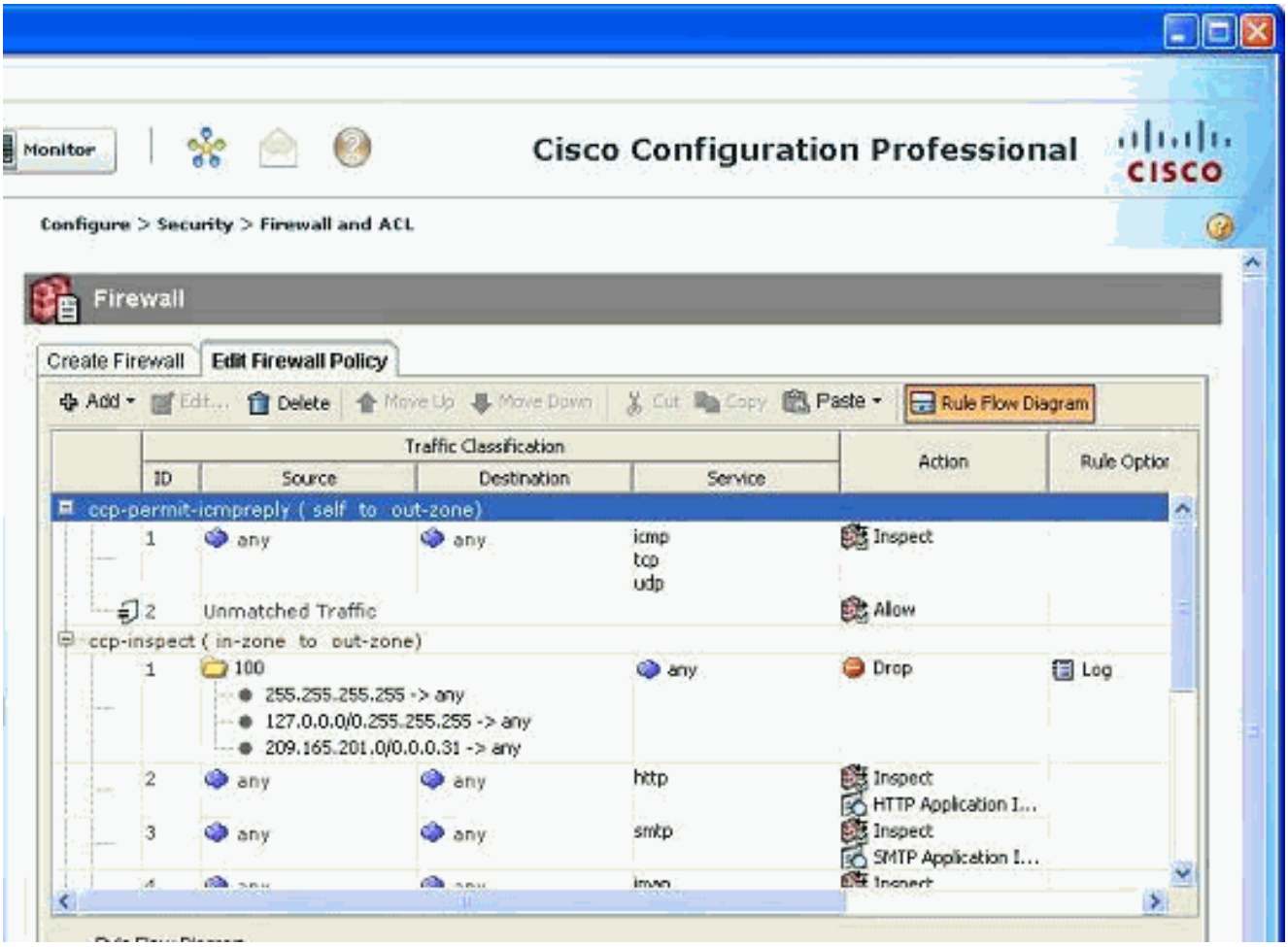
8. Cliquez sur **OK** pour

continuer.

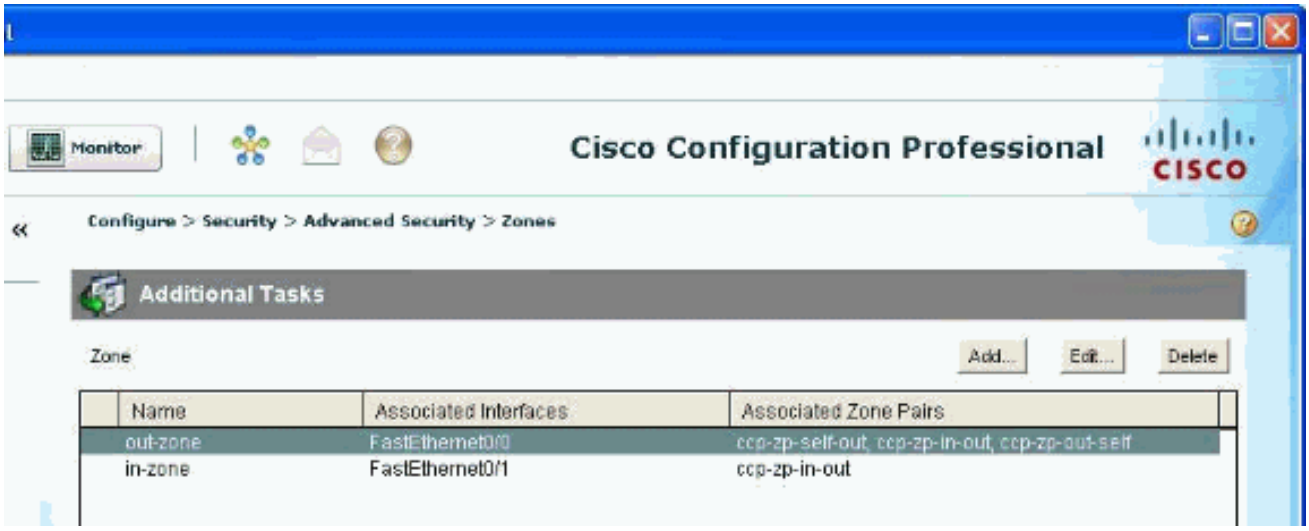
9. Cliquez à nouveau sur



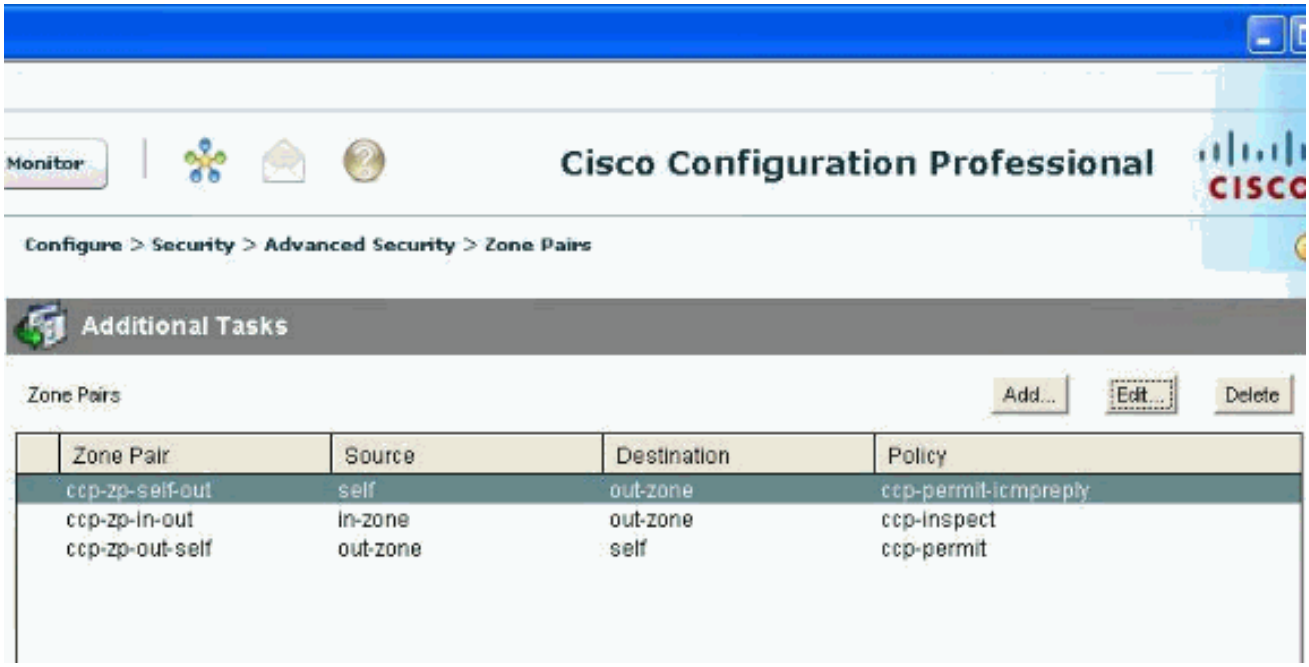
OK. La configuration est maintenant en vigueur et s'affiche sous l'onglet Stratégie de pare-feu.



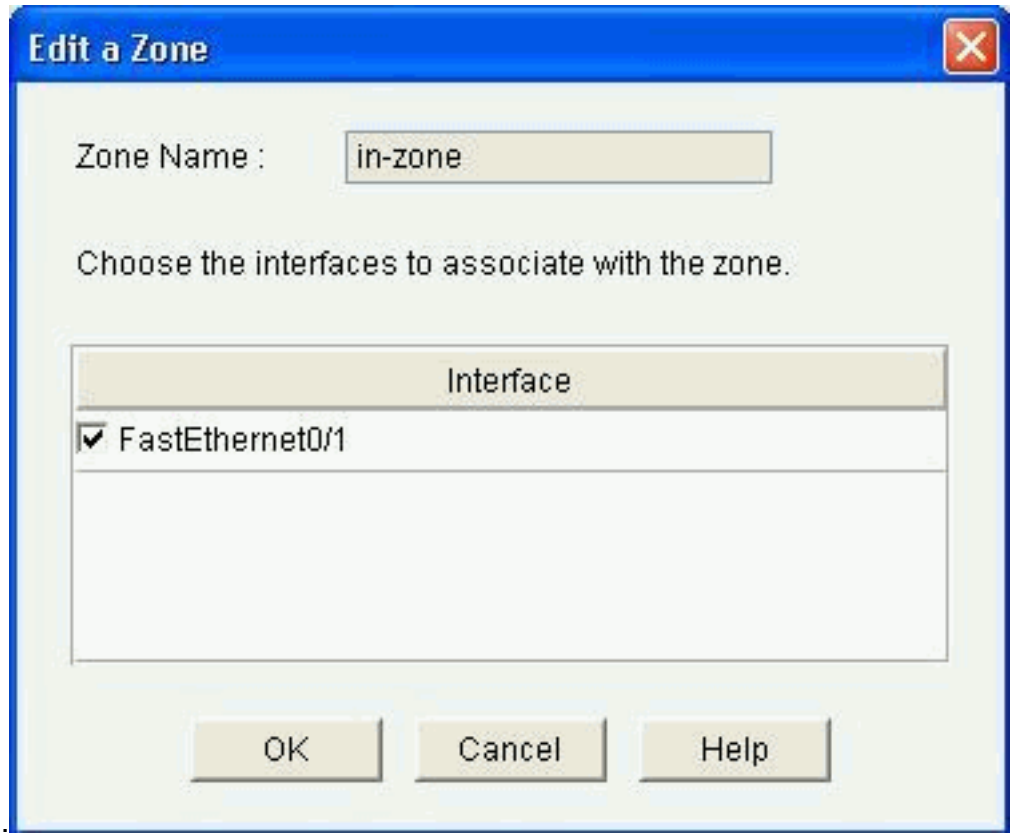
10. Les zones ainsi que les paires de zones qu'elles sont associées peuvent être affichées si vous accédez à **Configurer > Sécurité > Sécurité avancée > Zones**. Vous pouvez également ajouter de nouvelles zones en cliquant sur **Ajouter**, ou modifier les zones existantes en cliquant sur **Modifier**.



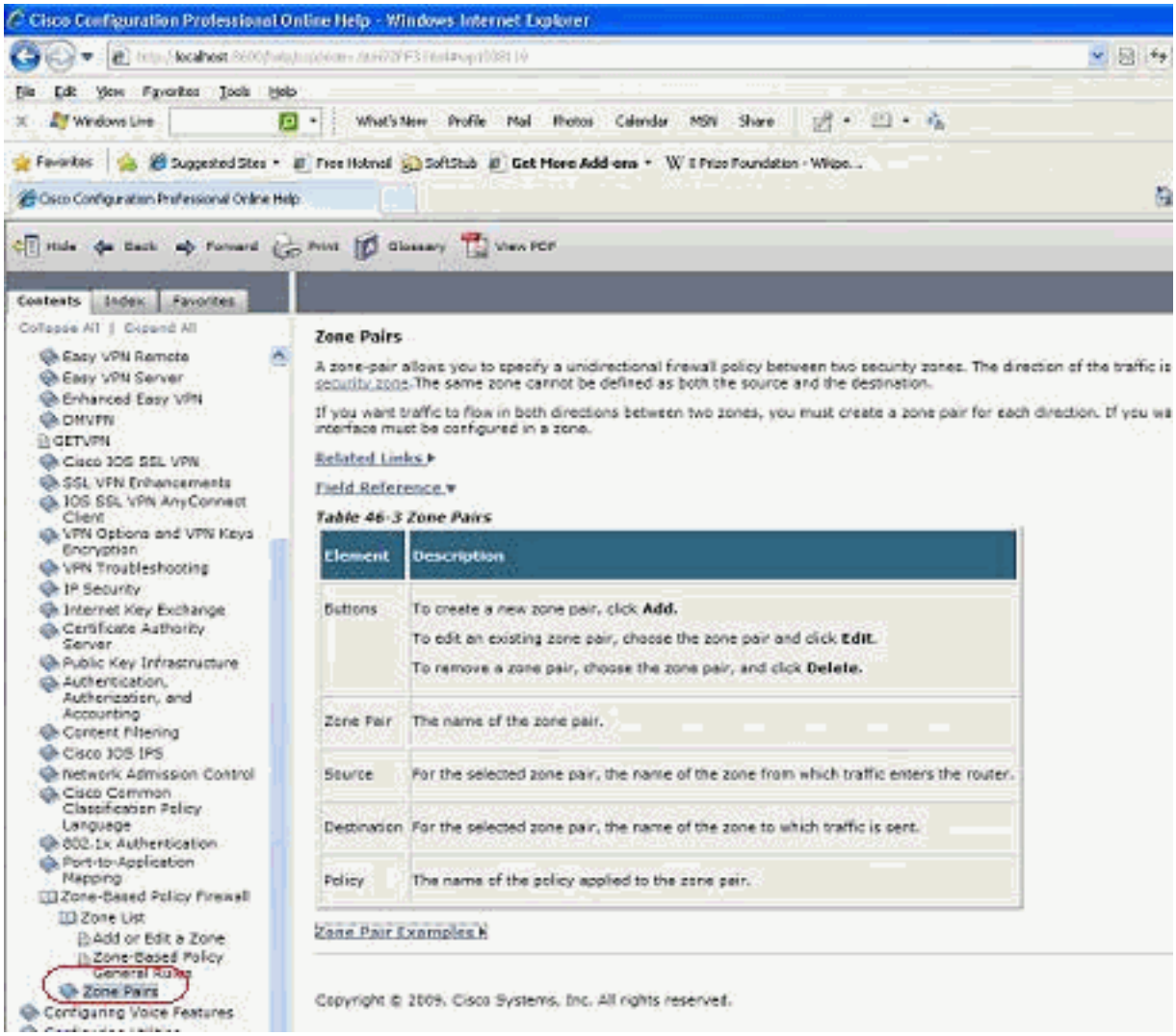
11. Accédez à **Configurer > Sécurité > Sécurité avancée > Paires de zones** pour afficher les détails des paires de zones.



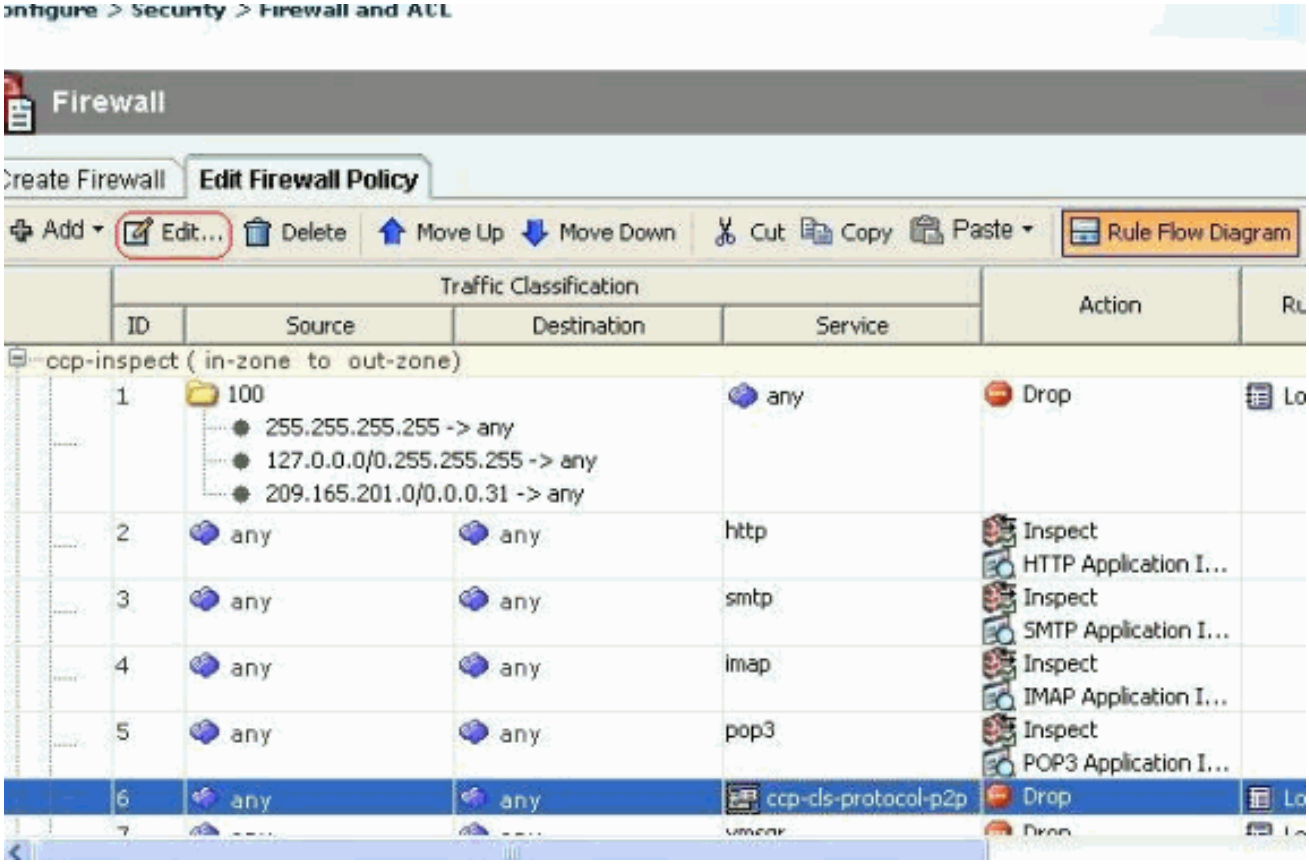
Une aide instantanée sur la façon de modifier/ajouter/supprimer des zones/paires de zones et d'autres informations connexes est facilement disponible avec les pages Web intégrées dans Cisco



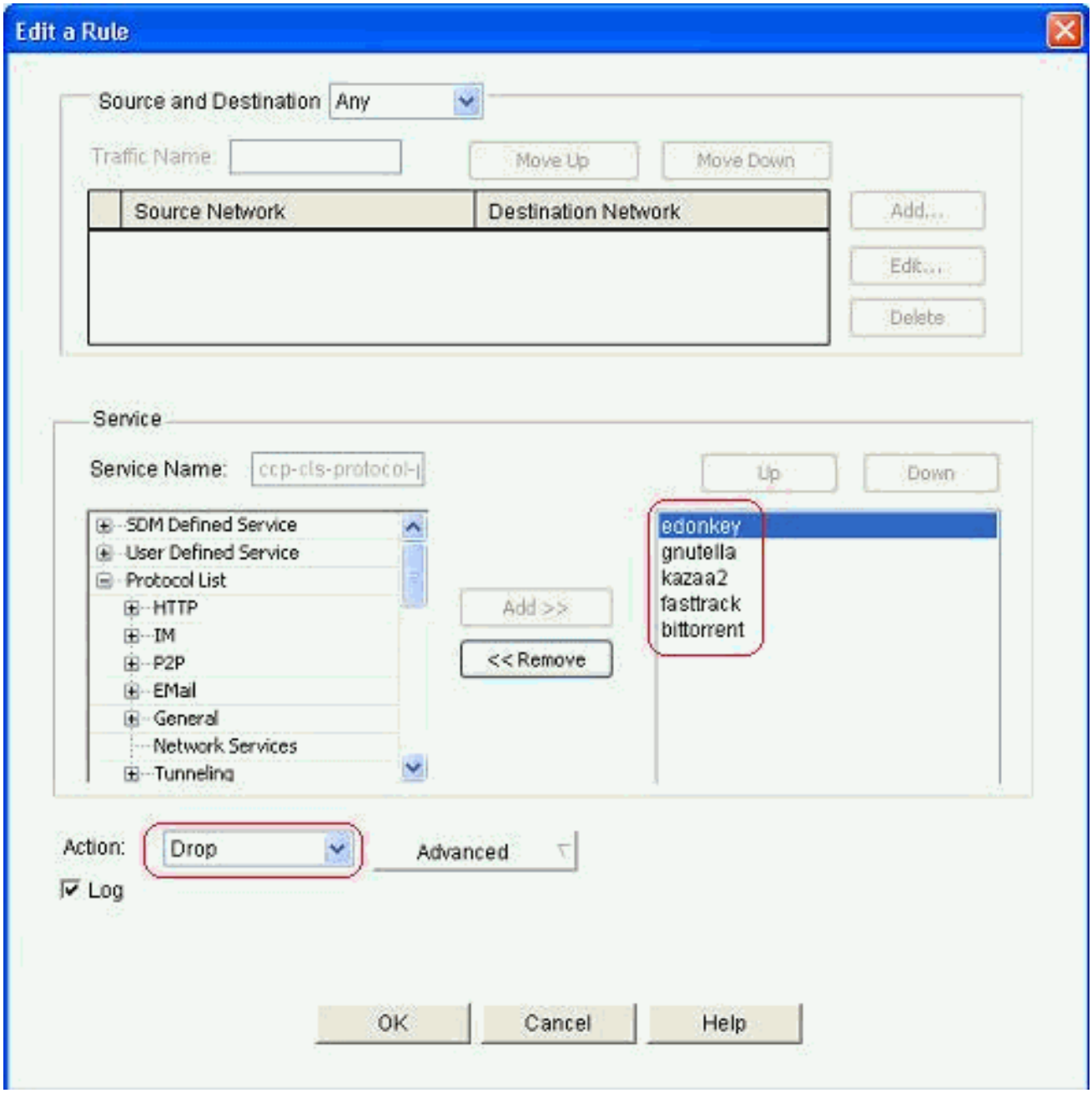
CP.



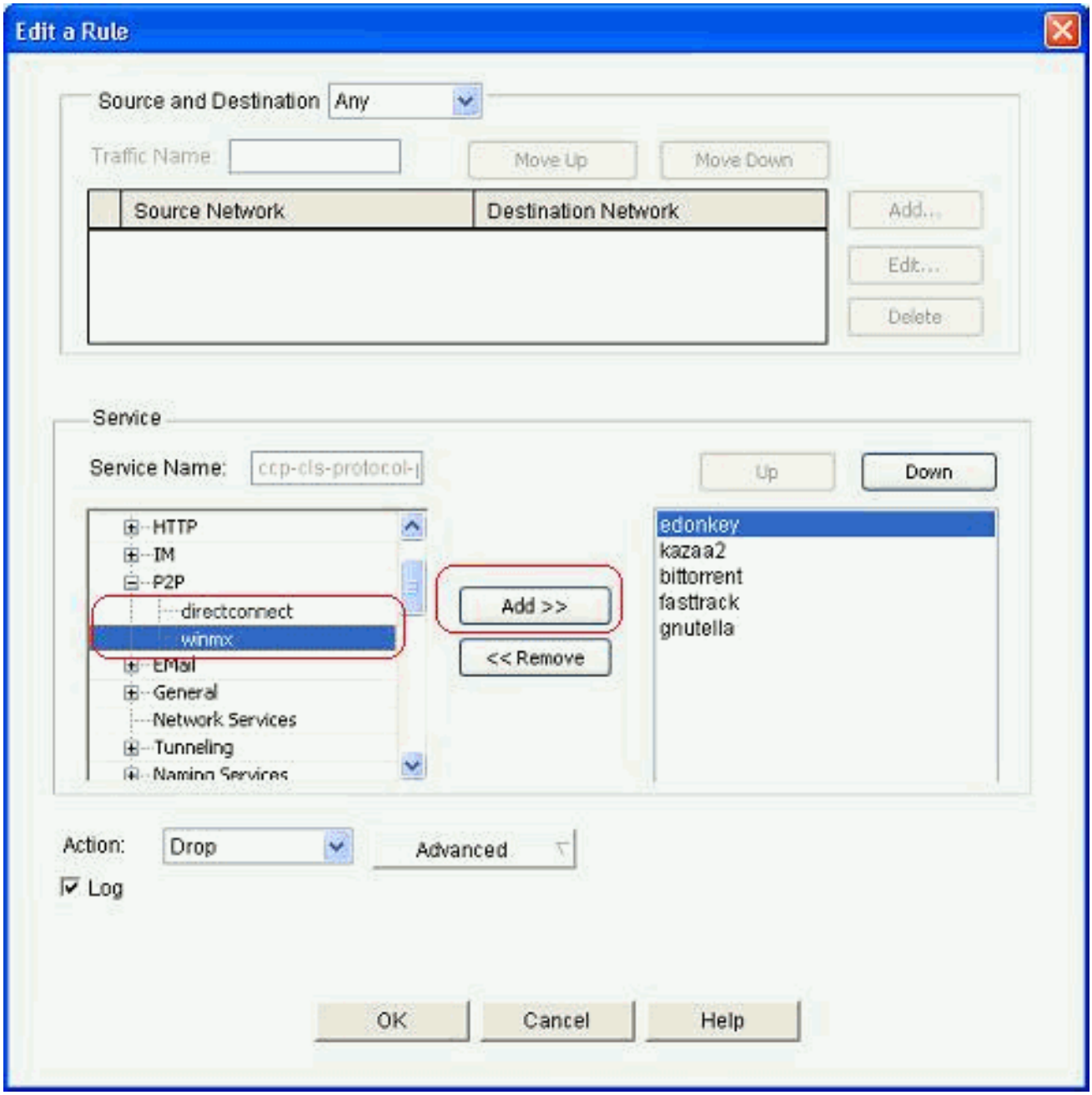
12. Afin de modifier les fonctionnalités d'inspection spécifiques aux applications pour certaines applications P2P, accédez à **Configuration > Security > Firewall and ACL**. Ensuite, cliquez sur **Modifier la stratégie de pare-feu** et choisissez la règle correspondante dans le mappage de stratégie. Cliquez sur
Edit.

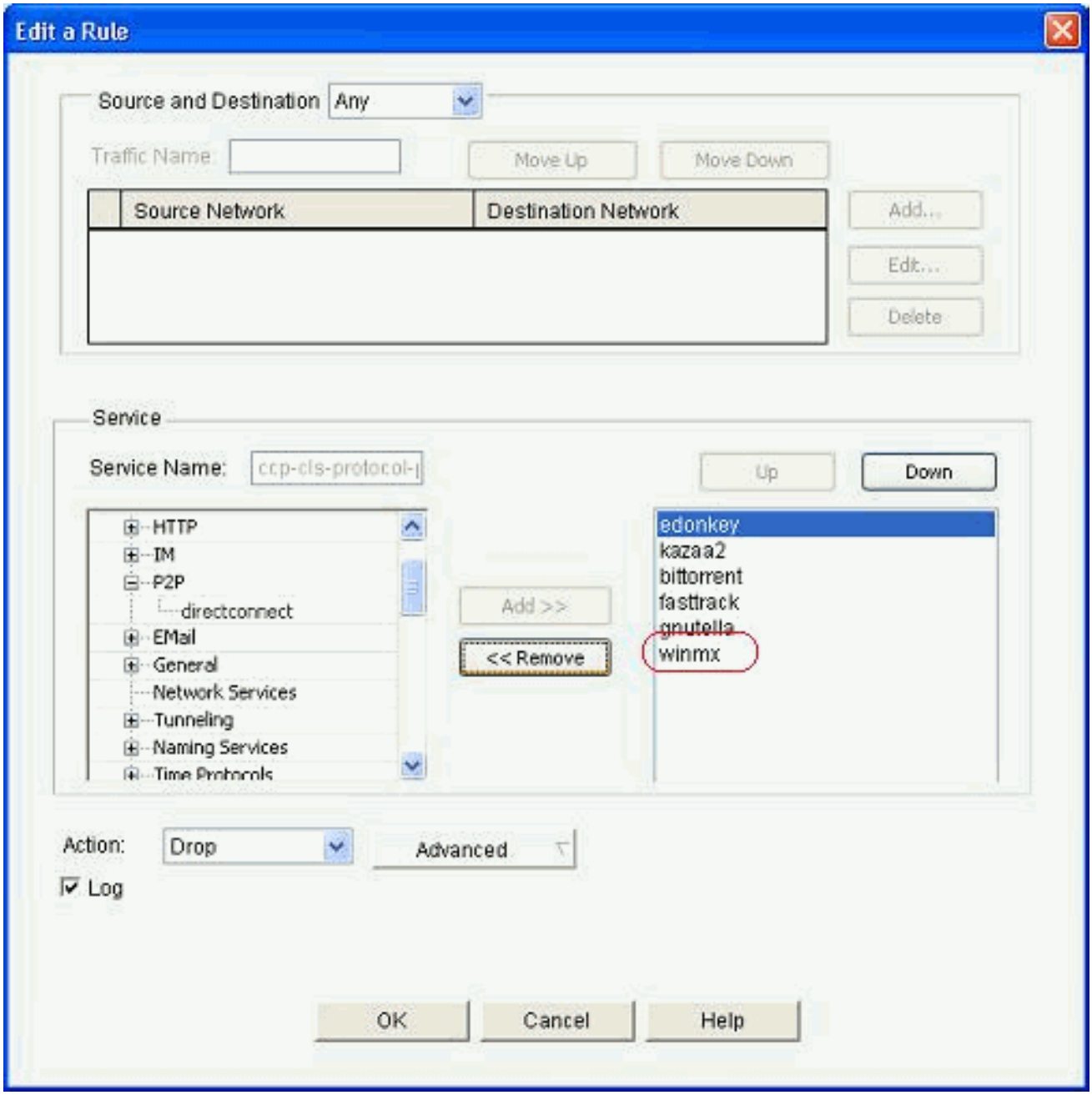


Affiche les applications P2P actuelles qui seront bloquées par la configuration par défaut.

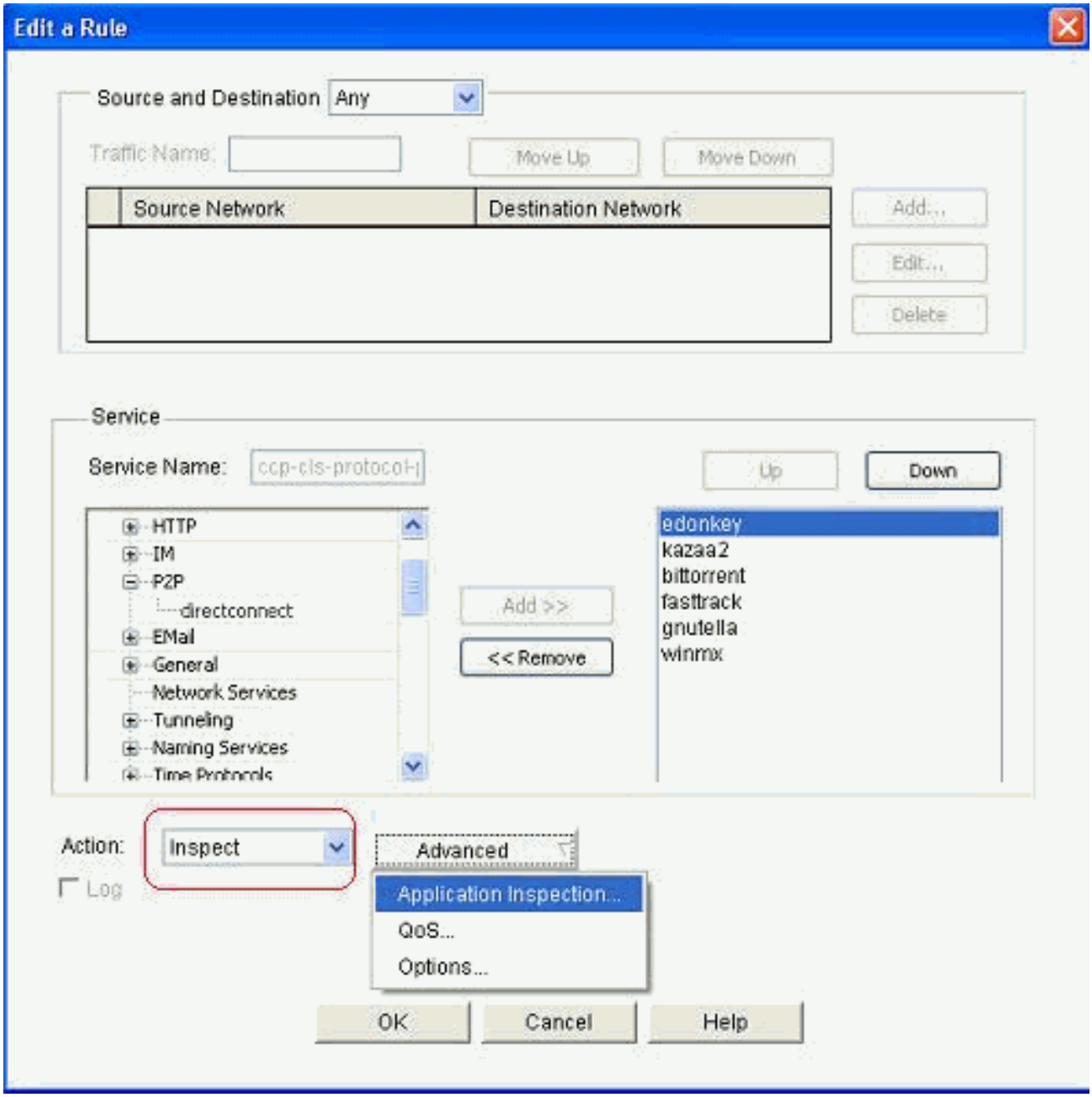


13. Vous pouvez utiliser les boutons Ajouter et Supprimer pour ajouter/supprimer des applications spécifiques. Cette capture d'écran montre comment ajouter l'application winmx pour bloquer
cela.


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

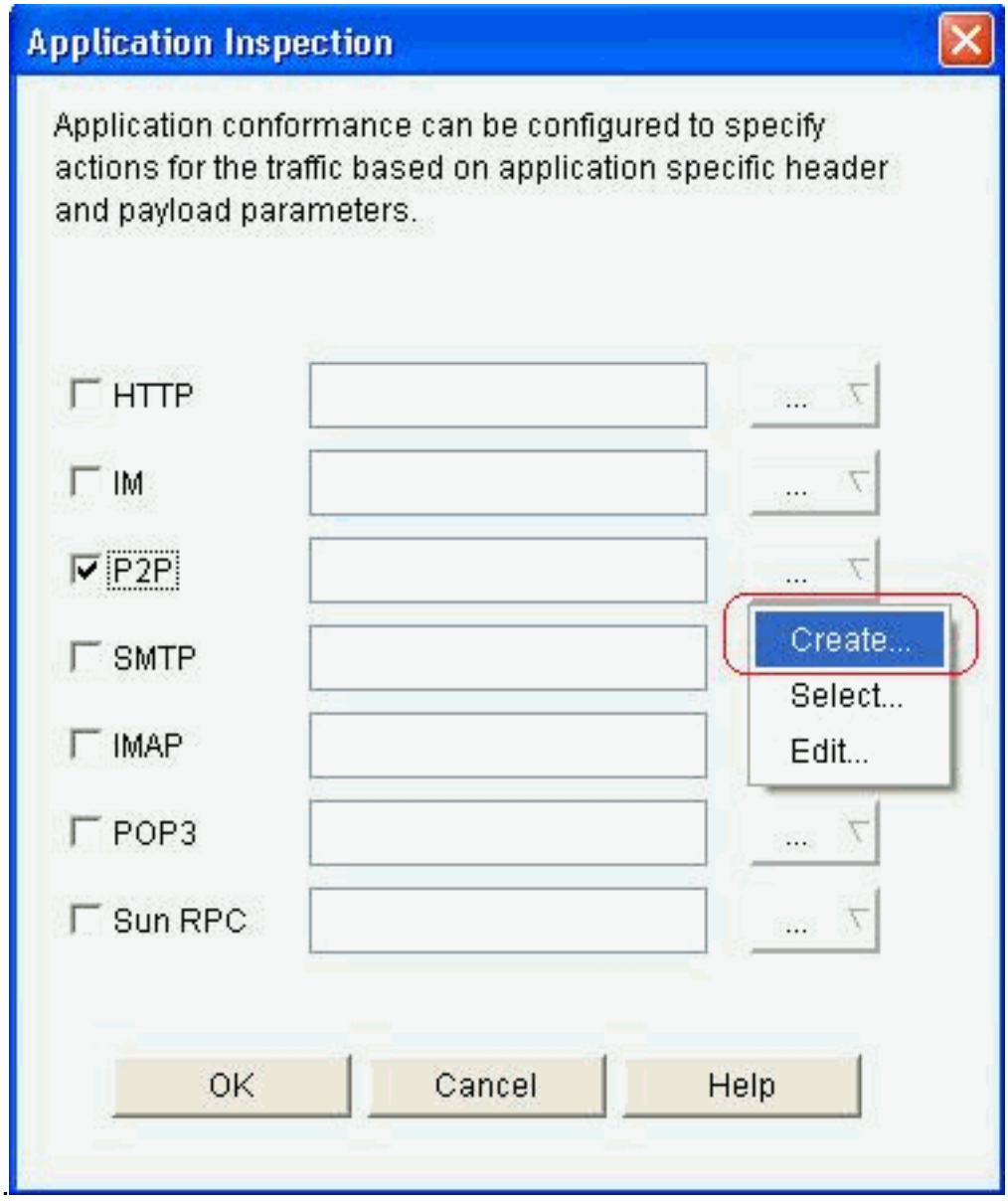


14. Au lieu de choisir l'action de suppression, vous pouvez également choisir l'action Inspect pour appliquer différentes options pour l'inspection approfondie des paquets.



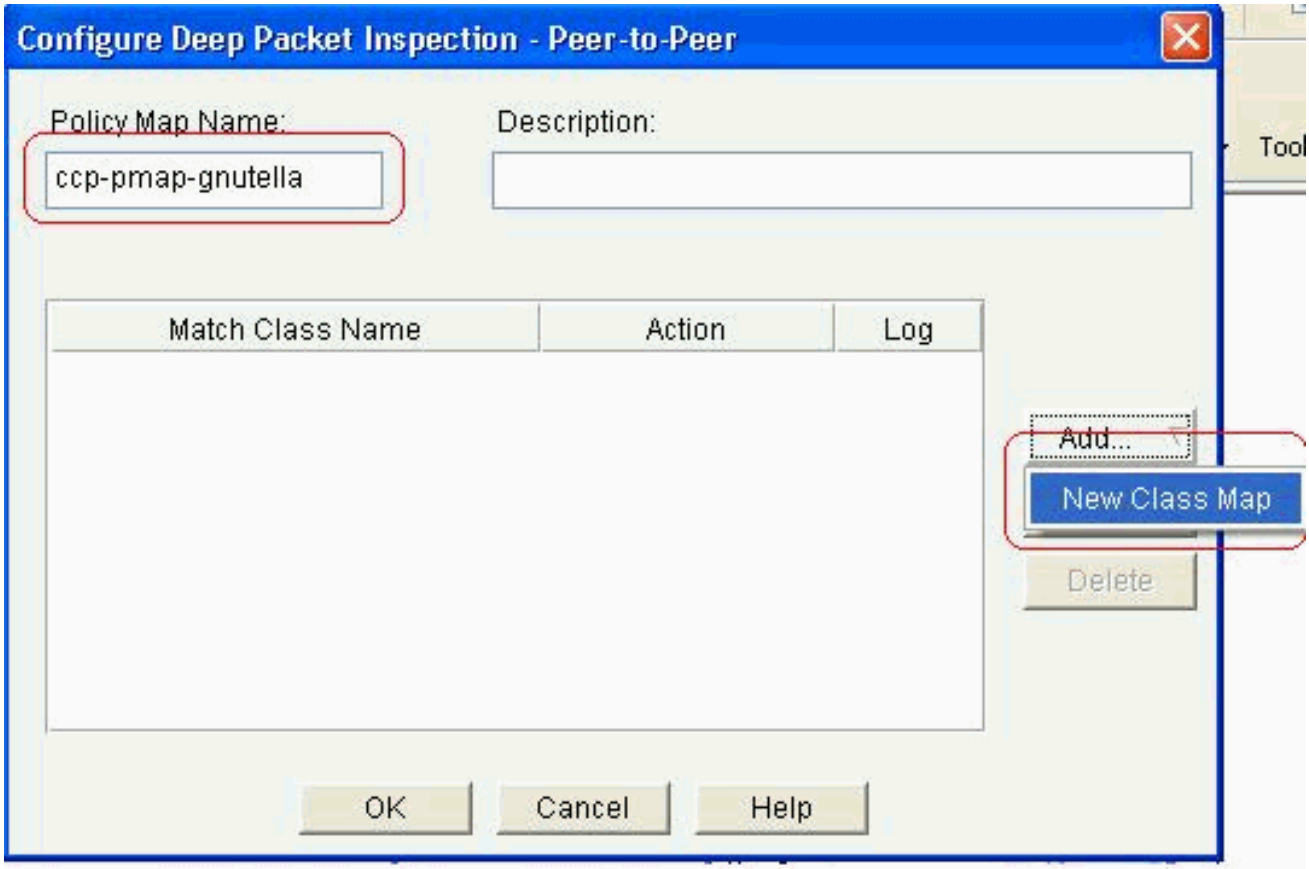
L'inspection P2P offre des politiques de couches 4 et 7 pour le trafic d'applications. Cela signifie que ZFW peut fournir une inspection dynamique de base pour autoriser ou refuser le trafic, ainsi qu'un contrôle granulaire de couche 7 sur des activités spécifiques dans les différents protocoles, de sorte que certaines activités d'application soient autorisées alors que d'autres sont refusées. Dans cette inspection d'application, vous pouvez appliquer différents types d'inspections spécifiques au niveau de l'en-tête pour les applications P2P. Un exemple de gnutella est présenté ci-après.

15. Cochez l'option **P2P** et cliquez sur **Créer** afin de créer une nouvelle carte de stratégie pour

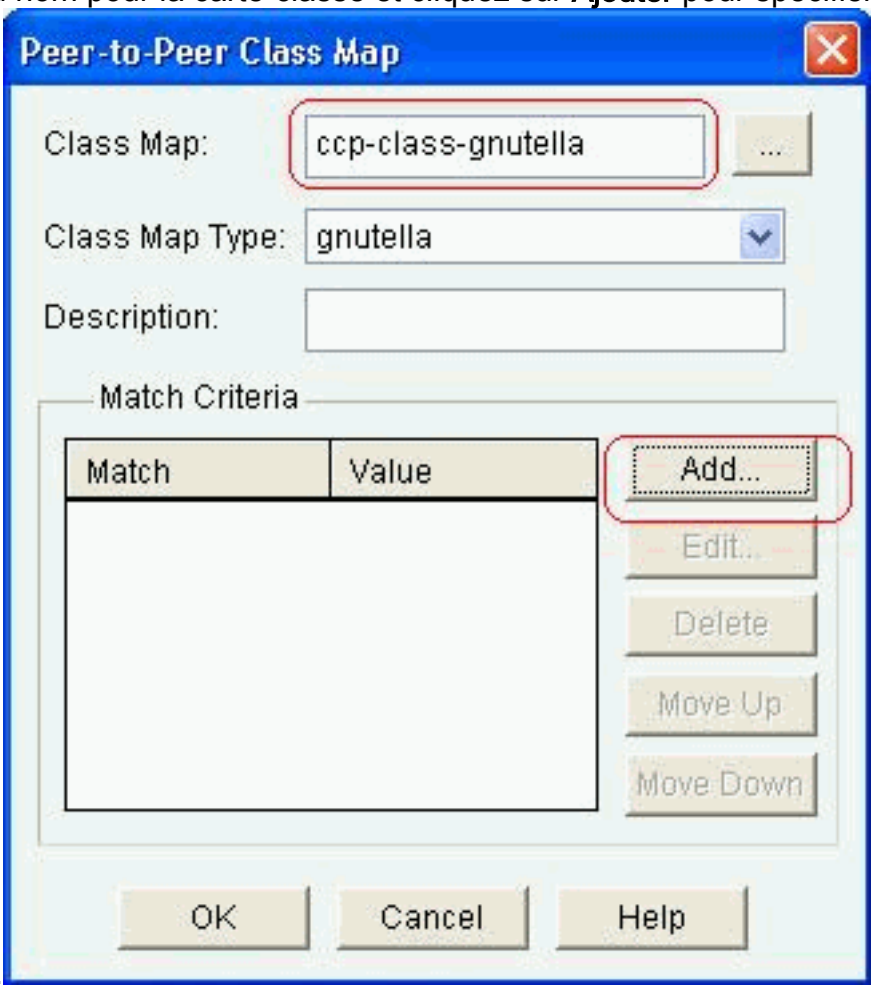


cela.

16. Créez une nouvelle carte de stratégie pour l'inspection approfondie des paquets pour le protocole gnutella. Cliquez sur **Ajouter**, puis sélectionnez **Nouveau mappage de classe**.



17. Donnez un nouveau nom pour la carte-classe et cliquez sur **Ajouter** pour spécifier un critère de correspondance.

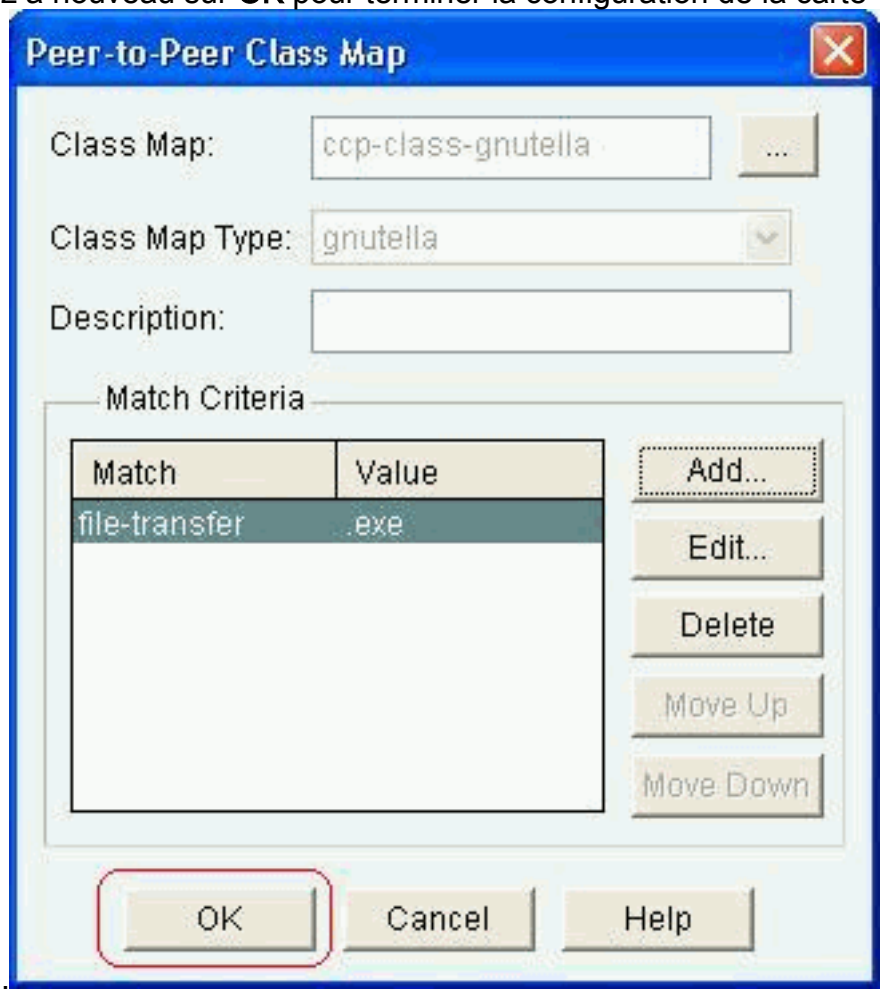


18. Utilisez file-transfer comme critère de correspondance et la chaîne utilisée est .exe. Cela indique que toutes les connexions de transfert de fichiers gnutella contenant la chaîne .exe correspondent à la stratégie de trafic. Click



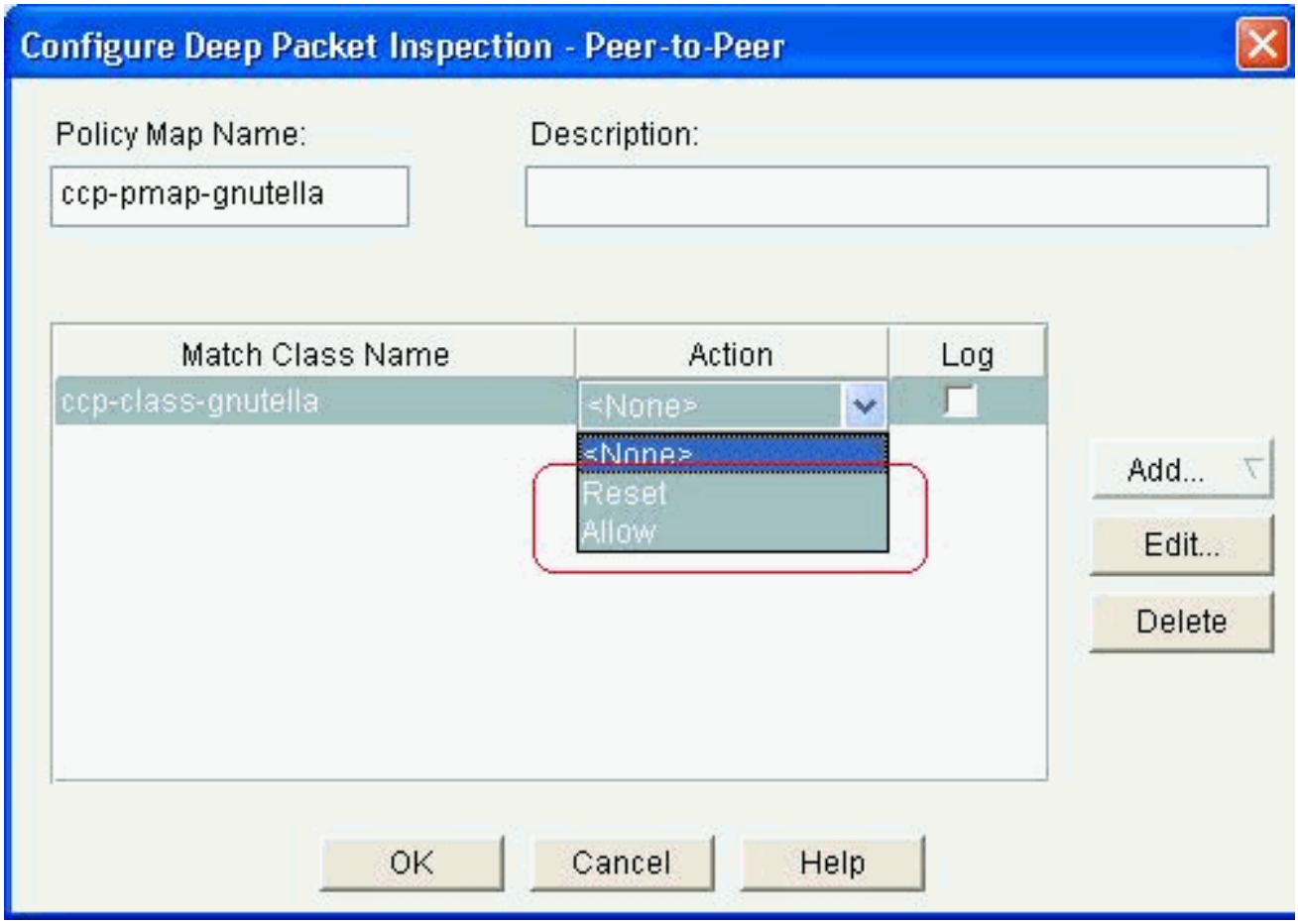
OK.

19. Cliquez à nouveau sur **OK** pour terminer la configuration de la carte-



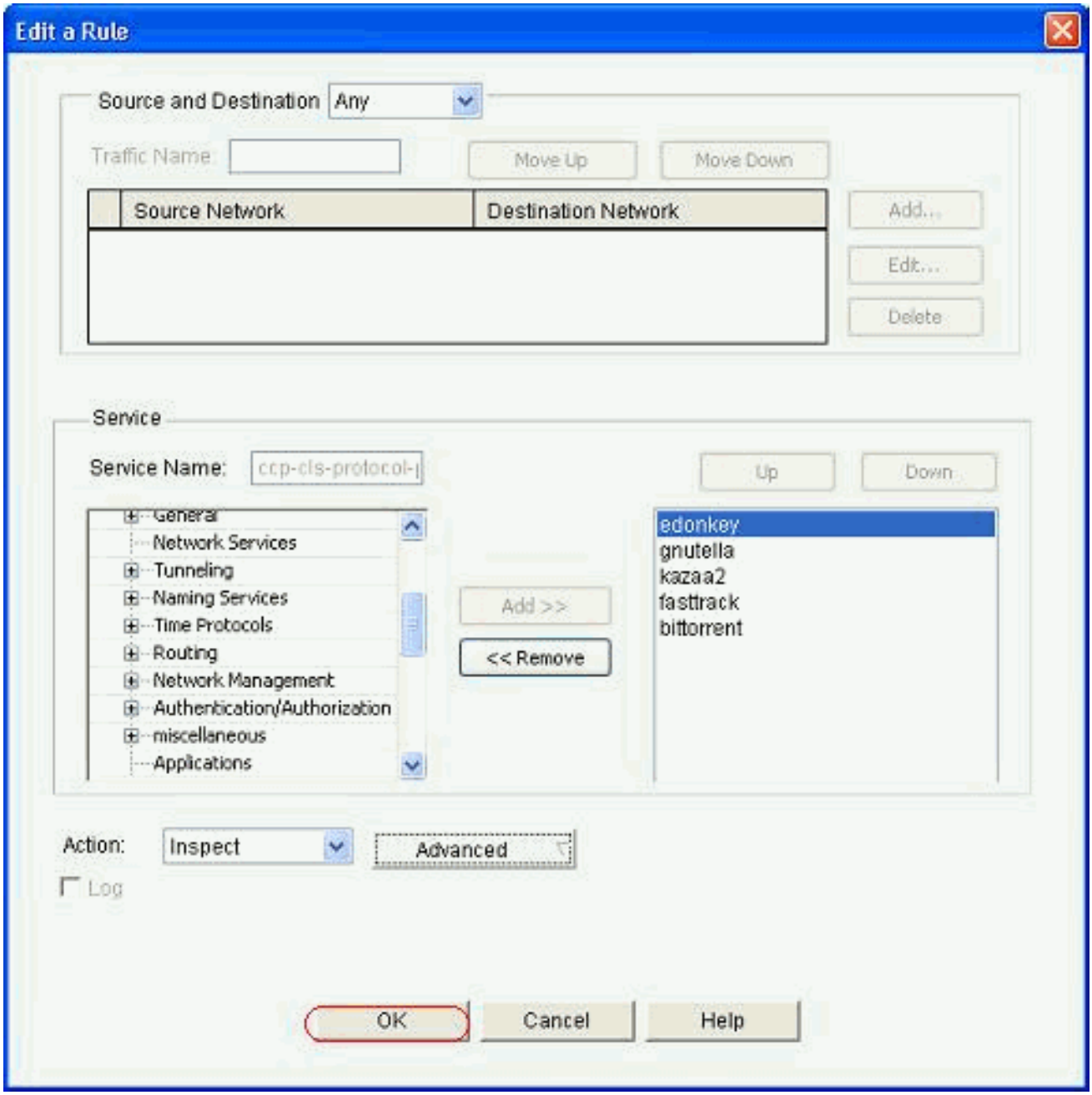
classe.

20. Choisissez l'option **Reset** ou **Allow**, qui dépend de la stratégie de sécurité de votre société. Cliquez sur **OK** pour confirmer l'action à l'aide de la carte de stratégie.



De la même manière, vous pouvez ajouter d'autres cartes de stratégie pour implémenter des fonctions d'inspection approfondie pour d'autres protocoles P2P en spécifiant différentes expressions régulières comme critère de correspondance.**Remarque :** Les applications P2P sont particulièrement difficiles à détecter, en raison du comportement “ des ” de saut de port et d'autres astuces pour éviter la détection, ainsi que des problèmes introduits par des changements et des mises à jour fréquents des applications P2P qui modifient les comportements des protocoles. ZFW associe l'inspection dynamique du pare-feu natif aux fonctionnalités de reconnaissance du trafic NBAR (Network-Based Application Recognition) pour fournir un contrôle des applications P2P.**Remarque :** L'inspection des applications P2P offre des fonctionnalités spécifiques à une application pour un sous-ensemble des applications prises en charge par l'inspection de couche 4 :edonkeyfasttrackgnutellakazaa2**Remarque :** Actuellement, ZFW n'a pas la possibilité d'inspecter le trafic de l'application « bittorrent ». Les clients BitTorrent communiquent généralement avec des trackers (serveurs d'annuaire homologue) via HTTP exécuté sur un port non standard. Ceci est généralement le TCP 6969, mais vous pourriez devoir contrôler le port traqueur spécifique au torrent. Si vous souhaitez autoriser BitTorrent, la meilleure méthode pour prendre en charge le port supplémentaire est de configurer HTTP comme l'un des protocoles de correspondance et d'ajouter TCP 6969 à HTTP à l'aide de cette commande ip port-map : **ip port-map http port tcp 6969**. Vous devrez définir le HTTP et BitTorrent comme critères de correspondance appliqués dans la carte-classe.

21. Cliquez sur **OK** pour terminer la configuration d'inspection avancée.



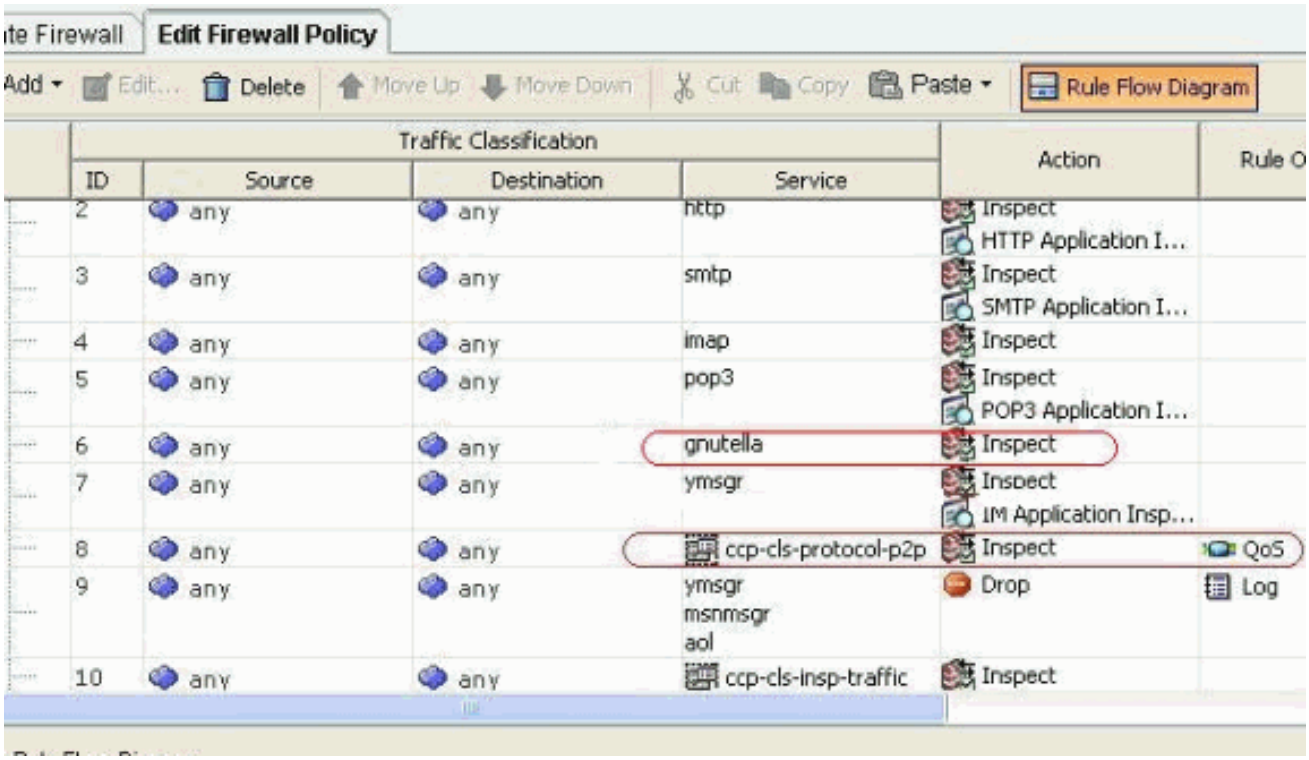
L’ensemble de commandes correspondant est transmis au routeur.

22. Cliquez sur **OK** pour terminer la copie du jeu de commandes sur le



routeur.

23. Vous pouvez observer les nouvelles règles qui se produisent dans l'onglet Modifier la stratégie de pare-feu sous **Configurer > Sécurité > Pare-feu et ACL**.



Configuration en ligne de commande du routeur ZFW

La configuration de la section précédente de Cisco CP donne les résultats suivants sur le routeur ZFW :

Routeur 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#
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

- ZBF-Router**#show policy-map type inspect zone-pair sessions** : affiche les statistiques de policy-map type d'inspection au moment de l'exécution pour toutes les paires de zones

existantes.

Informations connexes

- Guide de conception et d'application du pare-feu de stratégie basé sur la zone
- Exemple de configuration d'une application de pare-feu virtuel basé sur la zone et de pare-feu Cisco IOS classique
- Page d'accueil de Cisco Configuration Professional