

Cisco Configuration Professional : Pare-feu basé sur zone bloquant le pair pour scruter exemple de configuration du trafic

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Configuration de routeur pour diriger Cisco CP](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configuration par le Cisco Configuration Professional](#)

[Configuration de ligne de commande de routeur ZFW](#)

[Vérifiez](#)

[Informations connexes](#)

Introduction

Ce document fournit une approche pas à pas pour configurer un routeur Cisco IOS comme Pare-feu basé sur zone pour bloquer le trafic peer-to-peer (de P2P) à l'aide de l'assistant avancé de configuration de Pare-feu dans le 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 stratégies d'inter-zone offrent la flexibilité et la finesse considérables. Par conséquent, différentes stratégies d'inspection peuvent être appliquées à de plusieurs groupes hôte 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 région 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 certaines des applications les plus très utilisées sur l'Internet. Les réseaux P2P peuvent agir en tant que conduit pour des menaces malveillantes telles que des vers, offrant un chemin facile autour des Pare-feu et entraînant des soucis concernant la sécurité et confidentialité. Le Logiciel Cisco IOS version 12.4(9)T a introduit le soutien ZFW des applications de P2P. Les offres d'inspection de P2P posent 4 et posent 7 stratégies pour le trafic

de l'application. Ceci signifie que ZFW peut fournir l'inspection avec état de base pour permettre ou refuser le trafic, aussi bien que le contrôle granulaire de la couche 7 sur des activités spécifiques dans les divers protocoles, de sorte que certaines activités d'application soient permises tandis que d'autres sont refusées.

Cisco CP offre un facile-à-suivre, approche pas à pas pour configurer le routeur IOS comme Pare-feu basé sur zone à l'aide de l'assistant avancé de configuration de Pare-feu.

Conditions préalables

Conditions requises

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

- Le routeur IOS doit avoir la version de logiciel en tant que 12.4(9)T ou plus tard.
- Pour les modèles de routeur IOS qui prennent en charge Cisco CP, référez-vous aux [notes de mise à jour en Cisco CP](#).

Configuration de routeur pour diriger Cisco CP

Remarque: Exécutez ces étapes de configuration afin de diriger Cisco CP sur un routeur de 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
```

Composants utilisés

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

- Routeur IOS de Cisco 1841 qui exécute la version de logiciel d'IOS Software 12.4(15)T
- Version 2.1 de Cisco Configuration Professional (Cisco CP)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Informations générales

Pour l'exemple de ce document, le routeur est configuré comme Pare-feu basé sur zone pour bloquer le trafic P2P. Le routeur ZFW a deux interfaces, une interface d'inside(trusted) dans la Dans-zone et une interface (non approuvée) extérieure dans la -zone. Le routeur ZFW bloque des applications P2P telles que l'edonkey, la promotion accélérée, le gnutella et le kazaa2 avec se connecter l'action pour le trafic qui passe de la Dans-zone à la -zone.

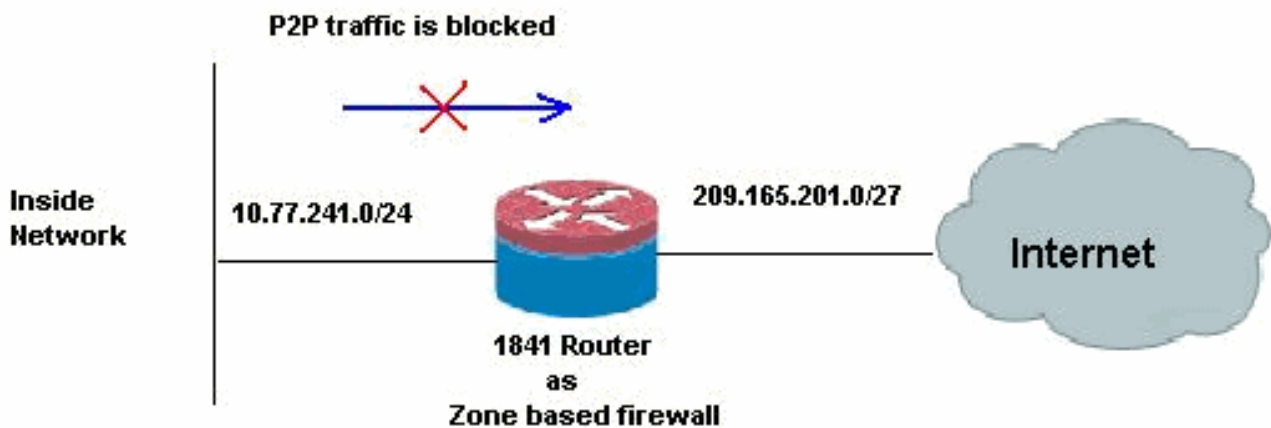
Configurez

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

Remarque: Utilisez l'outil [Command Lookup Tool](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

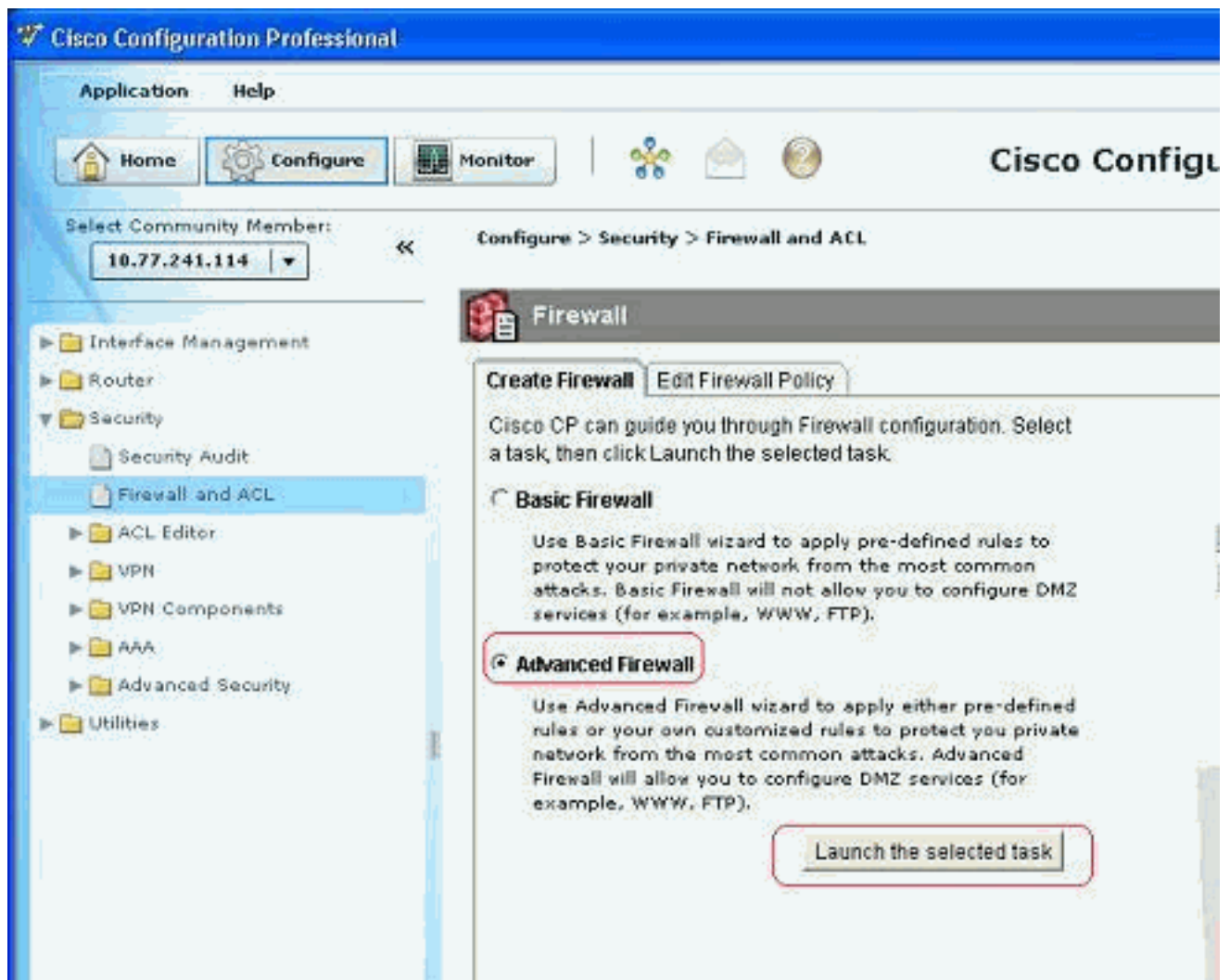


Configuration par le Cisco Configuration Professional

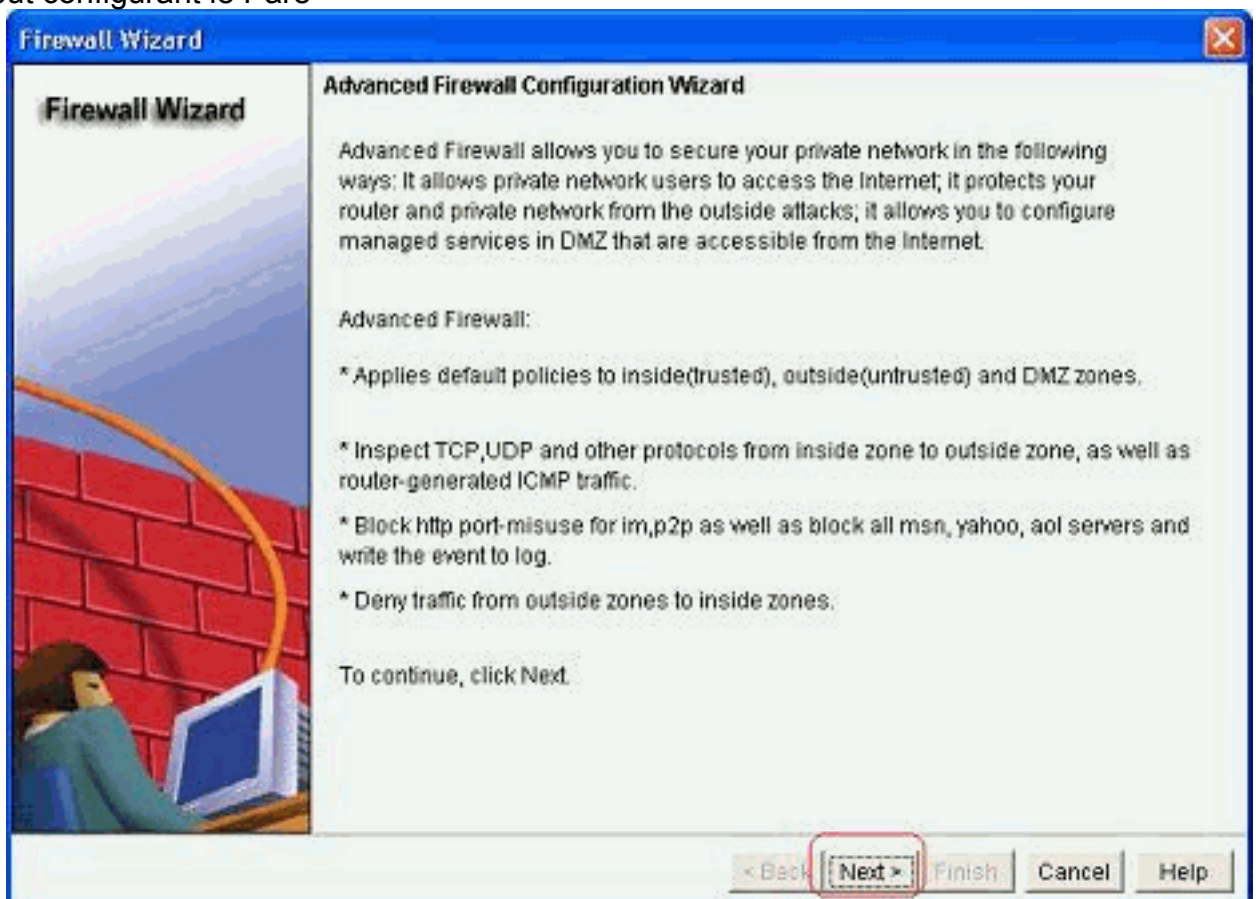
Cette section contient la procédure pas à pas sur la façon dont utiliser l'assistant pour configurer le routeur IOS comme Pare-feu basé sur zone.

Procédez comme suit :

1. Allez configurer > Sécurité > Pare-feu et ACL. Puis, choisissez la case d'option **avancée de Pare-feu**. Lancement de clic la tâche sélectionnée.

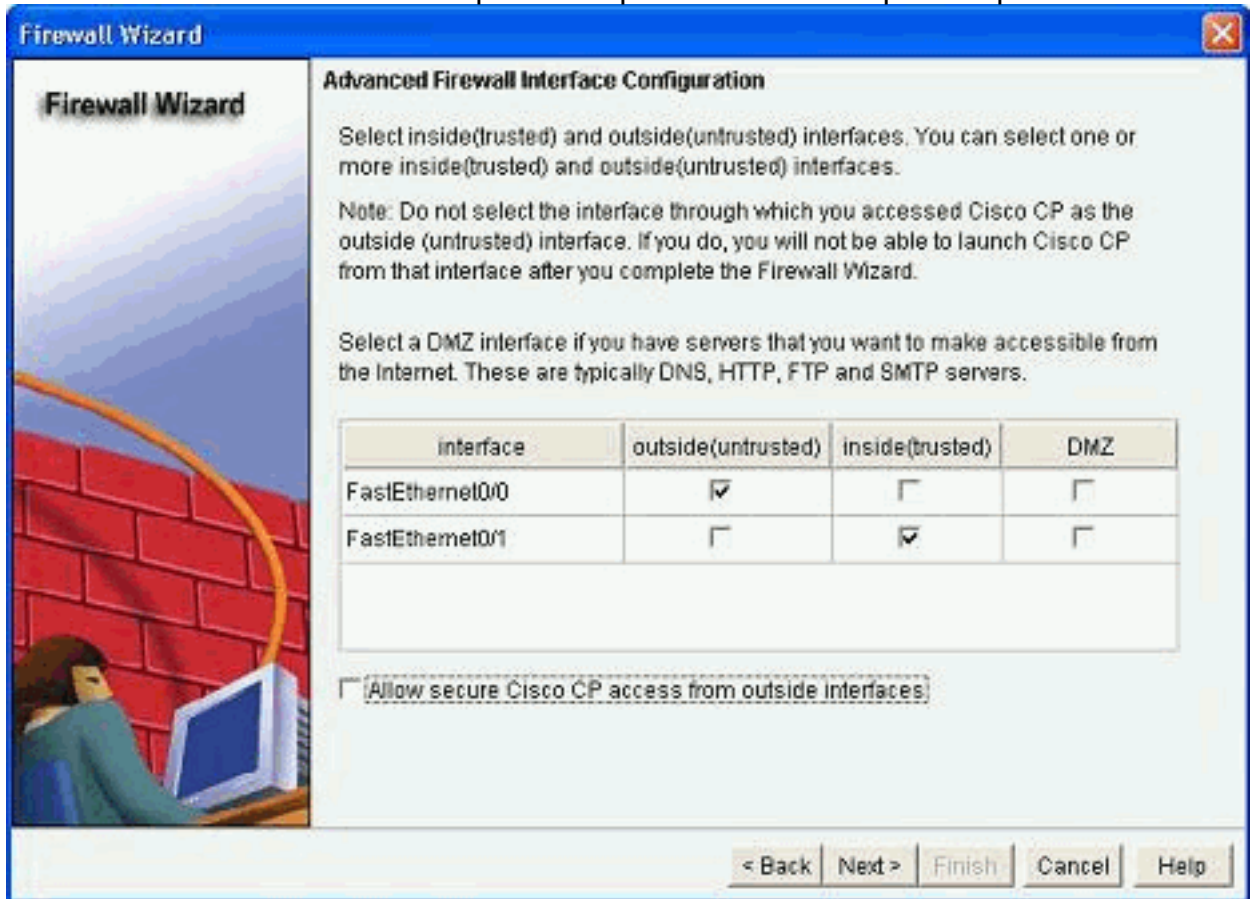


2. Cet écran suivant affiche une brève introduction au sujet de l'assistant firewall. Clic à côté du début configurant le Pare-



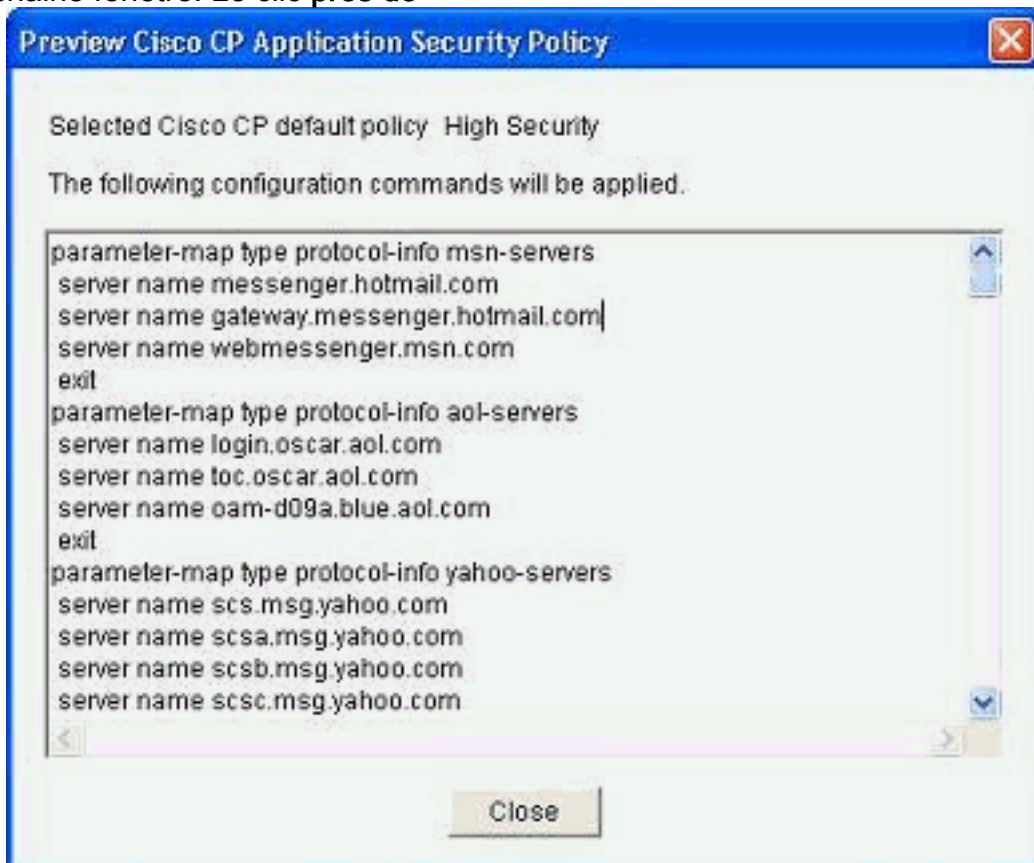
feu.

3. Sélectionnez les interfaces du routeur pour faire partie de zones et pour cliquer sur



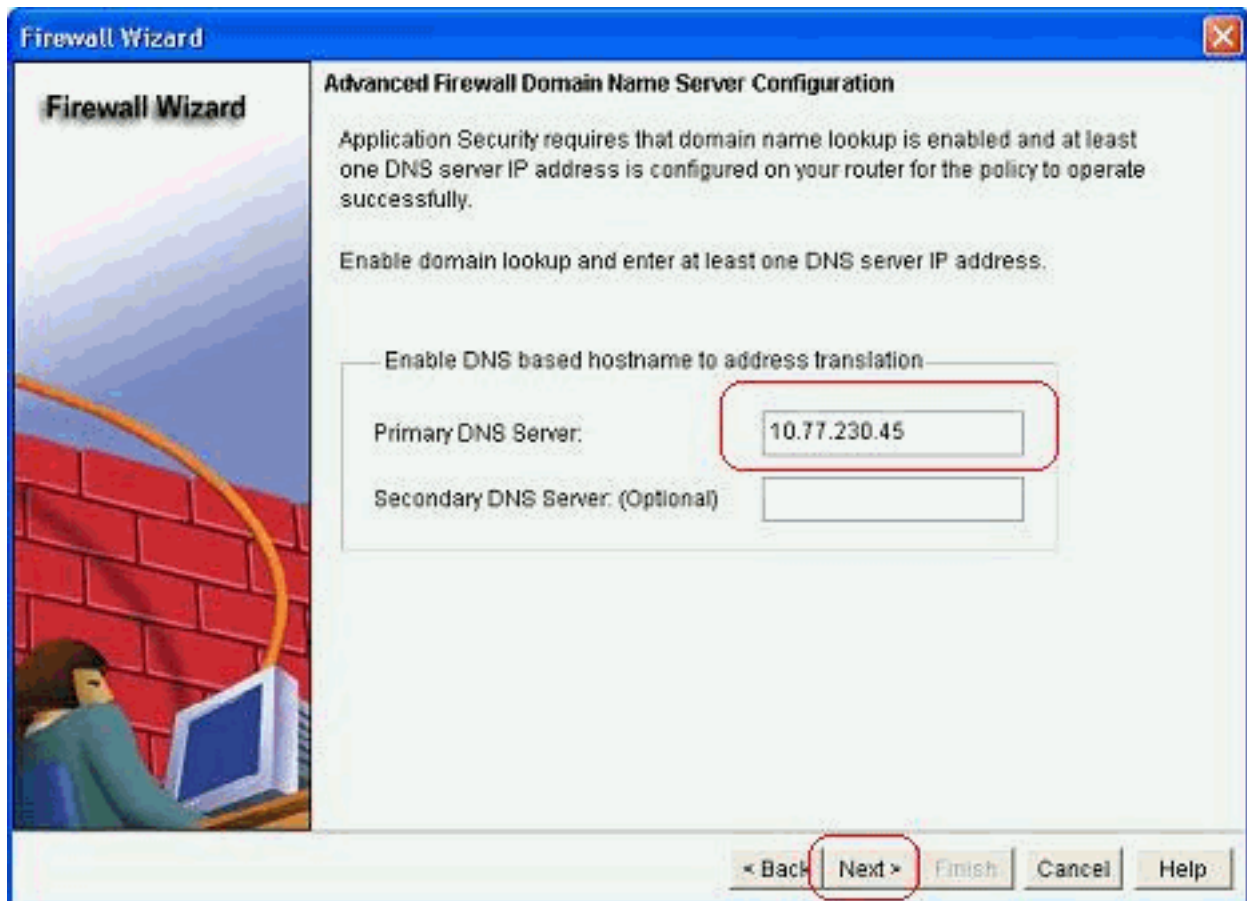
Next.

4. La stratégie par défaut avec la sécurité élevée avec l'ensemble de commandes est affichée dans la prochaine fenêtre. Le clic **près de**

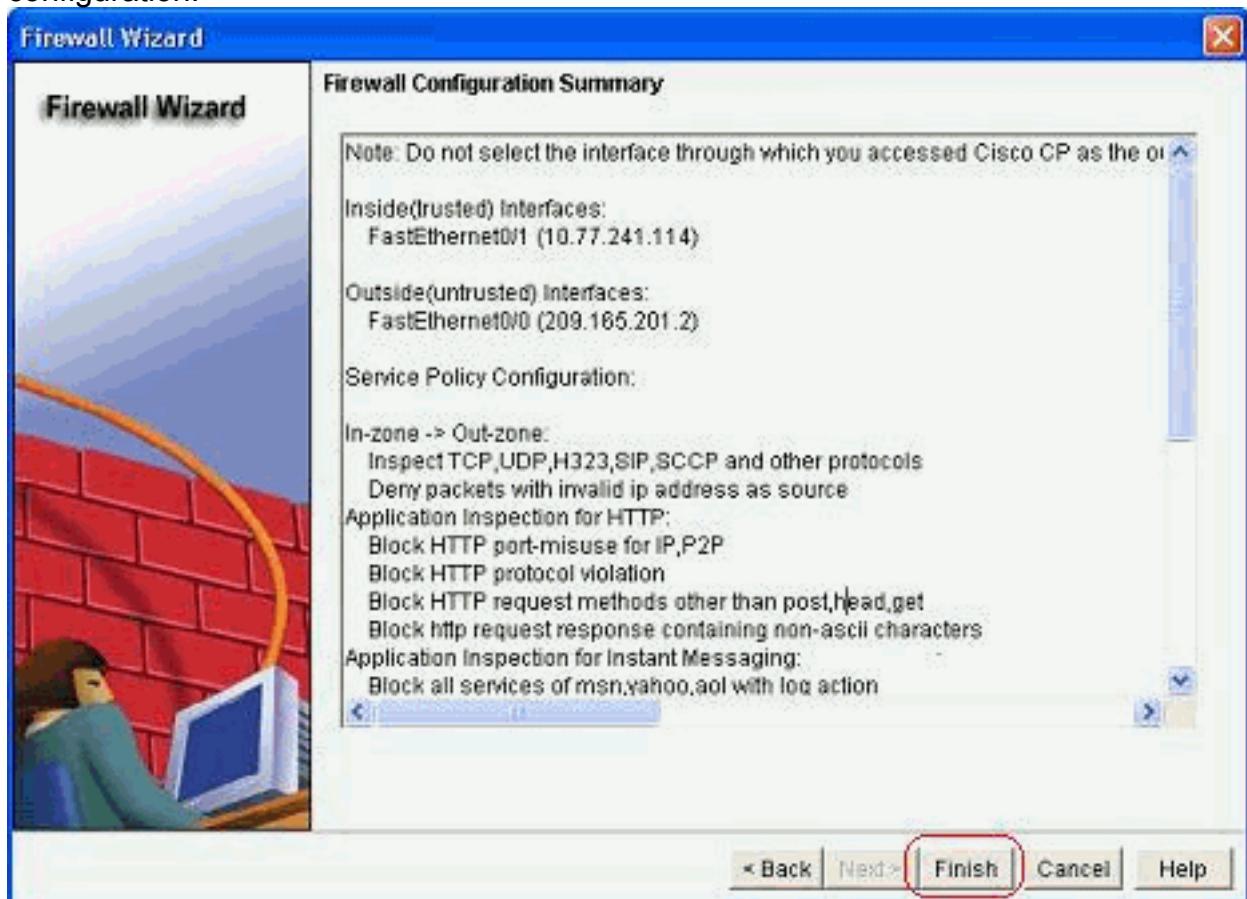


poursuivent.

5. Présentez les coordonnées du serveur DNS et cliquez sur Next.

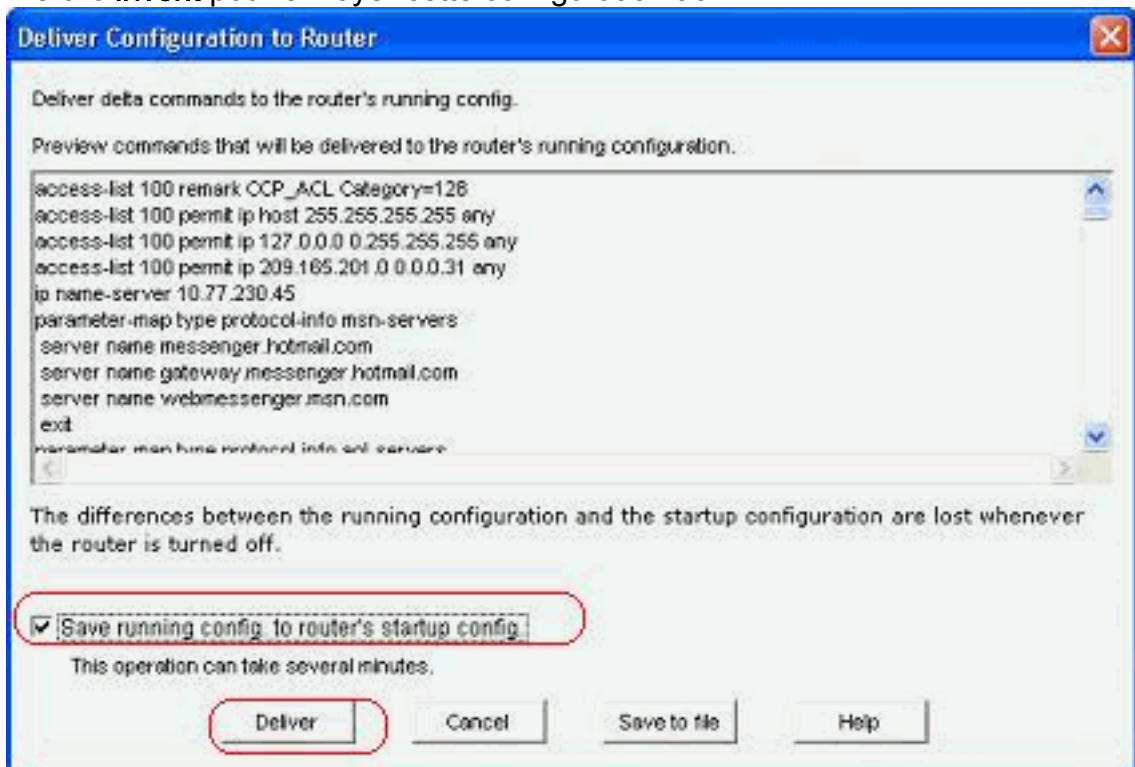


6. Cisco CP fournit un résumé de configuration tel que celui affiché ici. Cliquez sur Finish pour se terminer la configuration.

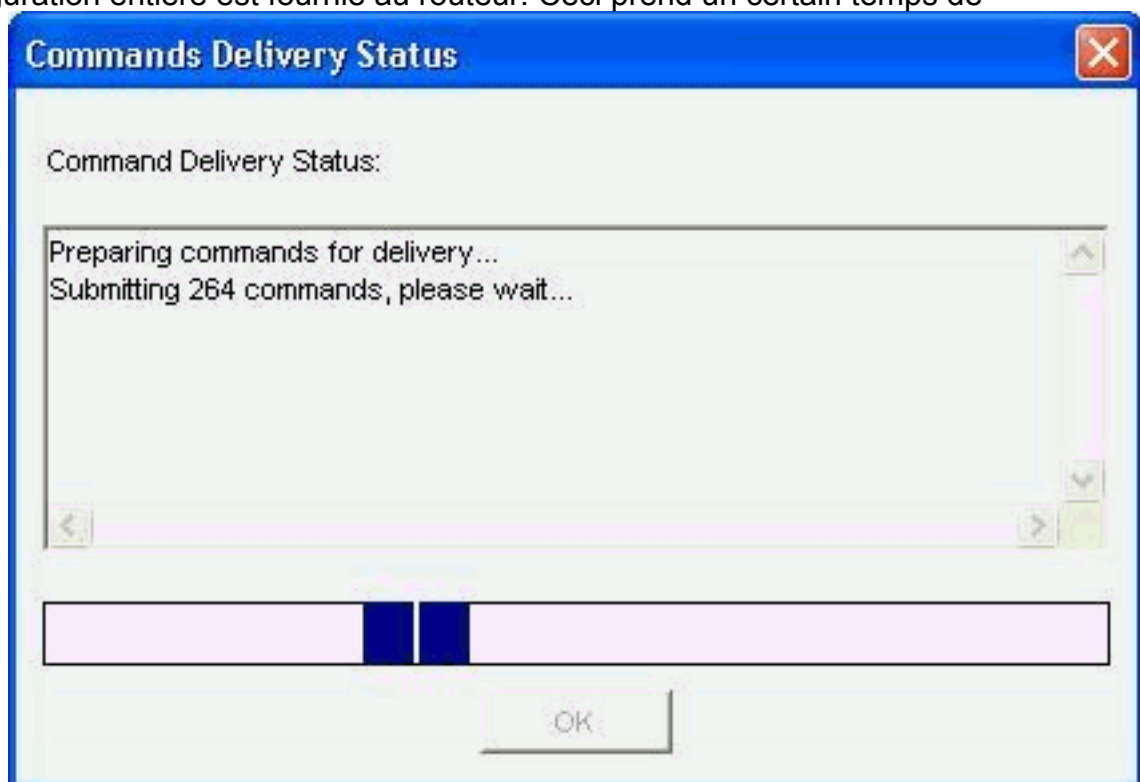


Le résumé de configuration détaillée est fourni dans cette table. C'est la configuration par défaut selon la stratégie de sécurité élevée de Cisco CP.

7. Cochez la **sauvegarde la configuration en cours** dans la case de démarrage du config du **routeur**. Le clic livrent pour envoyer cette configuration au

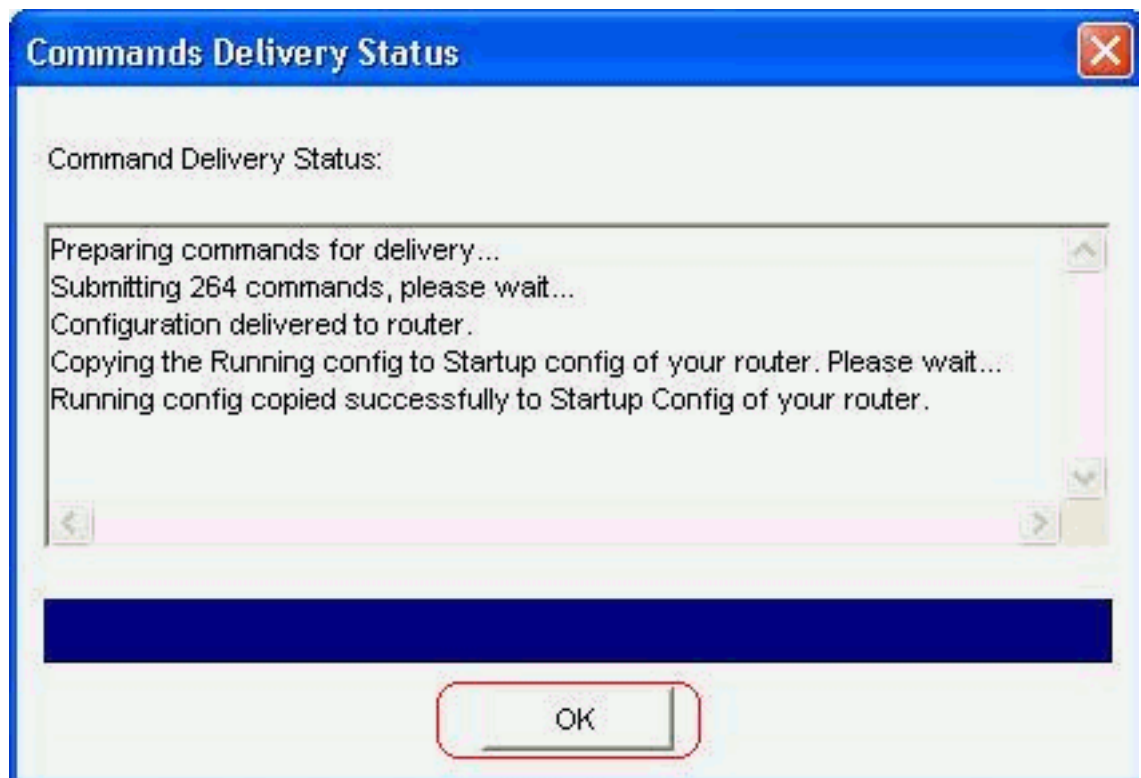


routeur. La configuration entière est fournie au routeur. Ceci prend un certain temps de



traiter.

8. Cliquez sur OK pour



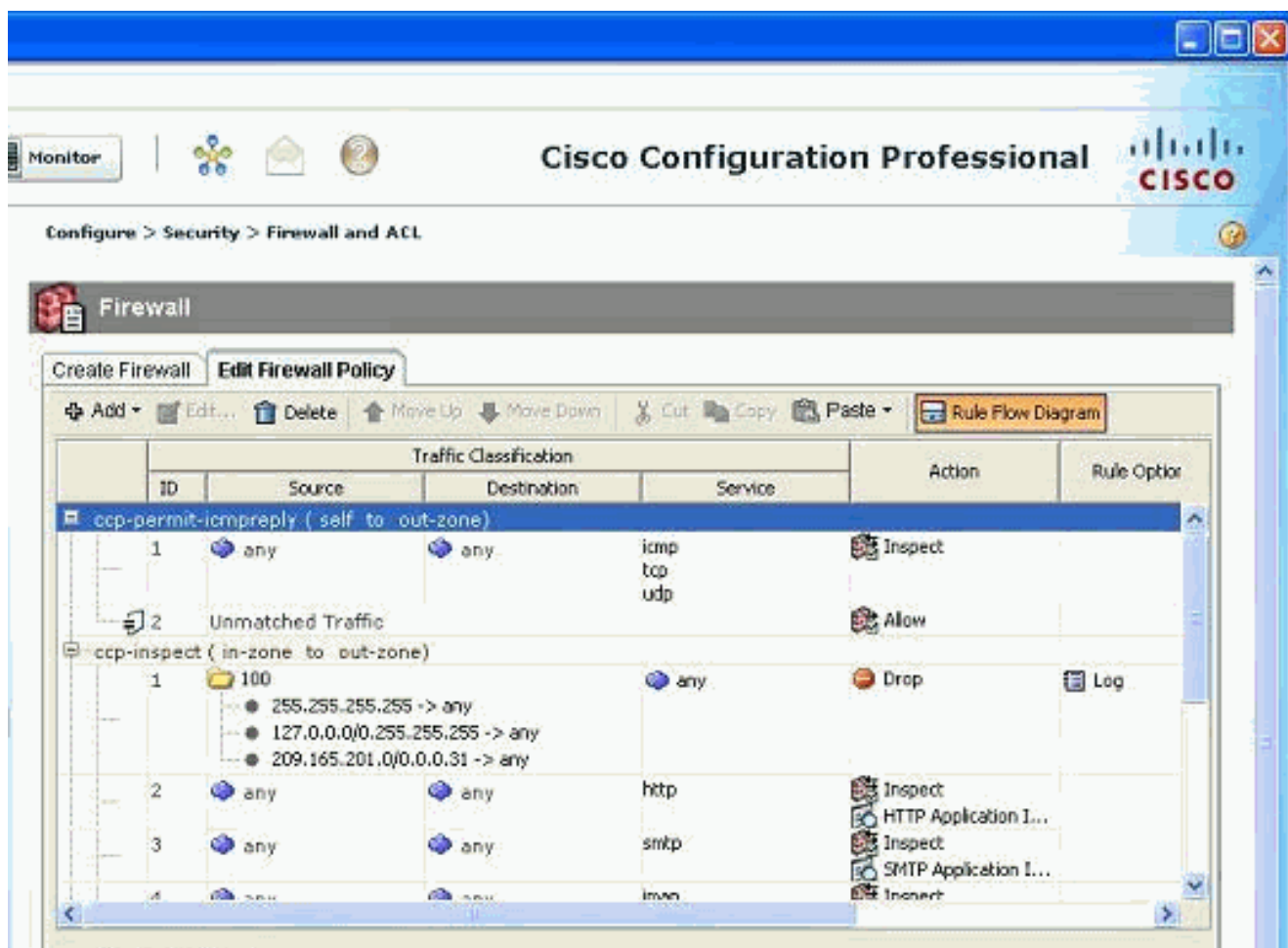
poursuivre.

9. Cliquez sur OK de

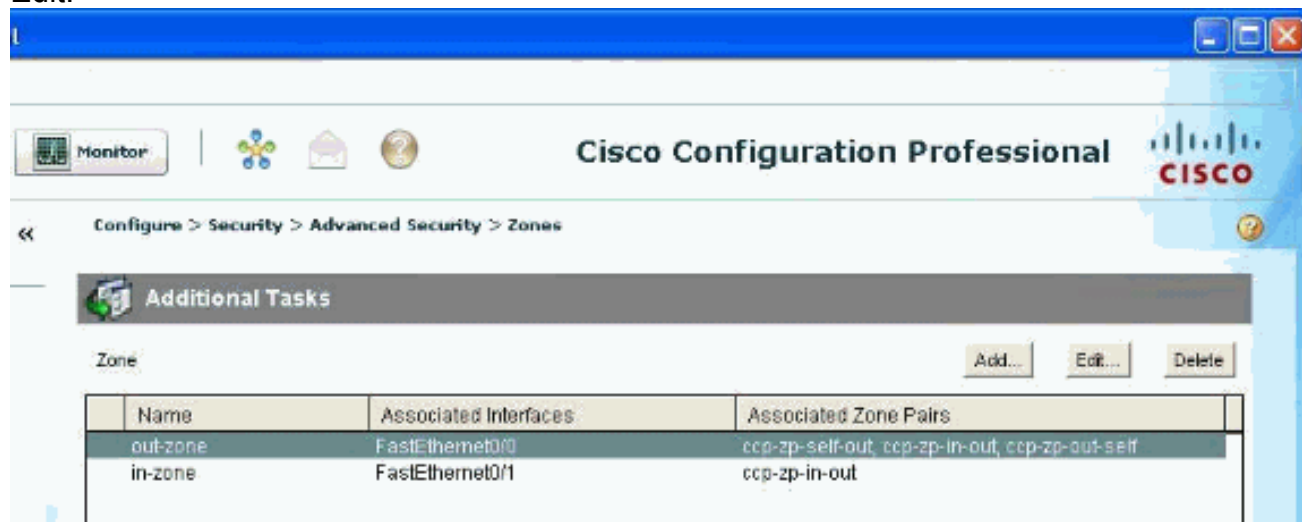


nouveau.

La configuration est maintenant en effet et est affichée comme règles sous l'onglet de stratégie de Pare-feu.



10. Les zones avec les paires de zone qu'elles sont associées peuvent être visualisées si vous allez **configurer > Sécurité > sécurité avancée > zones**. Vous pouvez également ajouter de nouvelles zones en cliquant sur Add, ou modifiez les zones existantes en cliquant sur Edit.



11. Allez **configurer > des paires de Sécurité > de sécurité avancée > de zone** pour visualiser les détails des paires de zone.

Monitor | Cisco Configuration Professional

Configure > Security > Advanced Security > Zone Pairs

Additional Tasks

Zone Pairs Add... Edit... Delete

Zone Pair	Source	Destination	Policy
ccp-zp-self-out	self	out-zone	ccp-permit-icmpreply
ccp-zp-in-out	in-zone	out-zone	ccp-inspect
ccp-zp-out-self	out-zone	self	ccp-permit

L'aide instantanée sur la façon dont modifier/ajoutent/zones d'effacement/paires de zone et d'autres informations relatives sont facilement disponibles avec les pages Web intégrées à Cisco

Edit a Zone [Close]

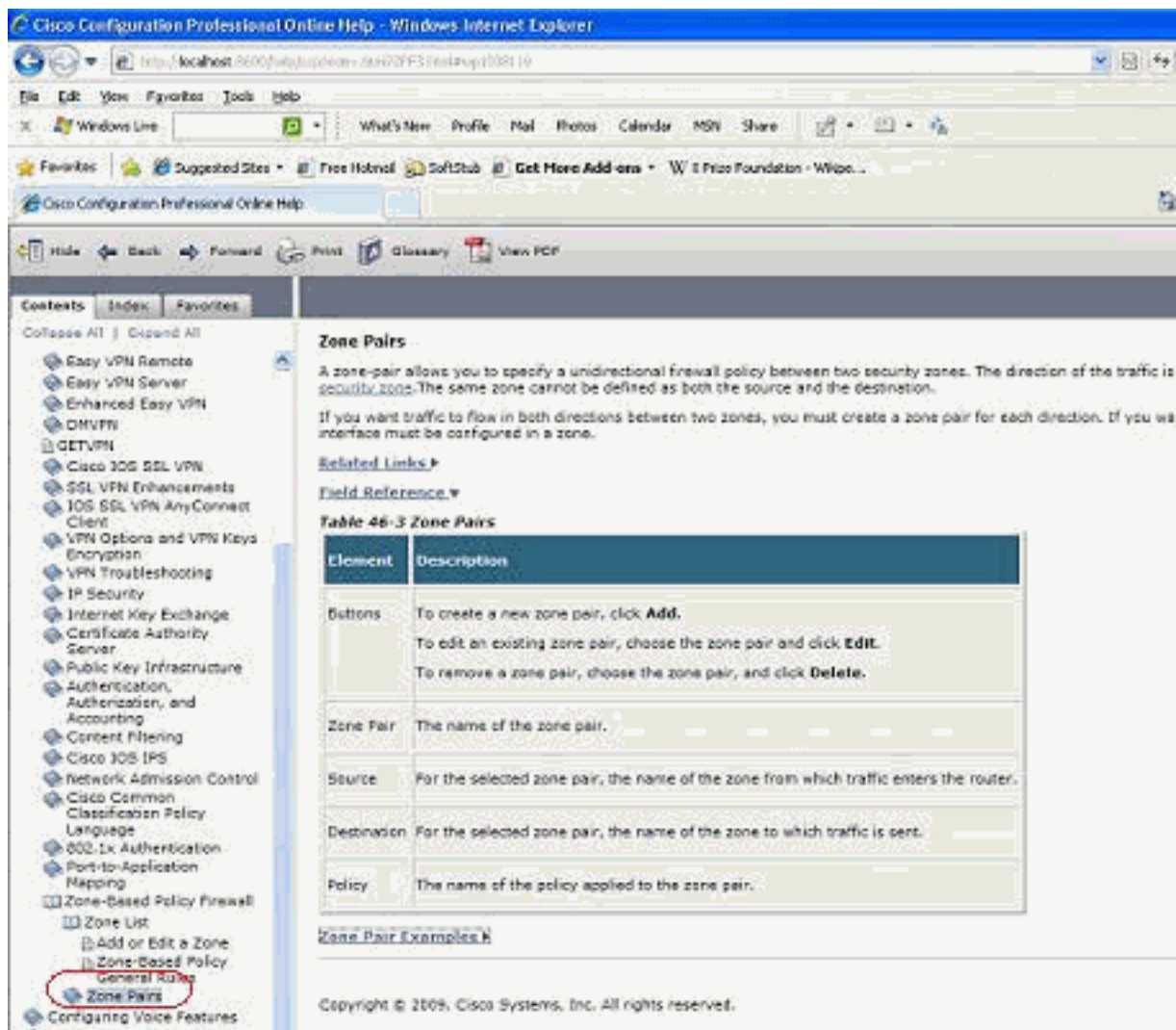
Zone Name :

Choose the interfaces to associate with the zone.

Interface
<input checked="" type="checkbox"/> FastEthernet0/1

OK Cancel Help

CP.

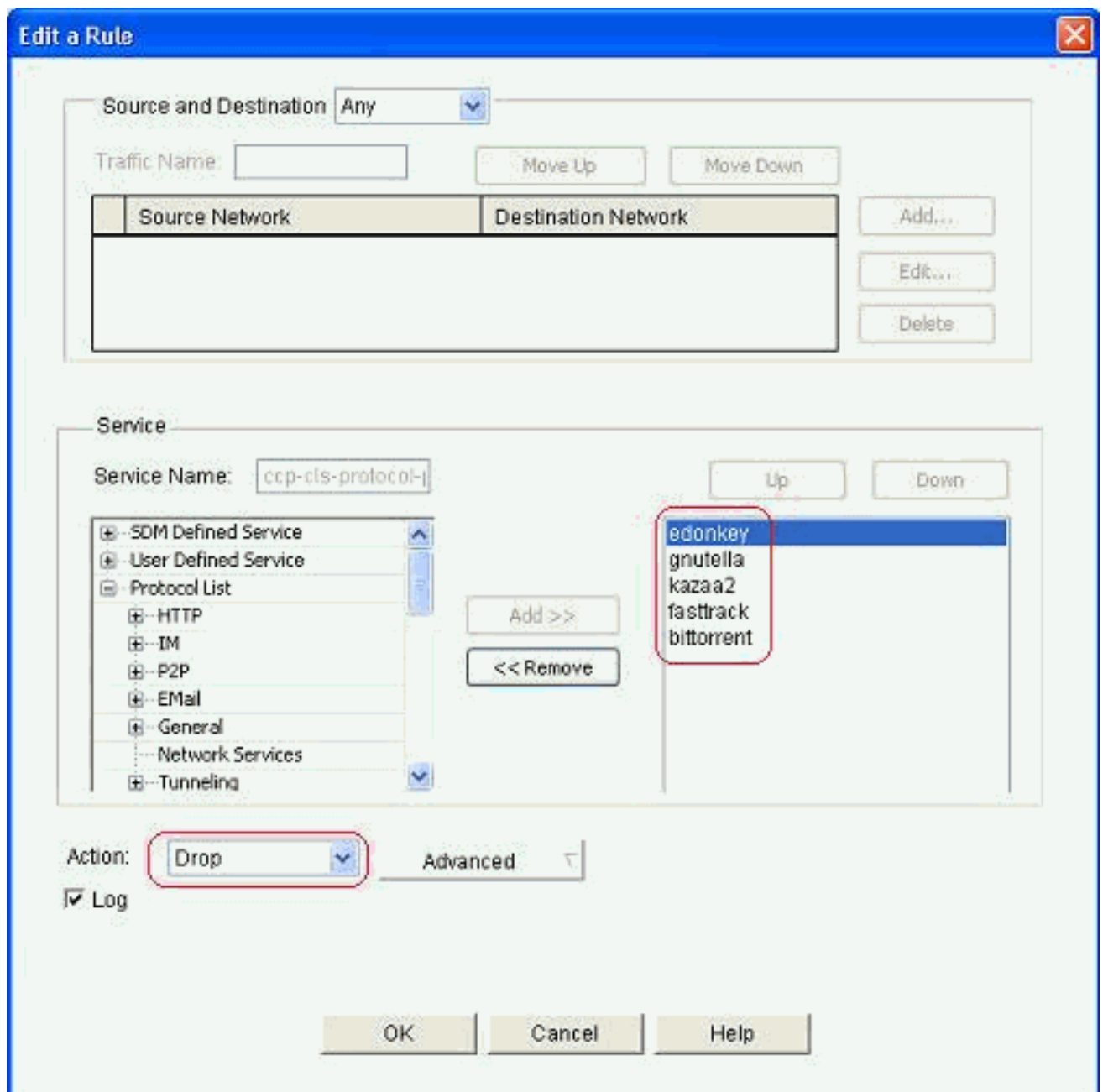


12. Afin de modifier les capacités spécifiques à l'application d'inspection pour certaines applications P2P, allez à la **configuration > à la Sécurité > au Pare-feu et à l'ACL**. Puis, cliquez sur Edit la **stratégie de Pare-feu** et choisissez la règle respective dans la carte de stratégie. Cliquez sur **Edit**.

The screenshot shows the 'Firewall' configuration window in a network management system. The 'Edit Firewall Policy' tab is active. A toolbar at the top includes buttons for 'Add', 'Edit...', 'Delete', 'Move Up', 'Move Down', 'Cut', 'Copy', 'Paste', and 'Rule Flow Diagram'. Below the toolbar is a table of firewall rules. The table has columns for ID, Source, Destination, Service, Action, and a partially visible 'Rule' column. Rule 1 is expanded to show a source address of '100' with three sub-entries: '255.255.255.255 -> any', '127.0.0.0/0.255.255.255 -> any', and '209.165.201.0/0.0.0.31 -> any'. Rule 6 is highlighted in blue and shows a service named 'ccp-cls-protocol-p2p' with a 'Drop' action. Rule 7 is partially visible below it.

ID	Traffic Classification			Action	Rule
	Source	Destination	Service		
ccp-inspect (in-zone to out-zone)					
1	100 <ul style="list-style-type: none">255.255.255.255 -> any127.0.0.0/0.255.255.255 -> any209.165.201.0/0.0.0.31 -> any		any	Drop	Lo
2	any	any	http	Inspect HTTP Application I...	
3	any	any	smtp	Inspect SMTP Application I...	
4	any	any	imap	Inspect IMAP Application I...	
5	any	any	pop3	Inspect POP3 Application I...	
6	any	any	ccp-cls-protocol-p2p	Drop	Lo
7	any	any	any	Drop	Lo

Ceci prouve aux applications P2P en cours que bloqué par configuration par défaut.



13. Vous pouvez utiliser l'ajouter et les boutons Remove à ajouter/retirent des applications spécifiques. Ce tir d'écran affiche comment ajouter l'application de 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: cc-p-cls-protocol-1

Up

Down

- HTTP
- IM
- P2P
 - directconnect
 - winx**
- Email
- General
- Network Services
- Tunneling
- Named Services

Add >>

<< Remove

- edonkey**
- kazaa2
- bittorrent
- fastrack
- gnutella

Action: Drop

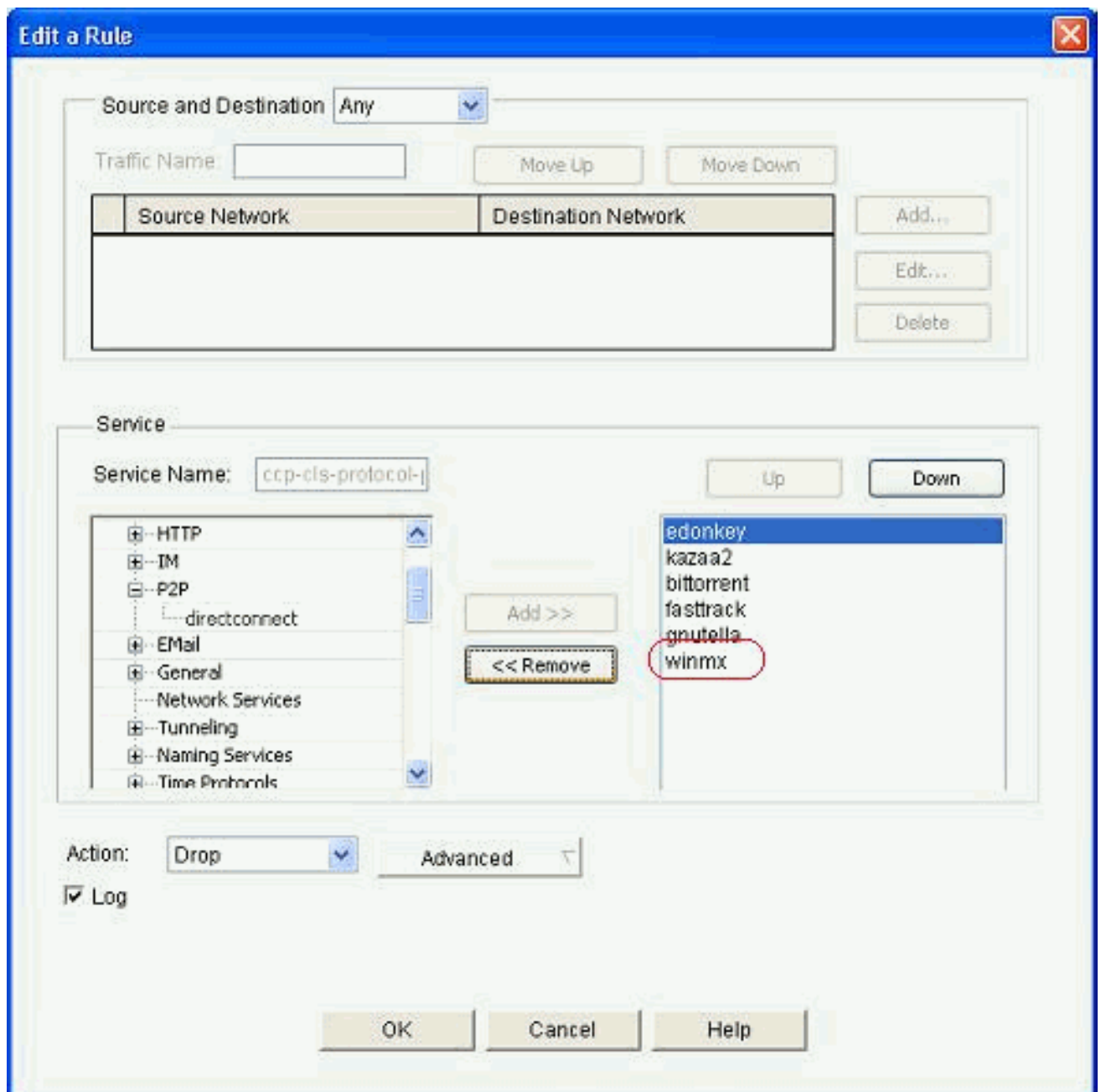
Advanced

Log

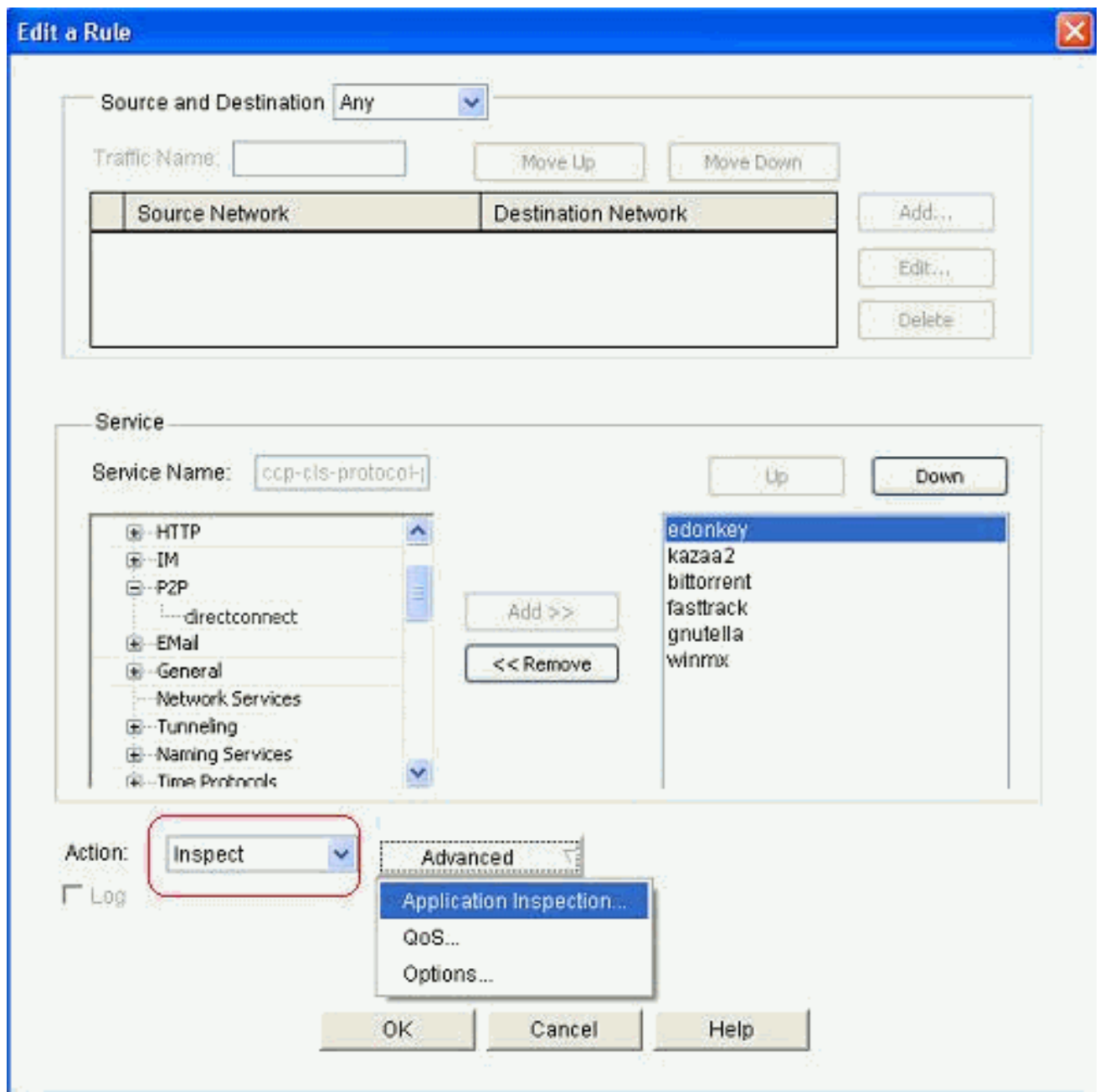
OK

Cancel

Help

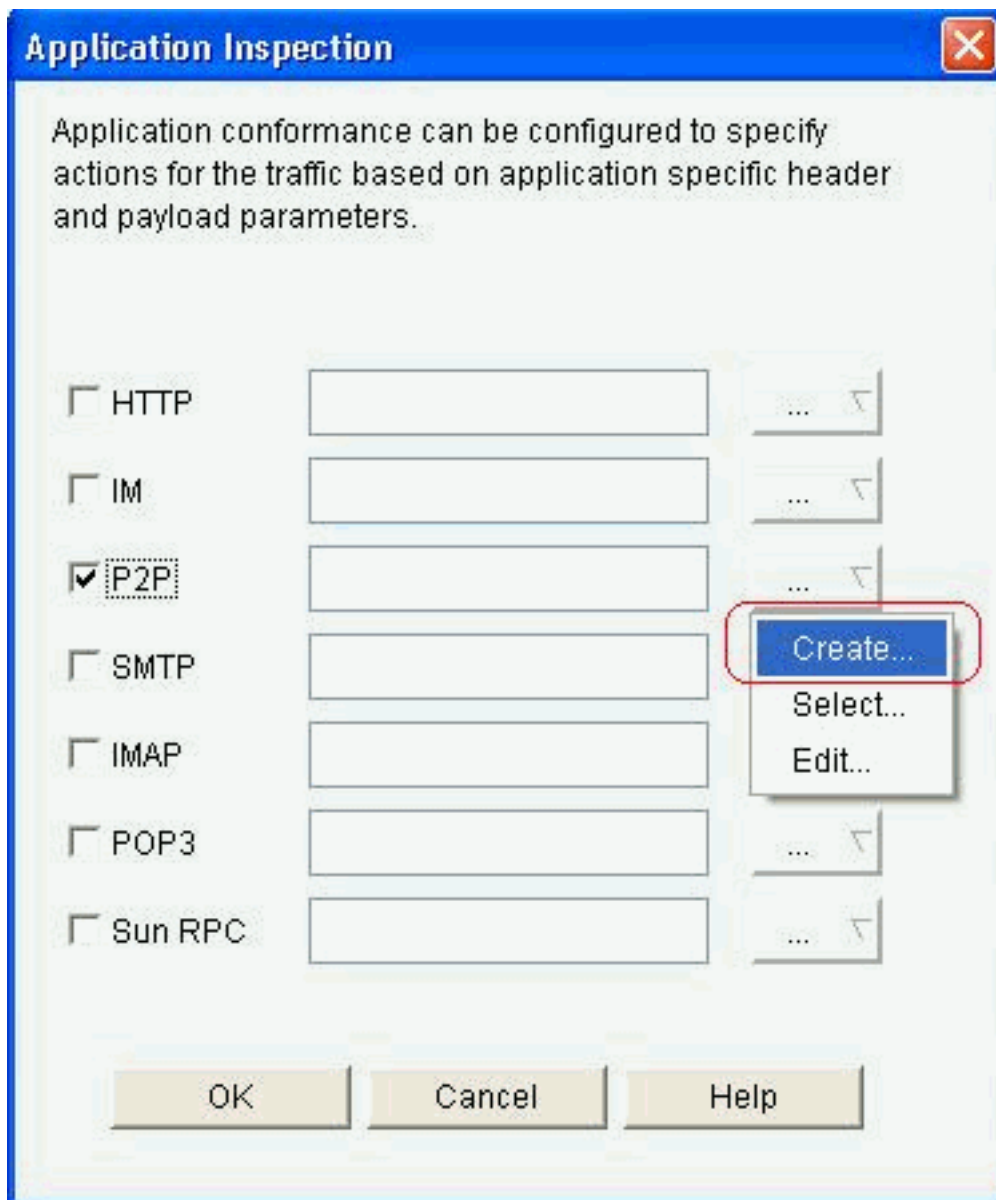


14. Au lieu de choisir l'action de baisse, vous pouvez également choisir l'action d'examiner d'appliquer différentes options pour l'inspection profonde de paquet.



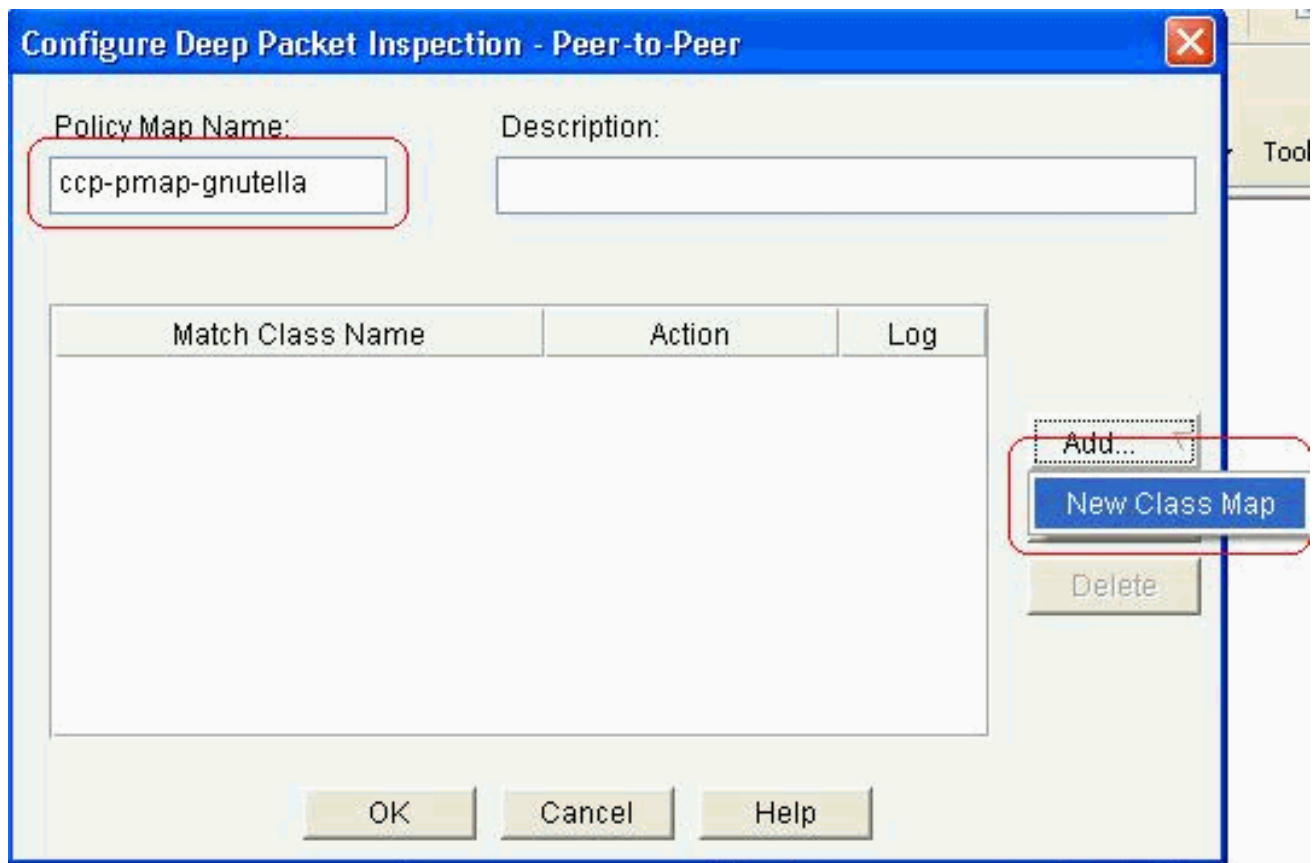
Les offres d'inspection de P2P posent 4 et posent 7 stratégies pour le trafic de l'application. Ceci signifie que ZFW peut fournir l'inspection avec état de base pour permettre ou refuser le trafic, aussi bien que le contrôle granulaire de la couche 7 sur des activités spécifiques dans les divers protocoles, de sorte que certaines activités d'application soient permises tandis que d'autres sont refusées. Dans cette inspection d'application, vous pouvez appliquer différents types d'inspections spécifiques de niveau d'en-tête pour des applications P2P. Un exemple pour le gnutella est affiché ensuite.

15. Vérifiez l'option de **P2P** et le clic **créent** afin de créer un nouveau policy-map pour

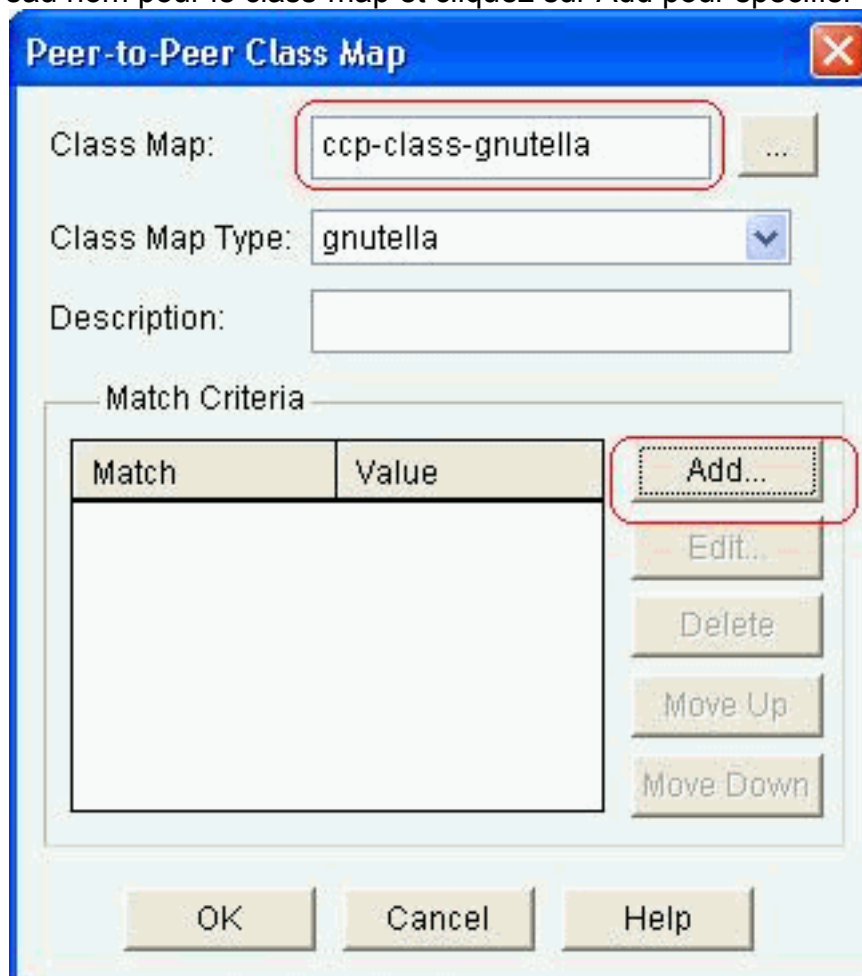


ceci.

16. Créez un nouveau policy-map pour l'inspection profonde de paquet pour le protocole de gnutella. Cliquez sur Add et puis choisissez le **nouveau class map**.



17. Donnez un nouveau nom pour le class-map et cliquez sur Add pour spécifier le critère de



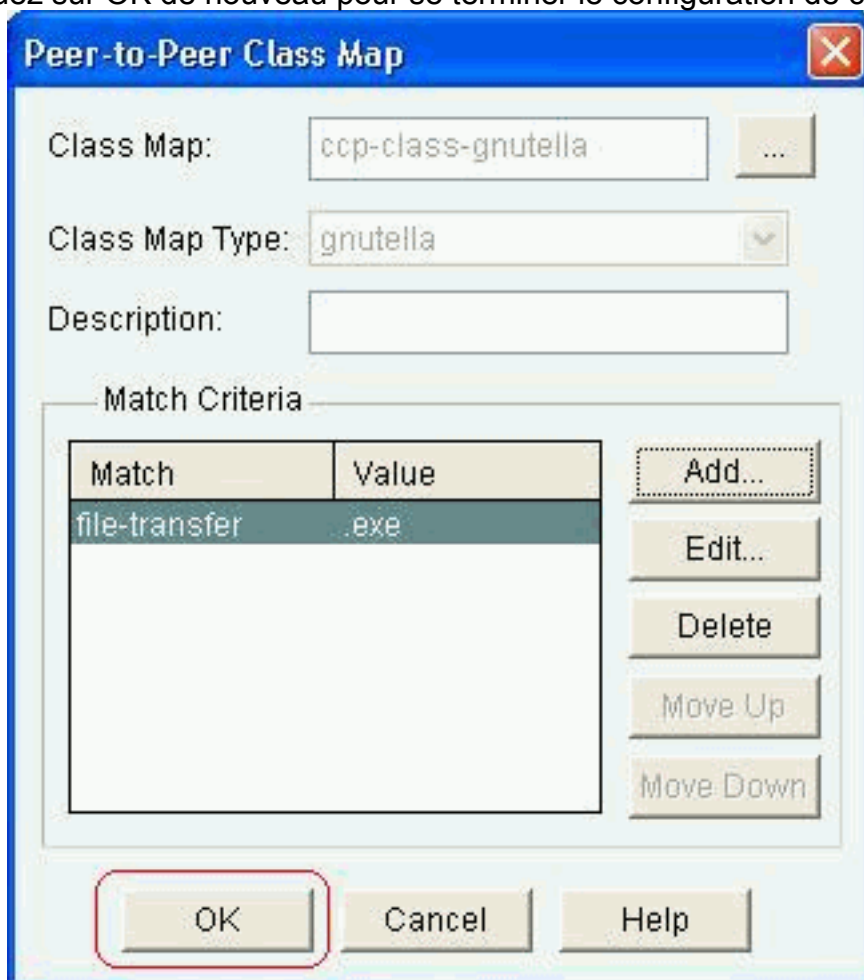
correspondance.

18. Utilisez le transfert de fichier car le critère de correspondance et la chaîne utilisés est .exe. Ceci indique que toutes les connexions de transfert de fichiers de gnutella contenant la vérification de la chaîne .exe pour la stratégie de trafic. Cliquez sur



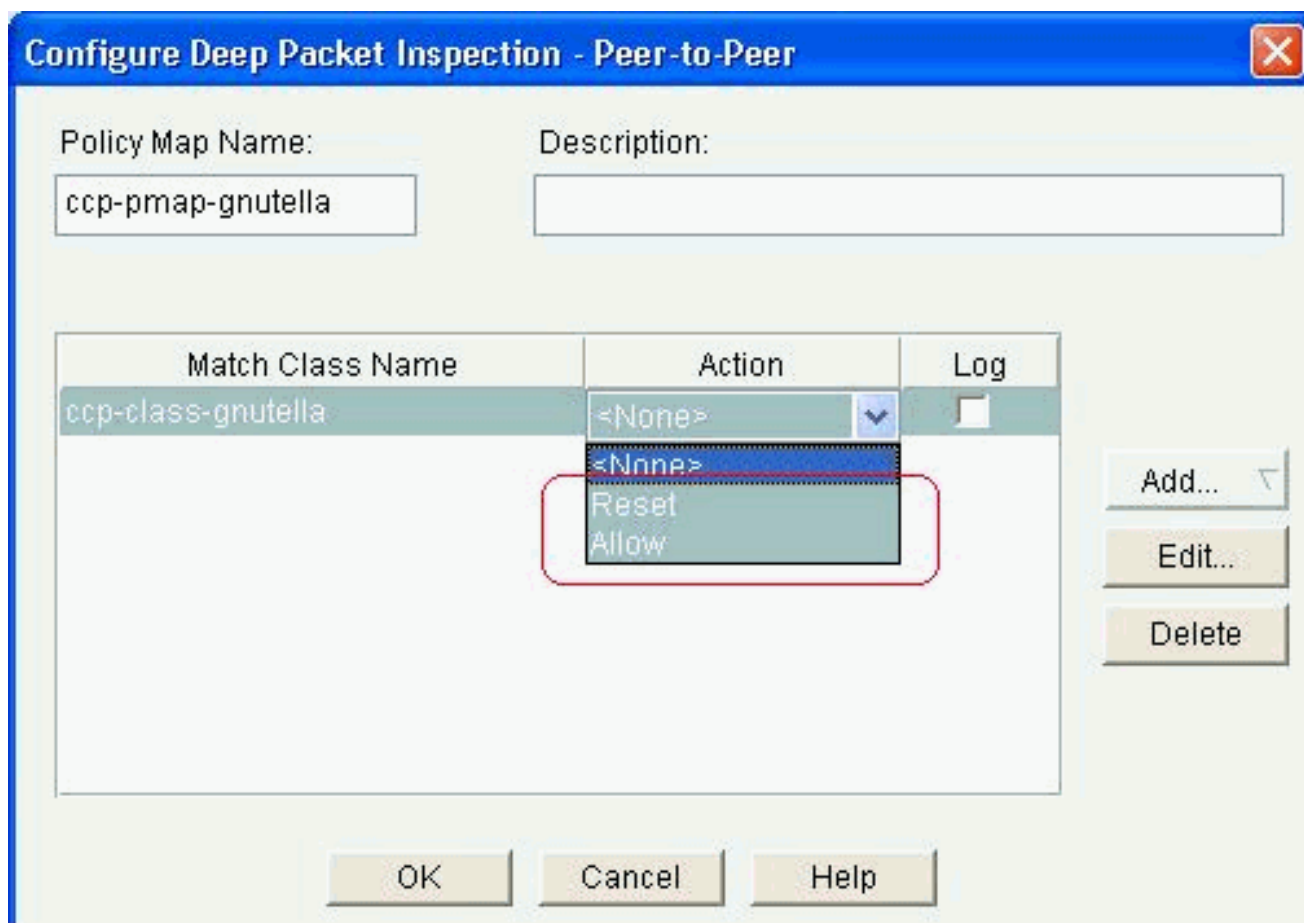
OK.

19. Cliquez sur OK de nouveau pour se terminer le configuration de class-



map.

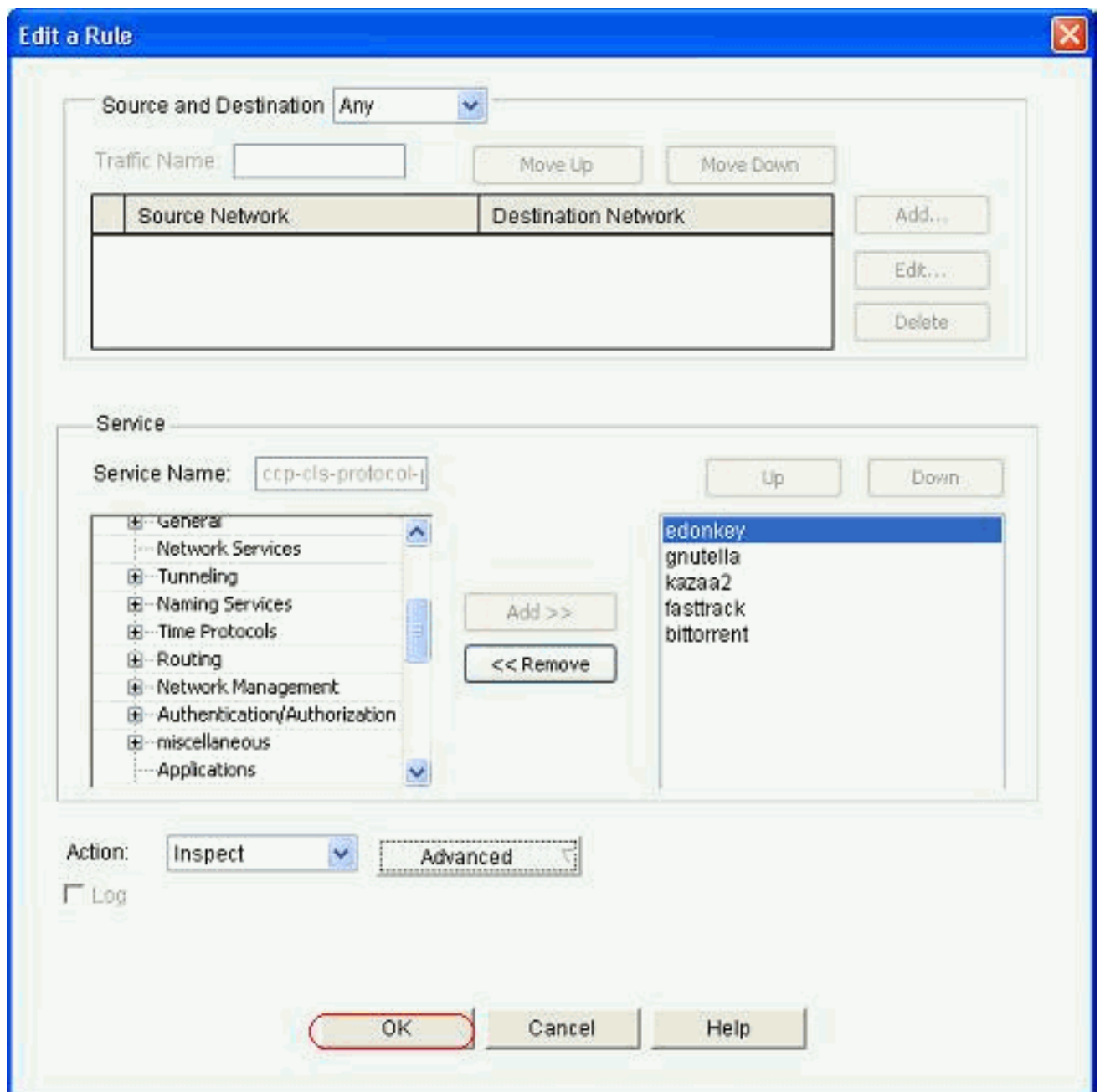
20. Choisissez la **remise** ou **permettez** l'option, qui dépend de la stratégie de sécurité de votre société. Cliquez sur OK pour confirmer l'action avec le policy-map.



De cette même façon vous pouvez ajouter d'autres policy-map pour implémenter les caractéristiques profondes d'inspection pour d'autres protocoles de P2P en spécifiant différentes expressions régulières comme critère de correspondance. **Remarque:** Les applications P2P sont particulièrement difficiles à détecter, en résultat d'un comportement « saut de port » et d'autres tours pour éviter la détection, aussi bien que des problèmes mis en place par les modifications et les mises à jour fréquentes pour les applications P2P qui modifient les comportements des protocoles. ZFW combine l'inspection avec état indigène de Pare-feu capacités de trafic-reconnaissance avec de Reconnaissance d'application fondée sur le réseau (NBAR) des 's pour fournir le contrôle d'application

P2P. **Remarque:** L'inspection de l'application P2P offre des capacités spécifiques pour un sous-ensemble des applications prises en charge par l'inspection de la couche 4 : edonkeypromotion accéléréegnutellakazaa2 **Remarque:** Actuellement, ZFW n'a pas une option d'examiner le trafic de l'application « bittorrent ». Les clients bittorrents communiquent habituellement avec des traqueurs (serveurs de répertoire de pair) par l'intermédiaire du HTTP s'exécutant sur un certain port non standard. Ceci est généralement le TCP 6969, mais vous pourriez devoir contrôler le port traqueur spécifique au torrent. Si vous souhaitez permettre BitTorrent, la meilleure méthode pour faciliter le port supplémentaire est de configurer le HTTP en tant qu'un des matchs protocoles et d'ajouter le TCP 6969 au HTTP utilisant cette commande d'ip port-map : **TCP 6969 de port de HTTP d'ip port-map**. Vous devrez définir le HTTP et BitTorrent comme critères de correspondance appliqués dans la carte-classe.

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



L'ensemble correspondant de commandes est fourni au routeur.

22. Cliquez sur OK pour se terminer en copiant l'ensemble de commandes sur le



routeur.

23. Vous pouvez observer les nouvelles règles avoir lieu de l'onglet de stratégie de Pare-feu d'éditer dessous pour configurer > Sécurité > Pare-feu et ACL.

ID	Traffic Classification			Service	Action	Rule O
	Source	Destination				
2	any	any		http	Inspect HTTP Application I...	
3	any	any		smtp	Inspect SMTP Application I...	
4	any	any		imap	Inspect	
5	any	any		pop3	Inspect POP3 Application I...	
6	any	any		gnutella	Inspect	
7	any	any		ymsgr	Inspect IM Application Insp...	
8	any	any		ccp-cls-protocol-p2p	Inspect	QoS
9	any	any		ymsgr msnmsgr aol	Drop	Log
10	any	any		ccp-cls-insp-traffic	Inspect	

Configuration de ligne de commande de routeur ZFW

La configuration dans la section précédente de Cisco CP a comme conséquence cette configuration 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
adsl.vip.scd.yahoo.com server name
radiol.launch.vip.dal.yahoo.com server name
inl.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#

```

Vérifiez

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**.

- **Sessions de zone-paire de policy-map type inspect de ZBF-Router#show** — Affiche le délai d'exécution examinant des statistiques de policy-map de type pour assurer toutes les paires existantes de zone.

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](#)
- [Guide utilisateur de Cisco Configuration Professional](#)
- [Support et documentation techniques - Cisco Systems](#)