Cisco Configuration Professional: Firewall Zona-basado que bloquea al par para mirar ejemplo de configuración del tráfico

Contenido

Introducción

Este documento proporciona un acercamiento gradual para configurar a un router del Cisco IOS como Firewall zona-basado para bloquear el tráfico entre iguales (P2P) usando el Asisitente avanzado de la configuración de escudo de protección en el Cisco Configuration Professional (Cisco CP).

El Firewall Zona-basado de la directiva (también conocido como el Firewall de la Zona-directiva, o ZFW) cambia la configuración de escudo de protección del más viejo modelo basado en la interfaz a un modelo zona-basado más flexible, más facilmente comprensible. Las interfaces se asignan a las zonas, y la directiva del examen se aplica para traficar la mudanza entre las zonas. las directivas de la Inter-zona ofrecen la considerable flexibilidad y el granularity. Por lo tanto, diversas directivas del examen se pueden aplicar a los grupos del host múltiple conectados con la interfaz del mismo router. Las zonas establecen las fronteras de la Seguridad de su red. Una zona define un límite donde el tráfico se sujeta a las restricciones de la directiva como él cruza a otra región de su red. La política predeterminada ZFW entre las zonas es niega todos. Si no se configura ninguna directiva explícitamente, todo el tráfico que se mueve entre las zonas se bloquea.

Las aplicaciones P2P son algunas de las aplicaciones más ampliamente utilizadas en Internet. Las redes P2P pueden actuar como conducto para las amenazas malévolas tales como gusanos, ofreciendo una trayectoria fácil alrededor de los Firewall y causando las preocupaciones por la aislamiento y la Seguridad. Soporte introducido Cisco IOS Software Release 12.4(9)T ZFW para

las aplicaciones P2P. El examen P2P ofrece la capa 4 y la capa 7 directivas para el tráfico de aplicación. Esto significa que ZFW puede proporcionar la inspección con estado básica al permit or deny el tráfico, así como el control granular de la capa 7 en las actividades específicas en los diversos protocolos, para permitir ciertas actividades de la aplicación mientras que se niegan otras.

Cisco CP ofrece un acercamiento fácil de seguir, gradual configurar al router IOS como Firewall zona-basado usando el Asisitente avanzado de la configuración de escudo de protección.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El router IOS debe tener la versión de software como 12.4(9)T o más adelante.
- Para los modelos del router IOS que soportan Cisco CP, refiera a los Release Note de Cisco CP.

Configuración del router para ejecutar Cisco CP

Nota: Realice estos pasos para la configuración para ejecutar Cisco CP en un router 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
```

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Router IOS de Cisco 1841 que funciona con la versión de software IOS 12.4(15)T
- 2.1 de la versión del Cisco Configuration Professional (Cisco CP)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Por el ejemplo de este documento, configuran al router como Firewall zona-basado para bloquear el tráfico P2P. El router ZFW tiene dos interfaces, una interfaz del inside(trusted) en la En-zona y una interfaz (untrusted) del exterior en la Hacia fuera-zona. El router ZFW bloquea las aplicaciones P2P tales como edonkey, vía rápida, gnutella y kazaa2 con la acción del registro para el tráfico que está pasando de la En-zona a la Hacia fuera-zona.

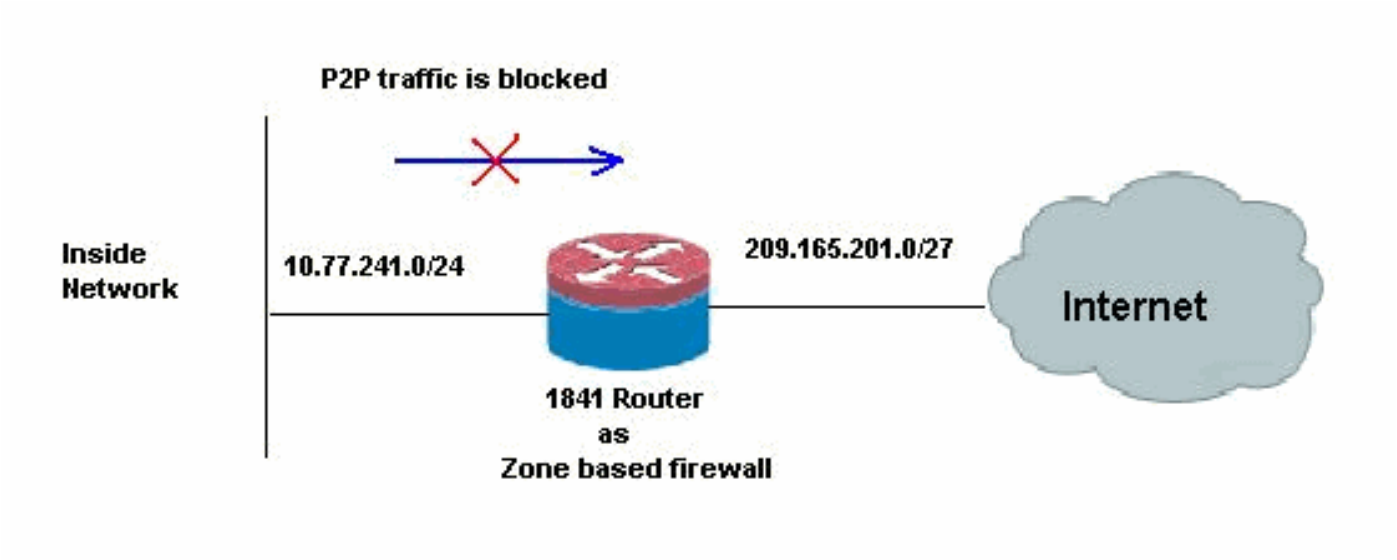
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

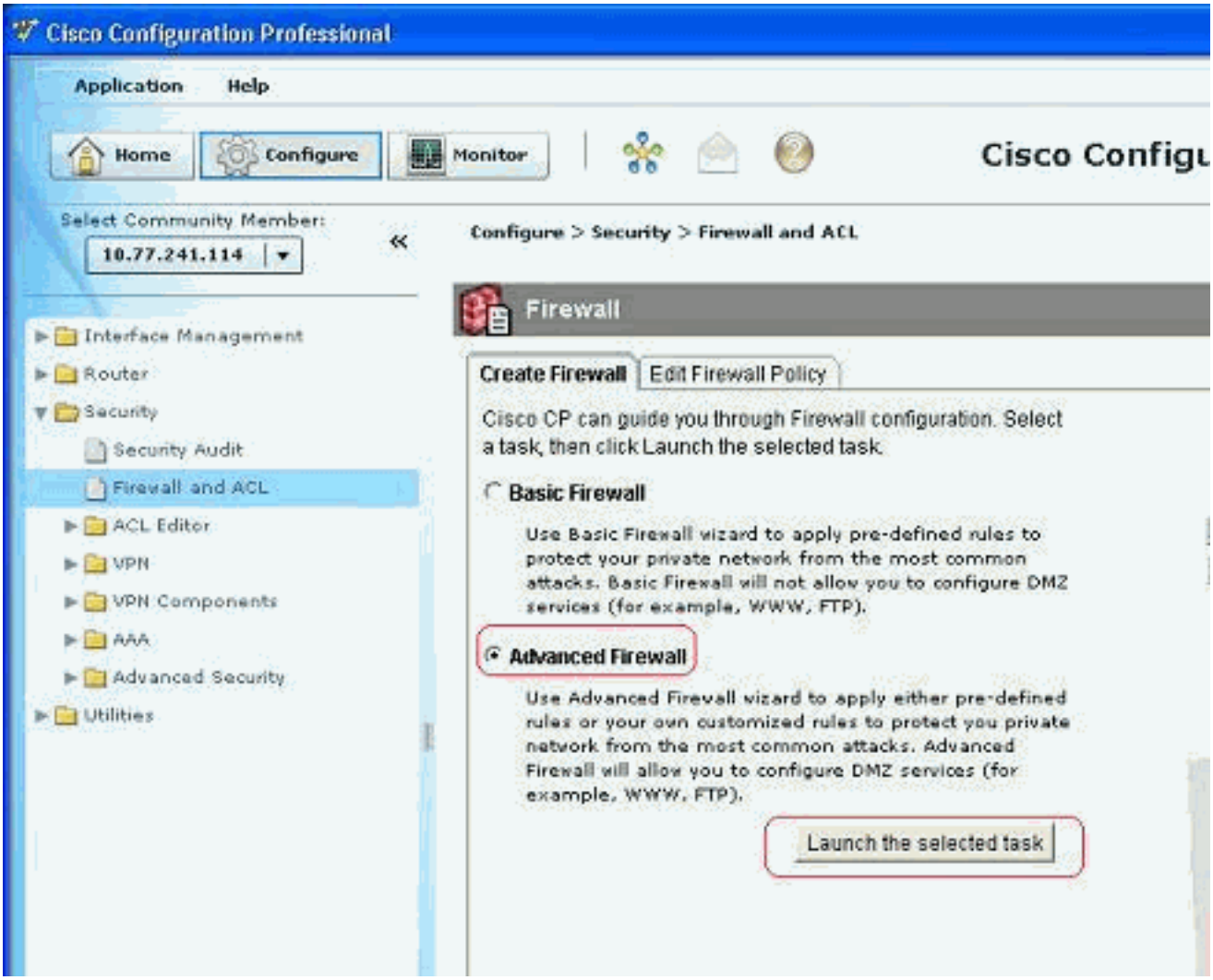


Configuración a través del Cisco Configuration Professional

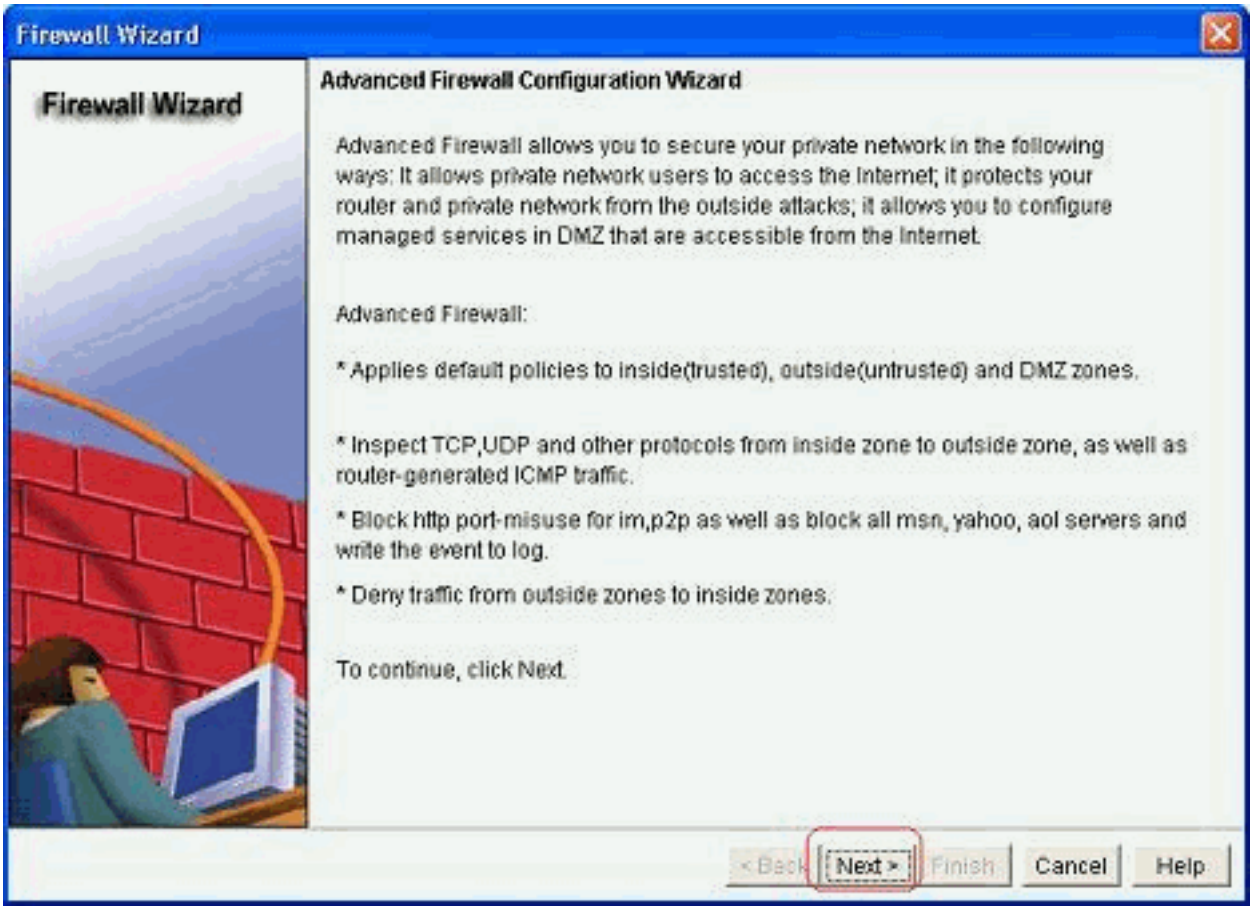
Esta sección contiene el procedimiento paso a paso en cómo utilizar al Asisitente para configurar al router IOS como Firewall zona-basado.

Complete estos pasos:

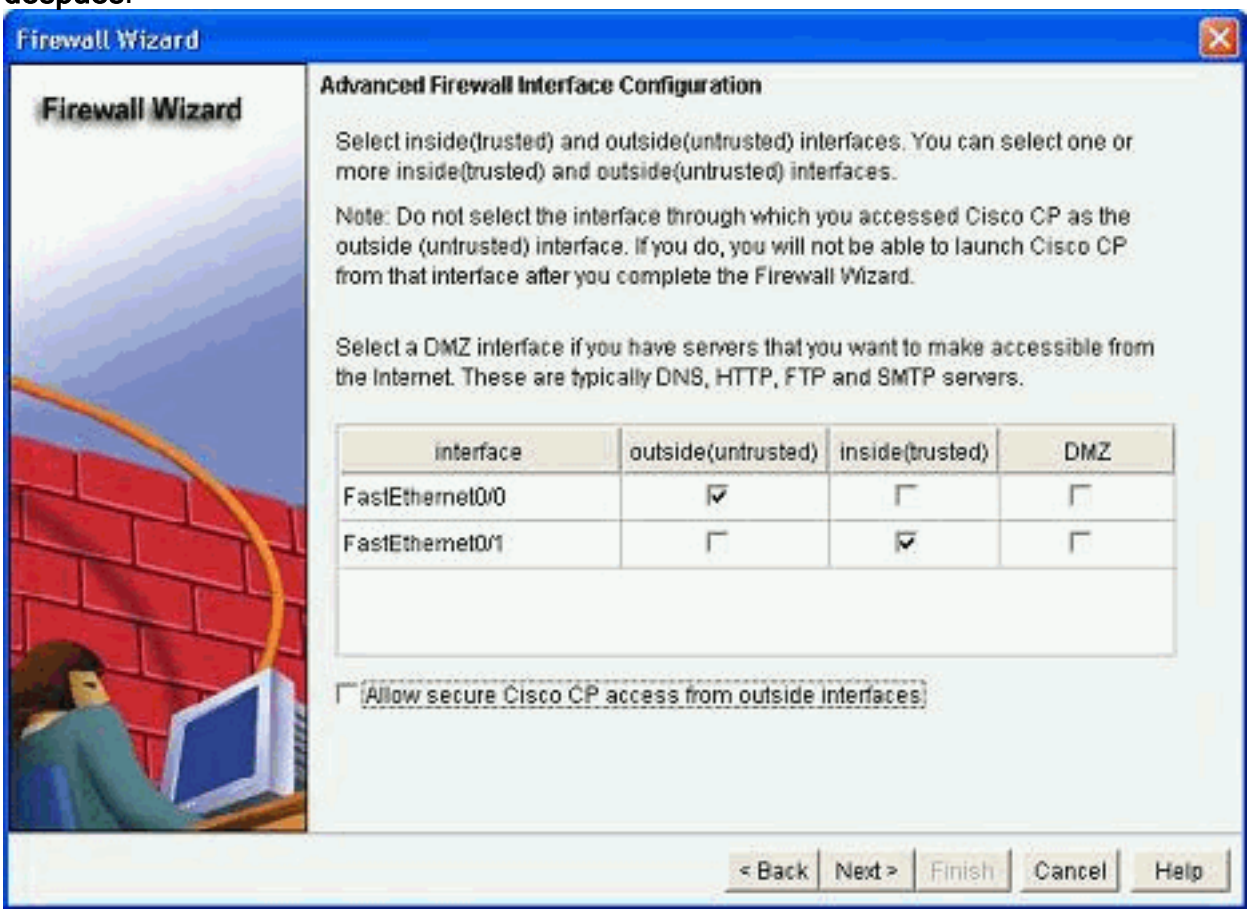
1. Vaya al **> Security (Seguridad) > al Firewall y al ACL de la configuración**. Entonces, elija el botón de radio **avanzado del Firewall**. Haga clic el **lanzamiento la tarea seleccionada**.



2. Esta siguiente pantalla muestra una introducción abreviada sobre el Asisitente del Firewall. Tecleo **al lado del** comienzo que configura el Firewall.



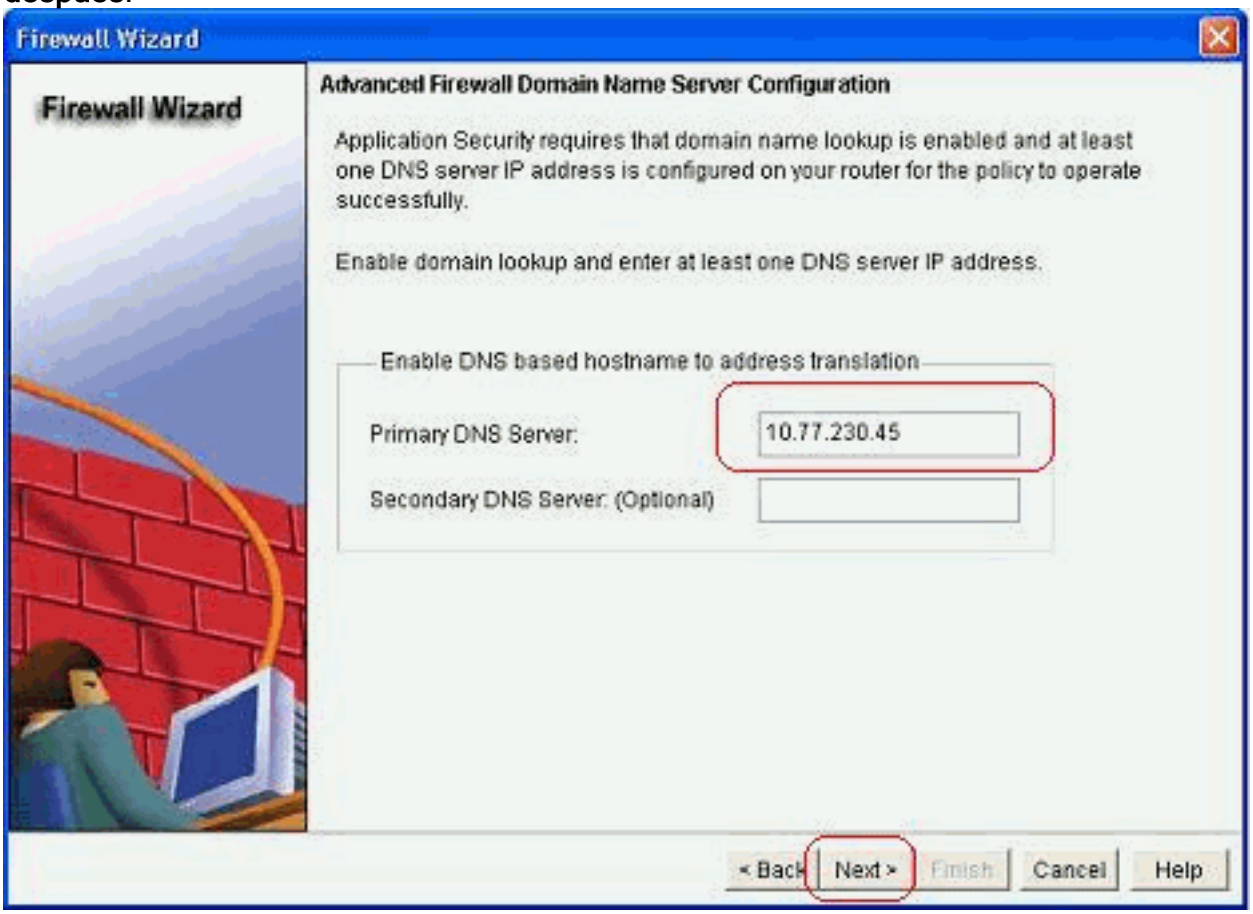
3. Seleccione las interfaces del router para ser zonas de la parte de y haga clic **después**.



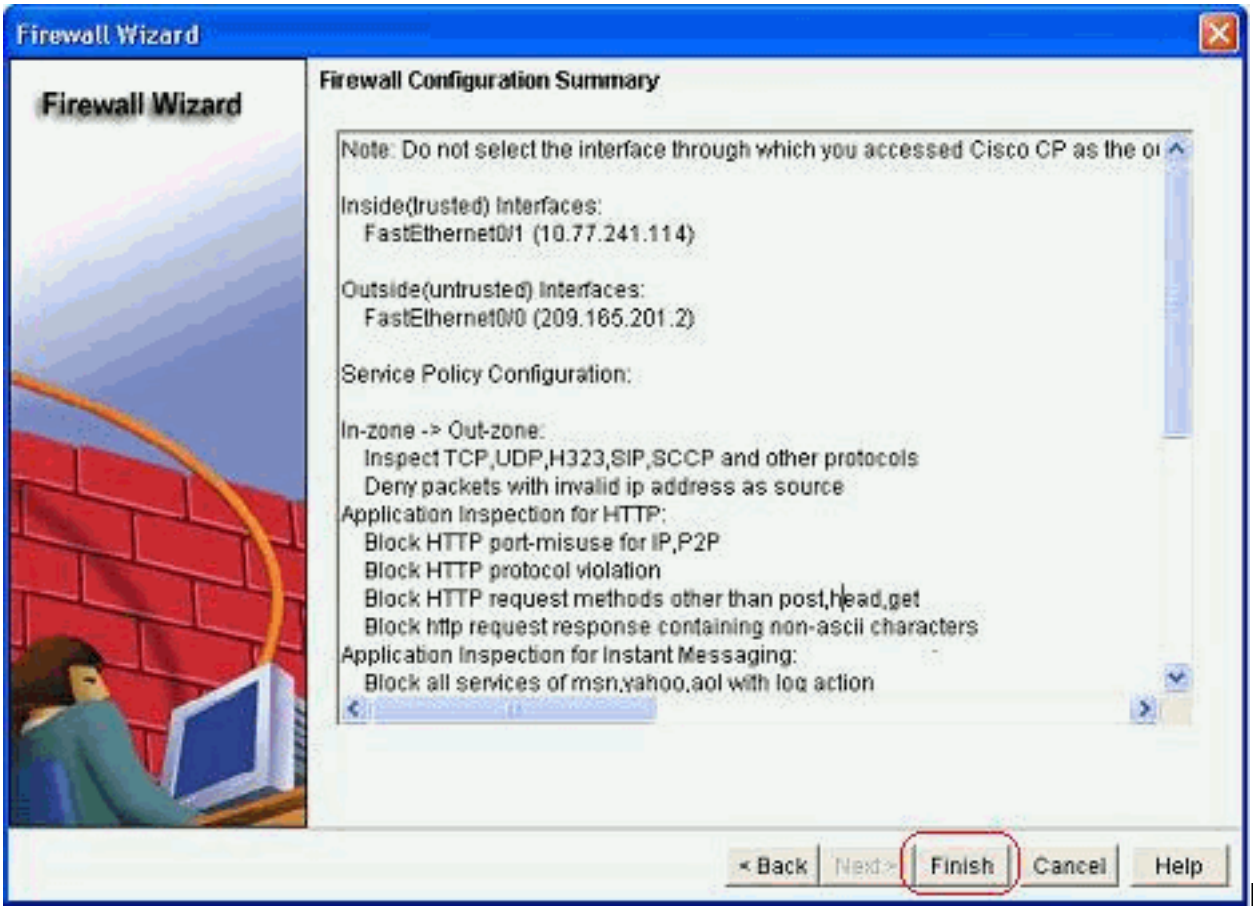
4. La política predeterminada con la gran seguridad junto con el conjunto de comandos se muestra en la próxima ventana. El tecleo **cerca de**

procede.

5. Ingrese a los detalles del servidor DNS y haga clic **después**.

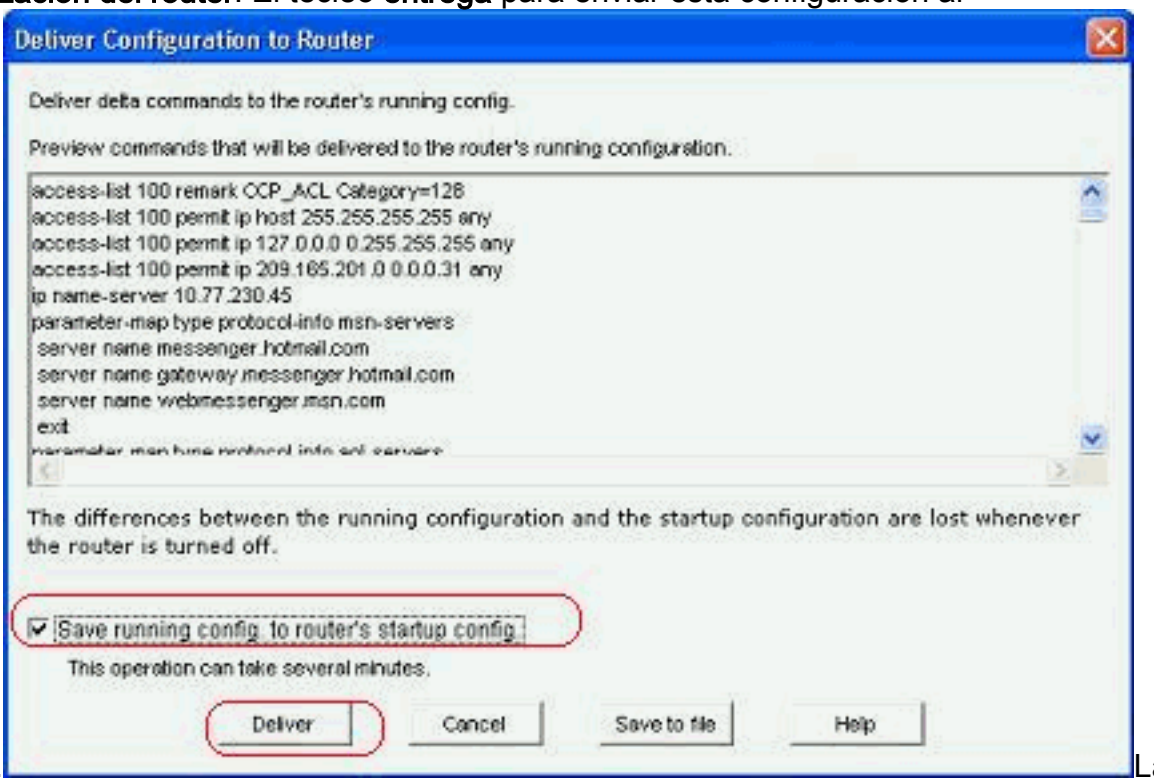


6. Cisco CP proporciona un resumen de la configuración tal como el que está mostrado aquí. Clic en Finalizar para completar la configuración.

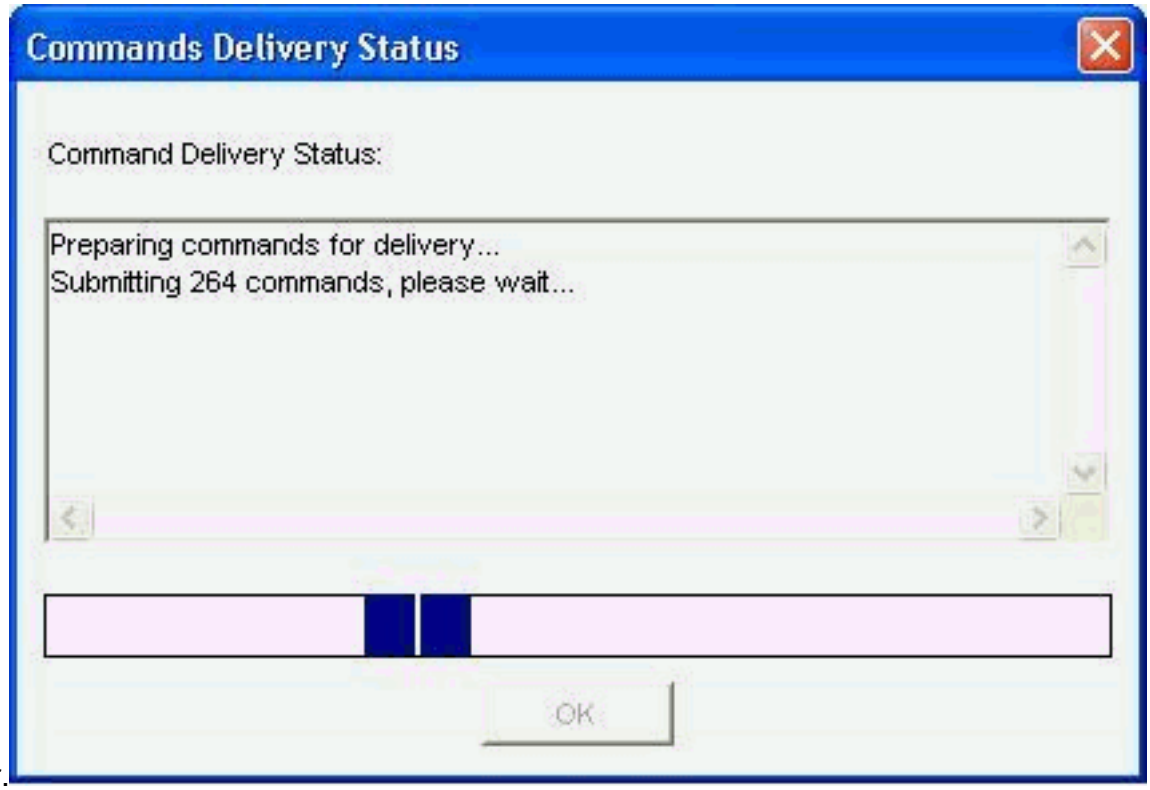


El resumen de la configuración detallada se proporciona en esta tabla. Ésta es la configuración predeterminada según la directiva de gran seguridad de Cisco CP.

7. Marque la **salvaguardia los config corrientes a la** casilla de verificación de la **configuración de inicialización del router**. El tecleo **entrega** para enviar esta configuración al



router. La configuración completa se entrega al router. Esto tarda un cierto tiempo para



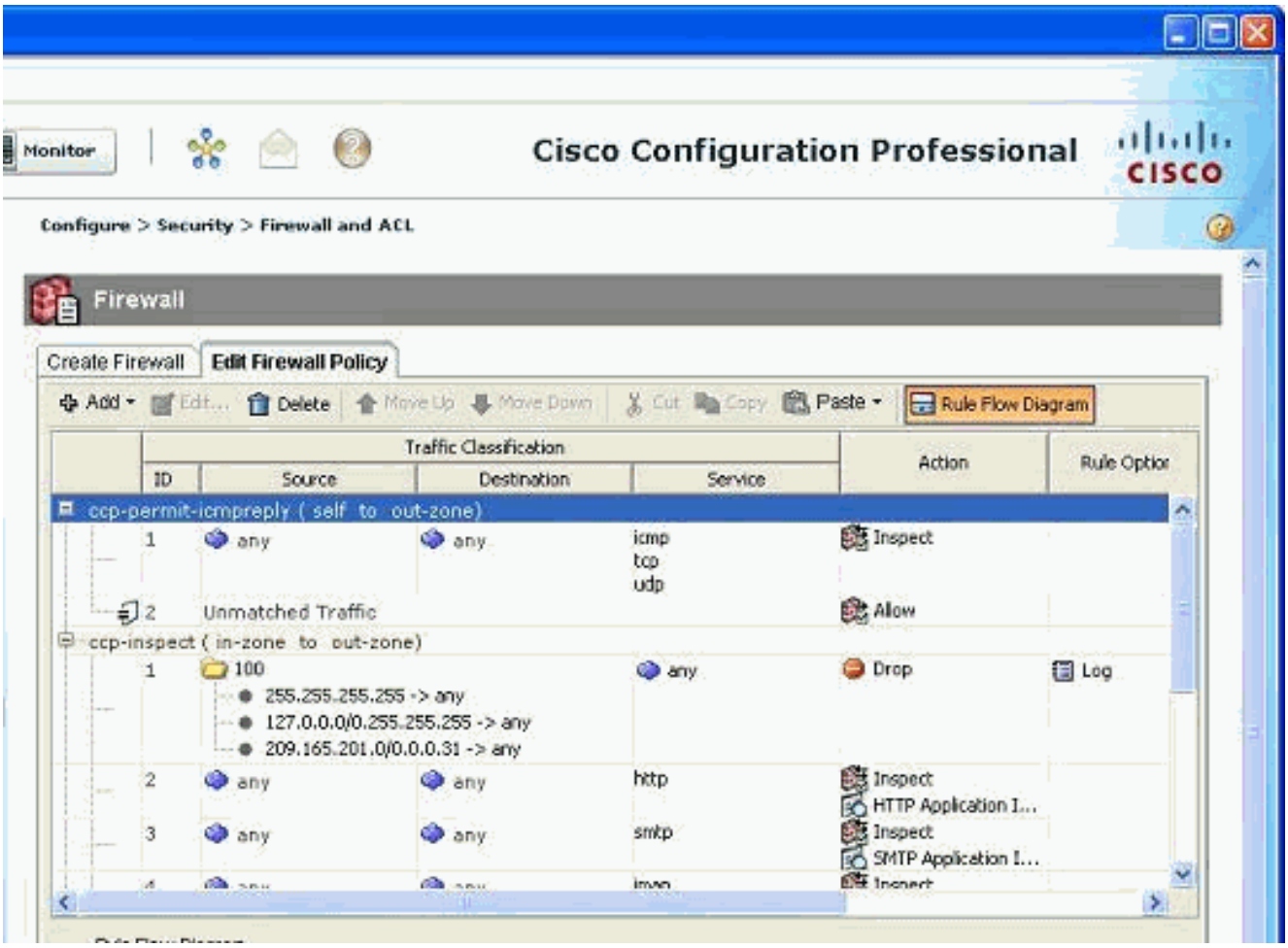
procesar.

8. Haga Click en OK a

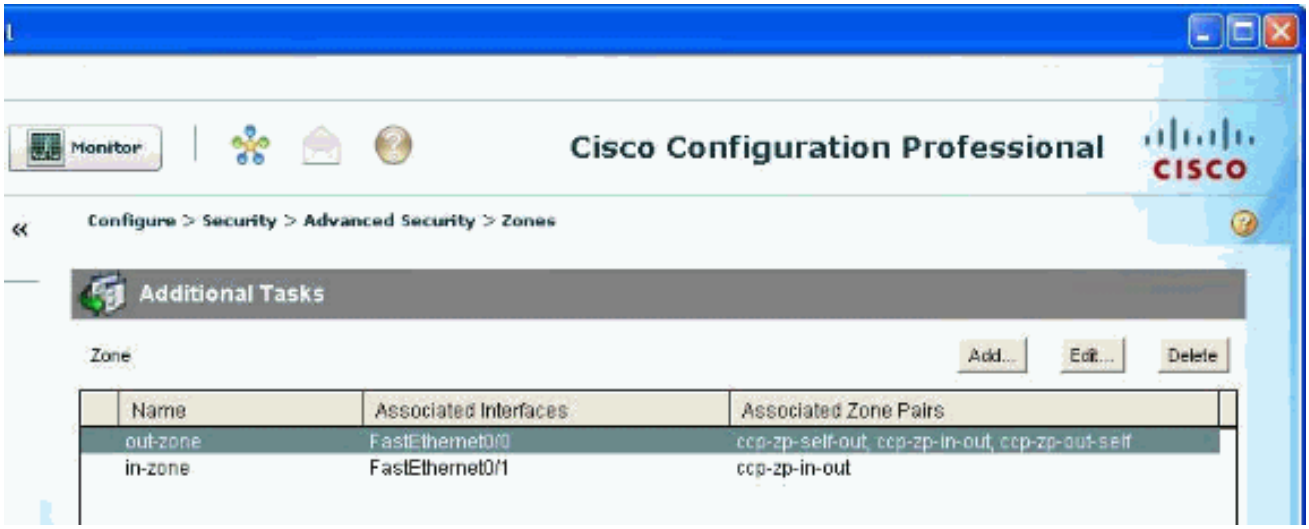
proceder.

9. Haga Click en OK otra

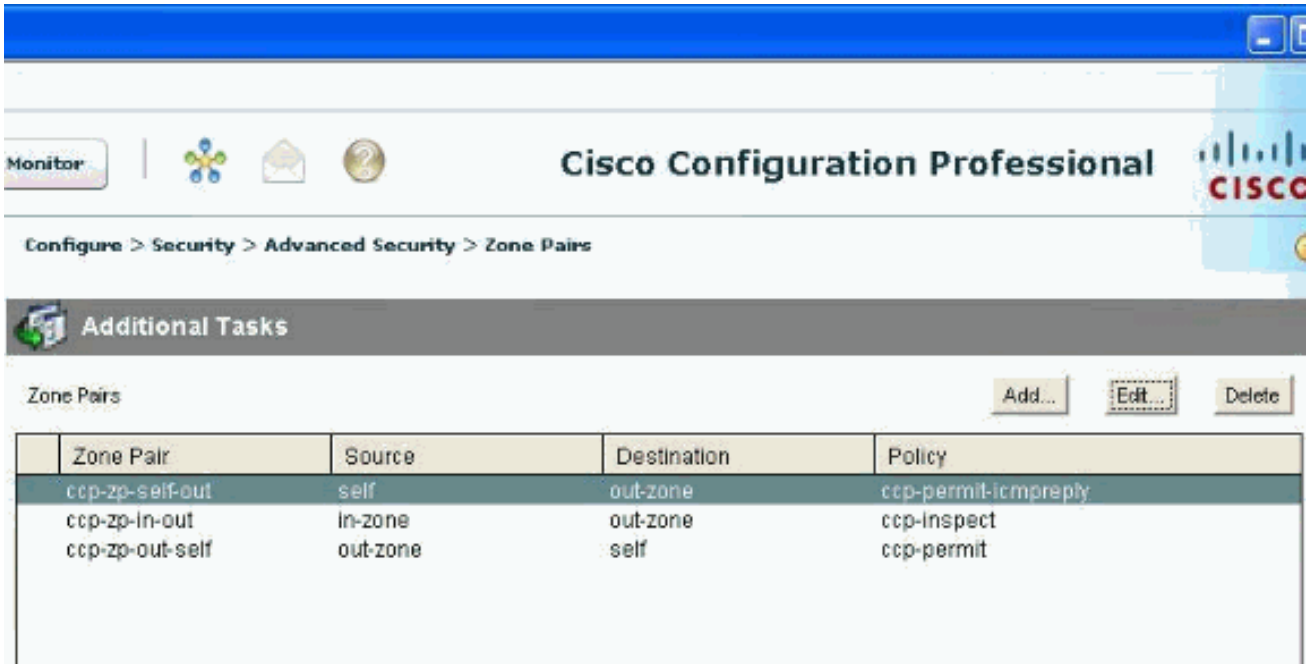
vez.La configuración ahora está en efecto y se muestra como las reglas bajo lengueta de las políticas del
firewall.



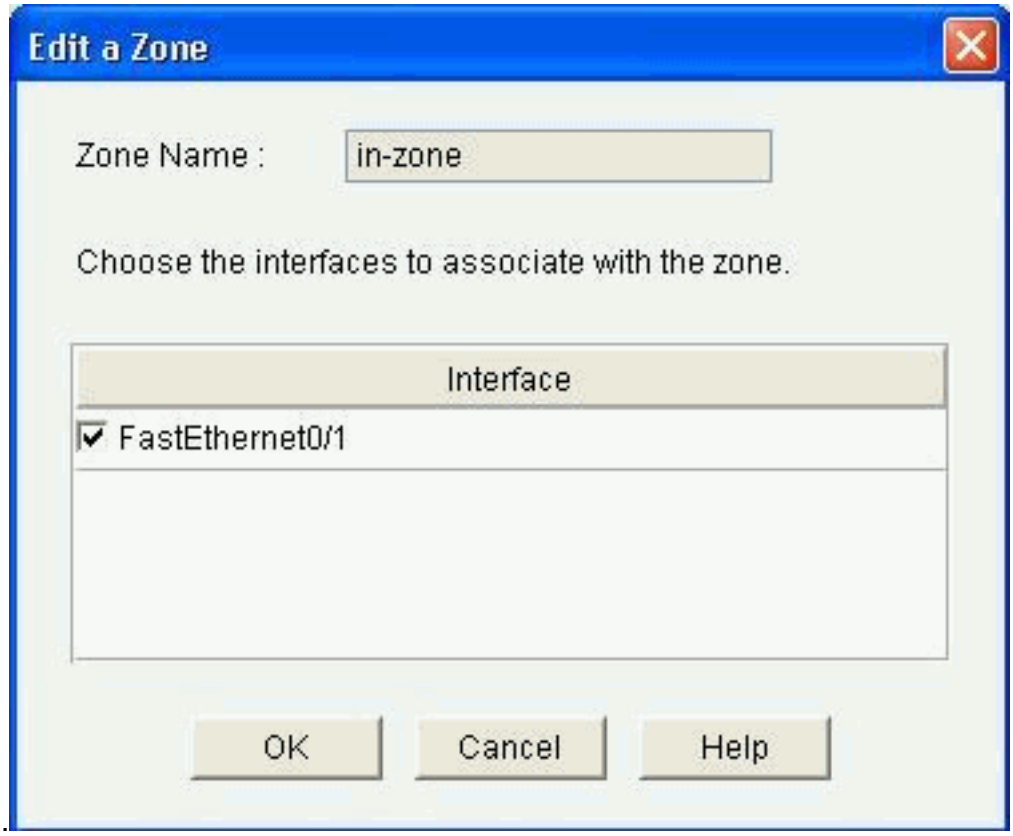
10. Las zonas junto con los pares de la zona que son asociadas pueden ser vistas si usted va al **> Security (Seguridad) > a la Seguridad avanzada > a las zonas de la configuración**. Usted puede también agregar las nuevas zonas haciendo clic **agrega**, o modifica las zonas existentes haciendo clic
edita.



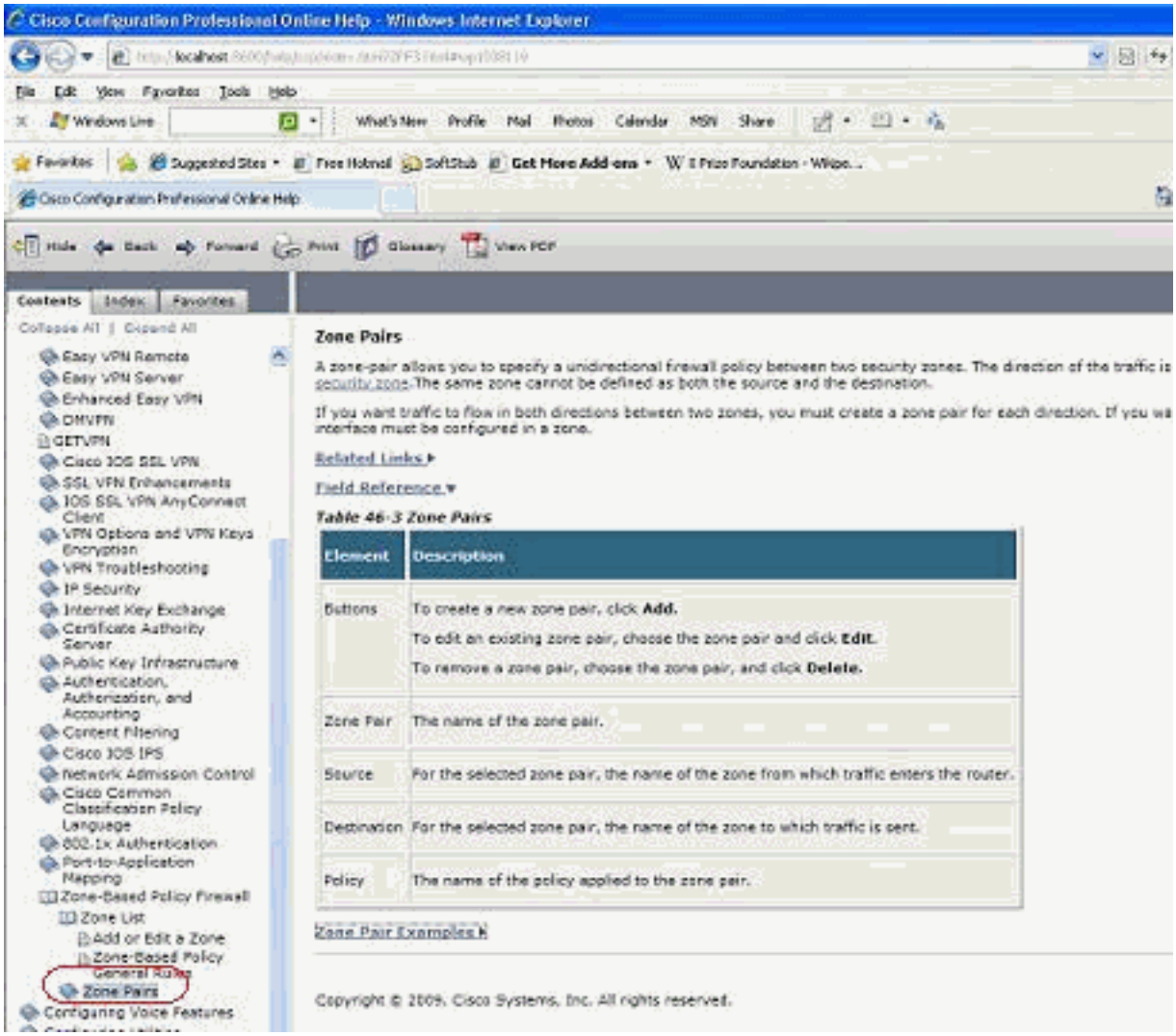
11. Vaya al **> Security (Seguridad) de la configuración > a los pares de la Seguridad avanzada > de la zona** para ver los detalles de los pares de la zona.



La ayuda inmediata en cómo modificarse/agregan/las zonas de la cancelación/los pares de la zona y la otra información relacionada es fácilmente disponible con las páginas web incorporadas en Cisco

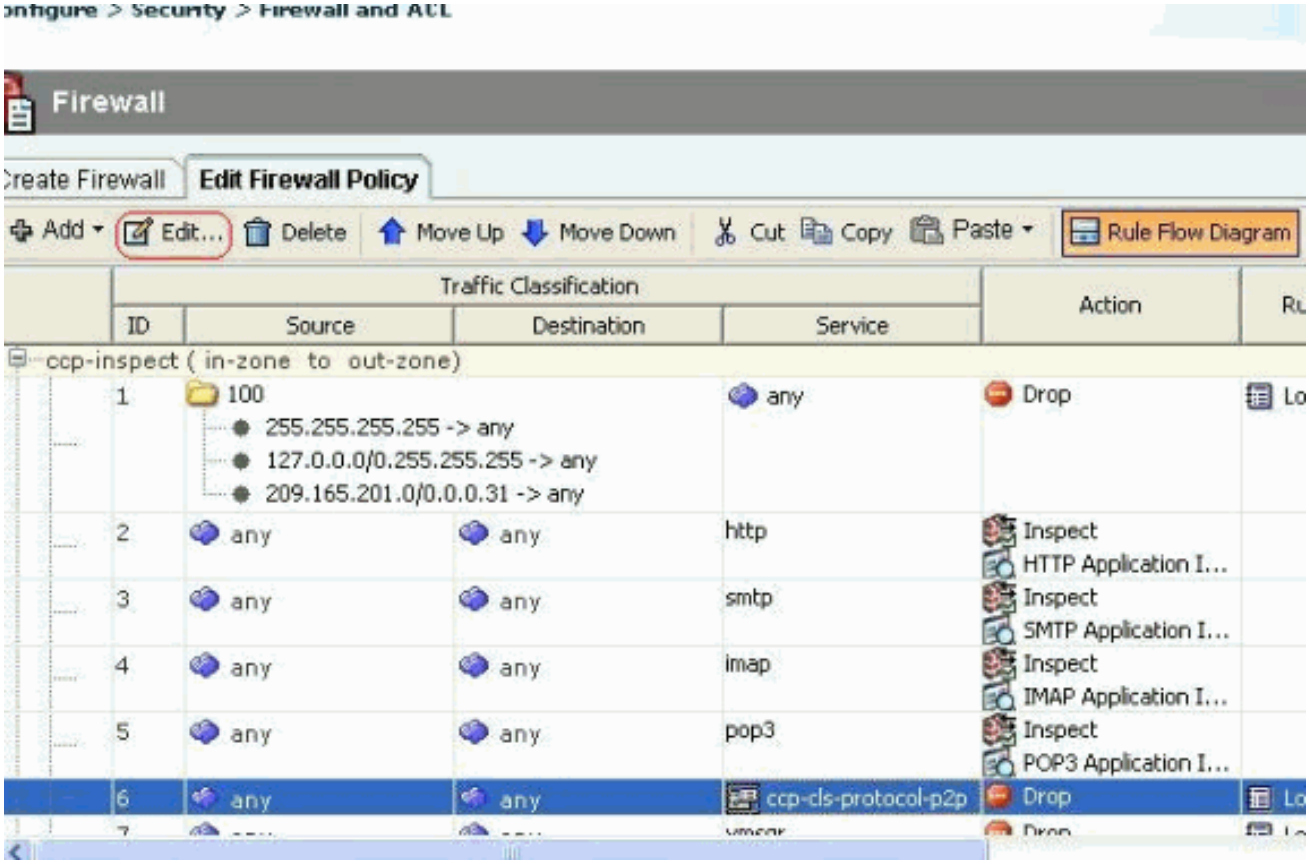


CP.

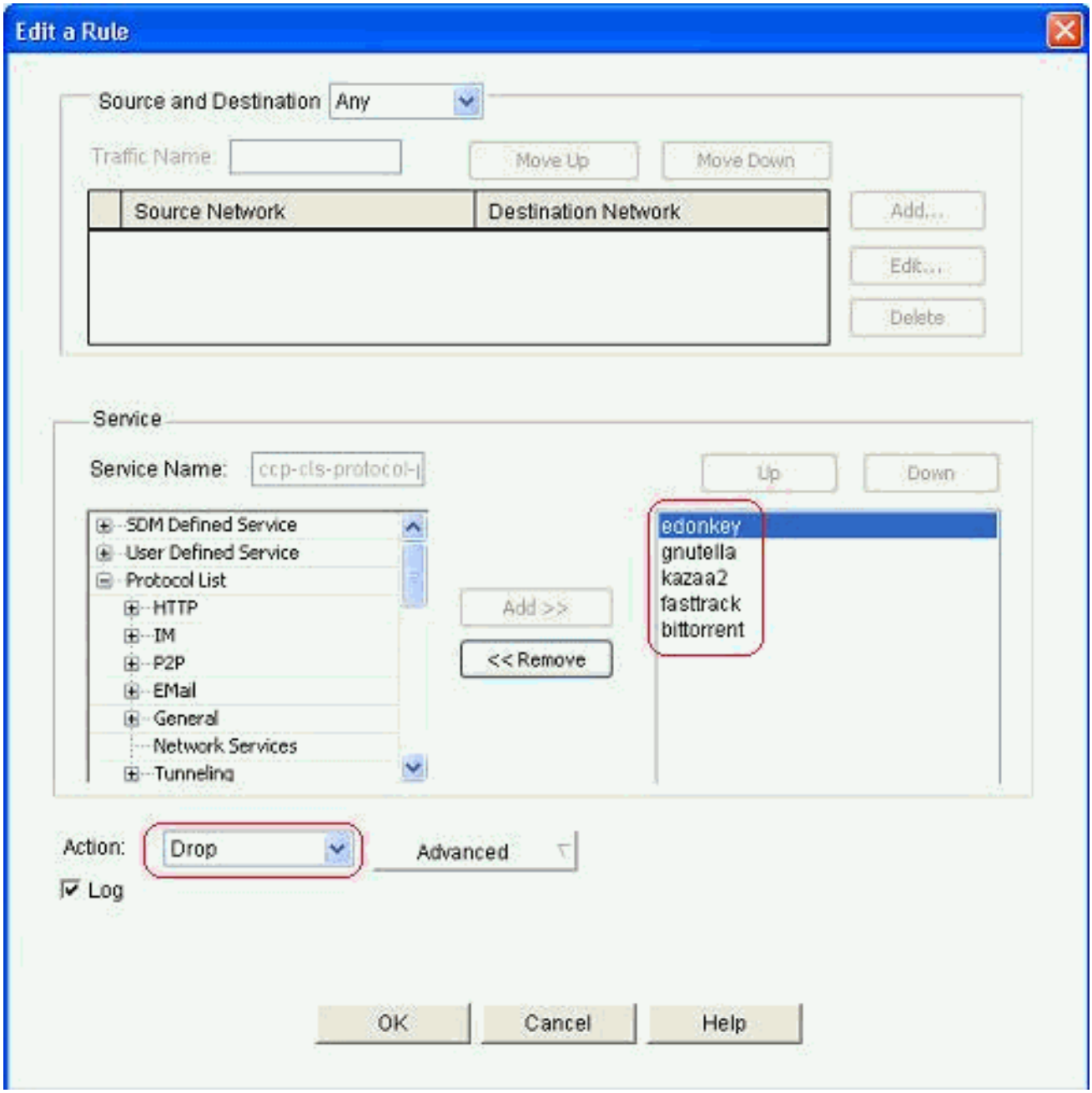


12. Para modificar las aplicaciones específicas a la aplicación P2P de las capacidades del examen con certeza, vaya al **> Security (Seguridad) de la configuración > al Firewall y al ACL**. Entonces, el tecleo **edita las políticas del firewall** y elige la regla respectiva en la

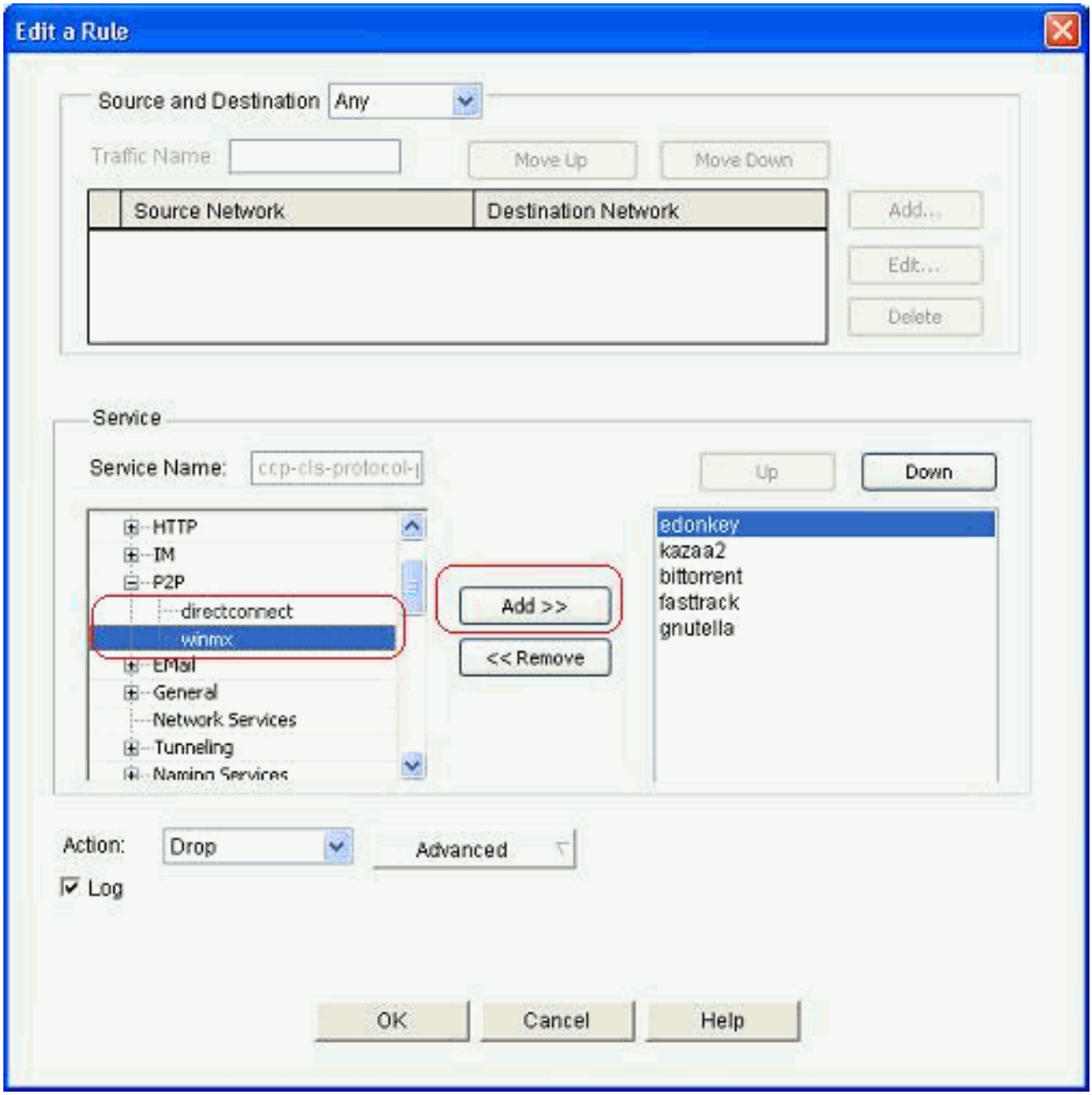
correspondencia de políticas. Haga clic en **Editar**.

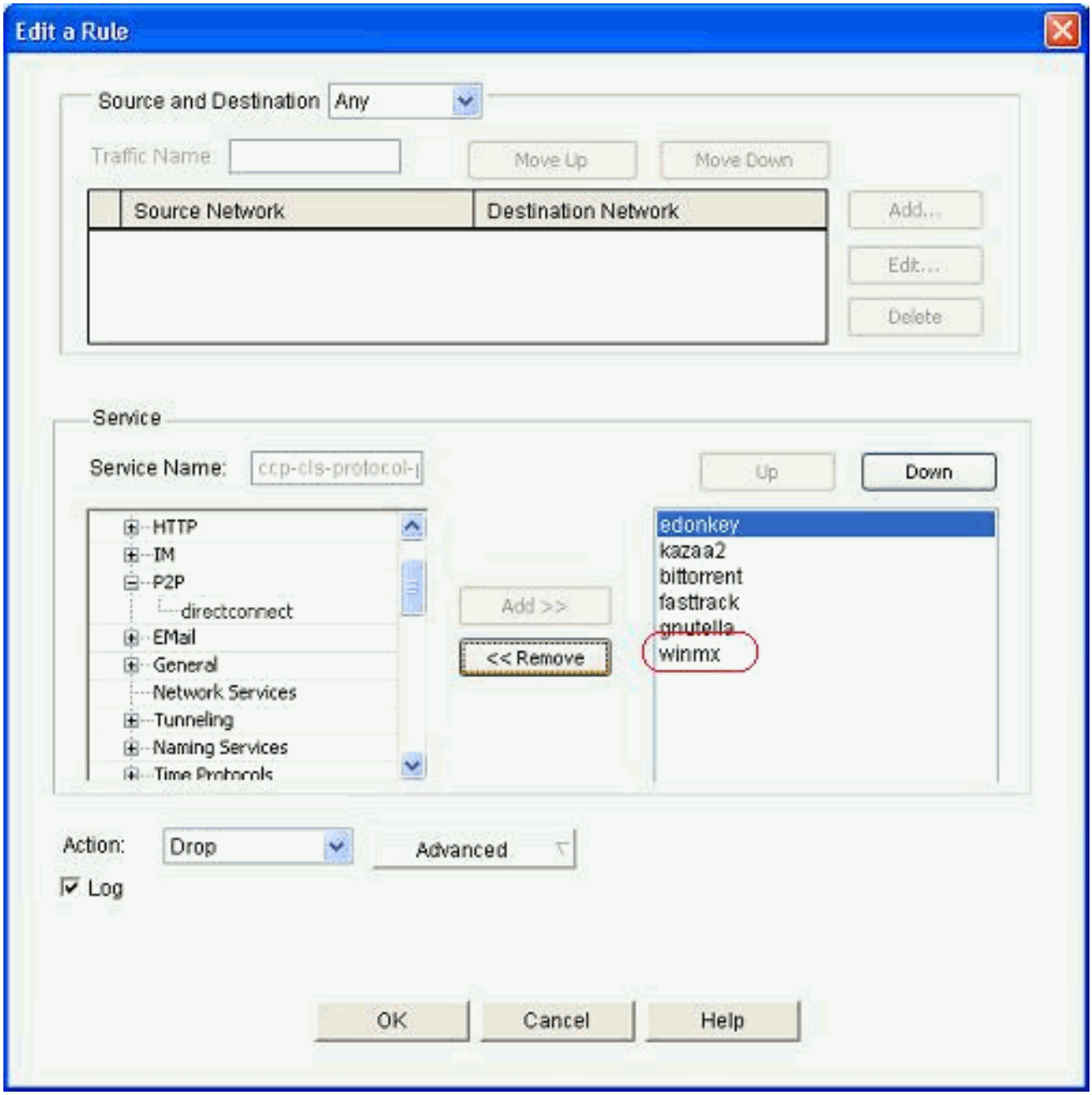


Esto muestra a aplicaciones actuales P2P que por abandono configuración bloqueada.

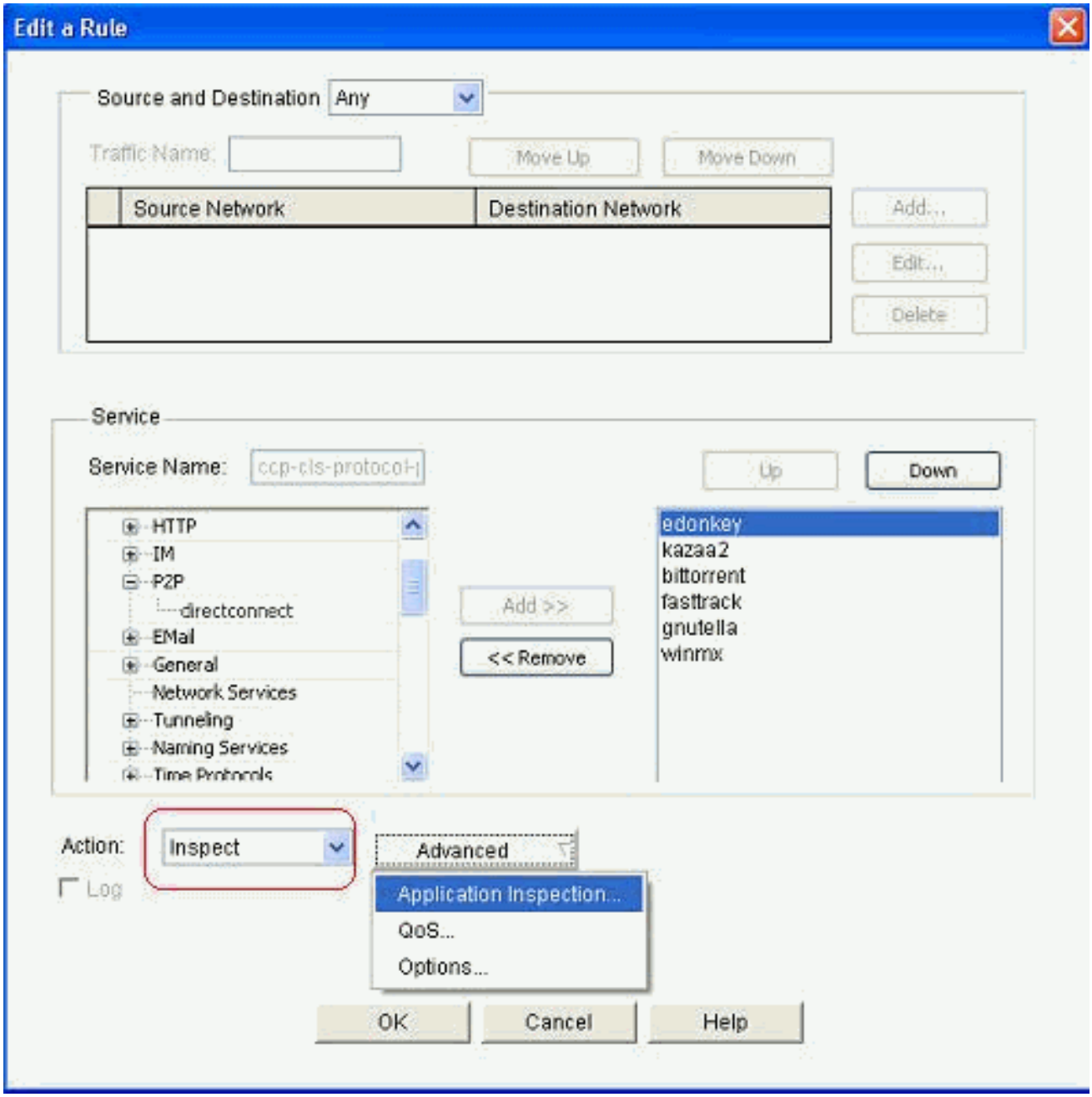


13. Usted puede utilizar el agregar y los botones Remove Button a agregar/quitan las aplicaciones específicas. Este tiro de pantalla muestra cómo agregar la aplicación del winmx para bloquear
eso.


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

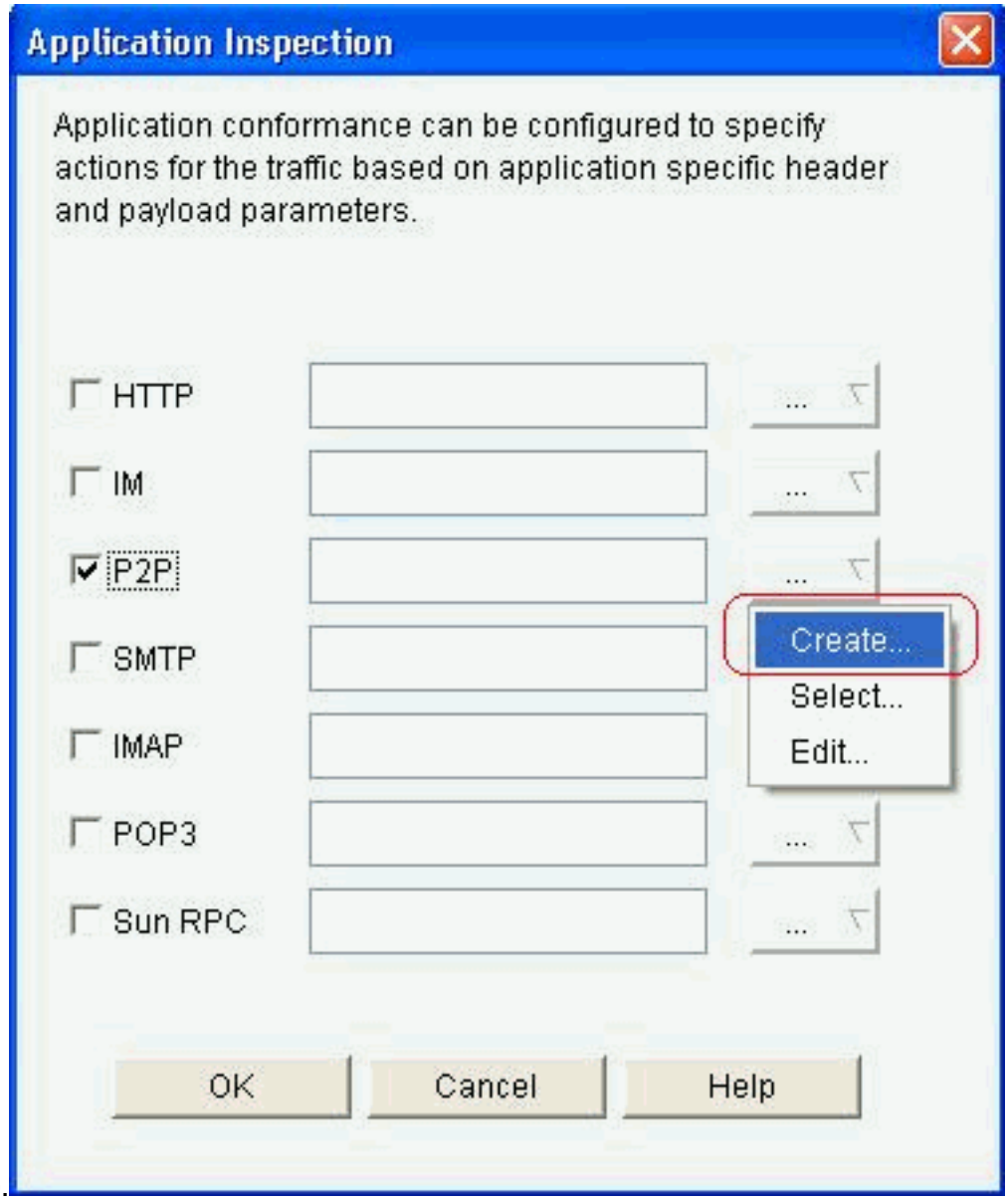


14. En vez de elegir la acción de descarte, usted puede también elegir la acción de la inspección para aplicar diversas opciones para la inspección de paquetes profunda.



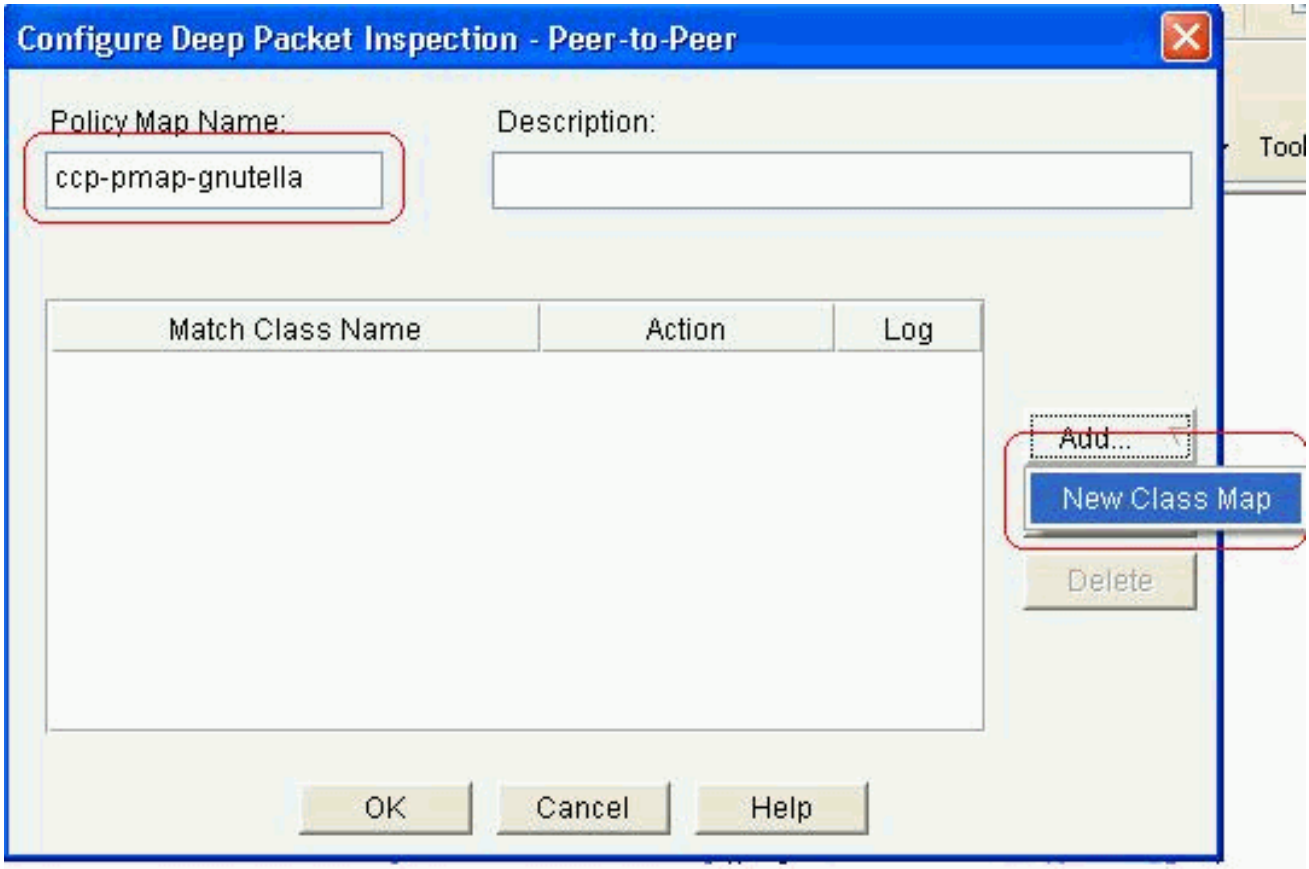
El examen P2P ofrece la capa 4 y la capa 7 directivas para el tráfico de aplicación. Esto significa que ZFW puede proporcionar la inspección con estado básica al permit or deny el tráfico, así como el control granular de la capa 7 en las actividades específicas en los diversos protocolos, para permitir ciertas actividades de la aplicación mientras que se niegan otras. En esta Inspección de la aplicación, usted puede aplicar diversos tipos de exámenes específicos del nivel de la encabezado para las aplicaciones P2P. Un ejemplo para el gnutella se muestra después.

15. Marque la opción **P2P** y el tecleo **crea** para crear un nuevo directiva-mapa para

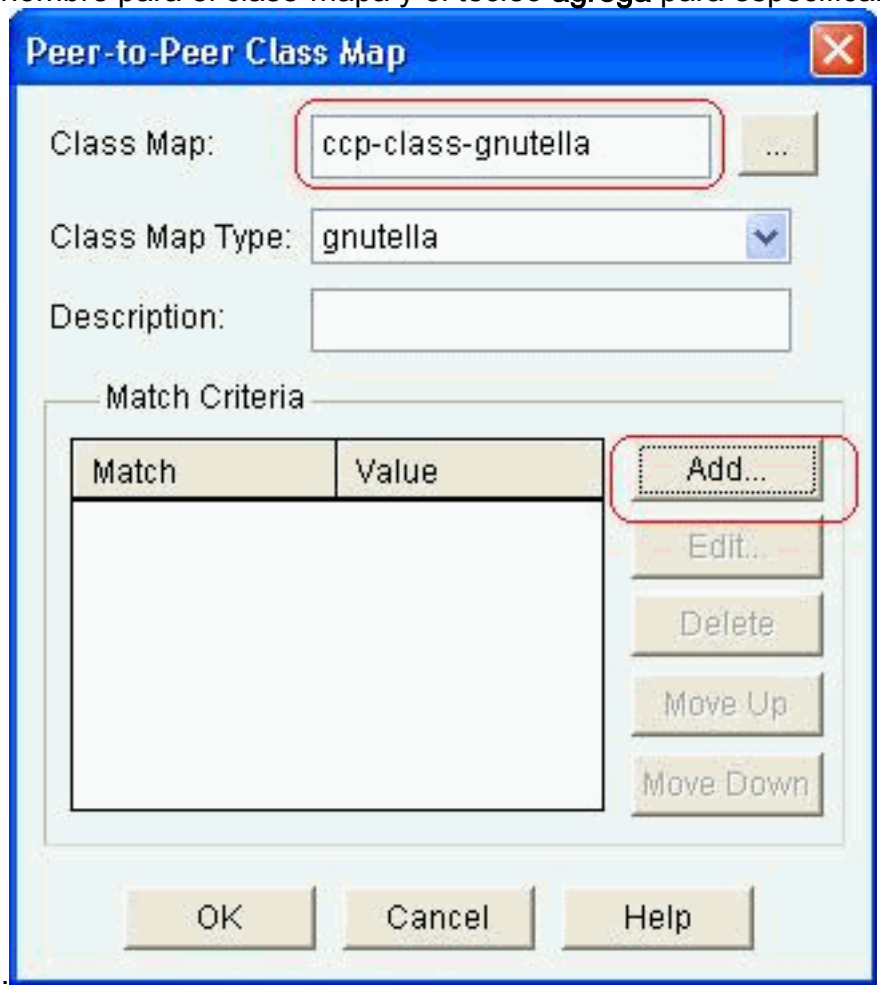


esto.

16. Cree un nuevo directiva-mapa para la inspección de paquetes profunda para el protocolo del gnutella. El tecleo **agrega** y después elige el **nuevo mapa de la clase**.

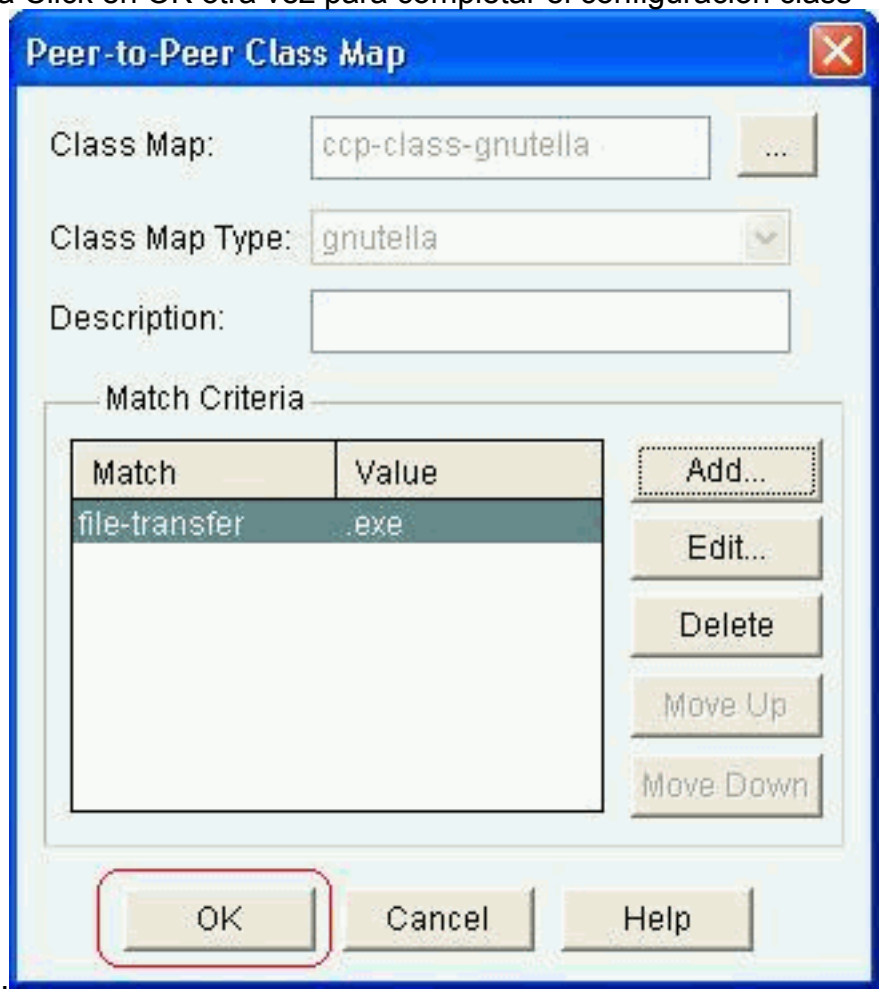


17. Dé un nuevo nombre para el clase-mapa y el tecleo **agrega** para especificar los criterios de concordancia.

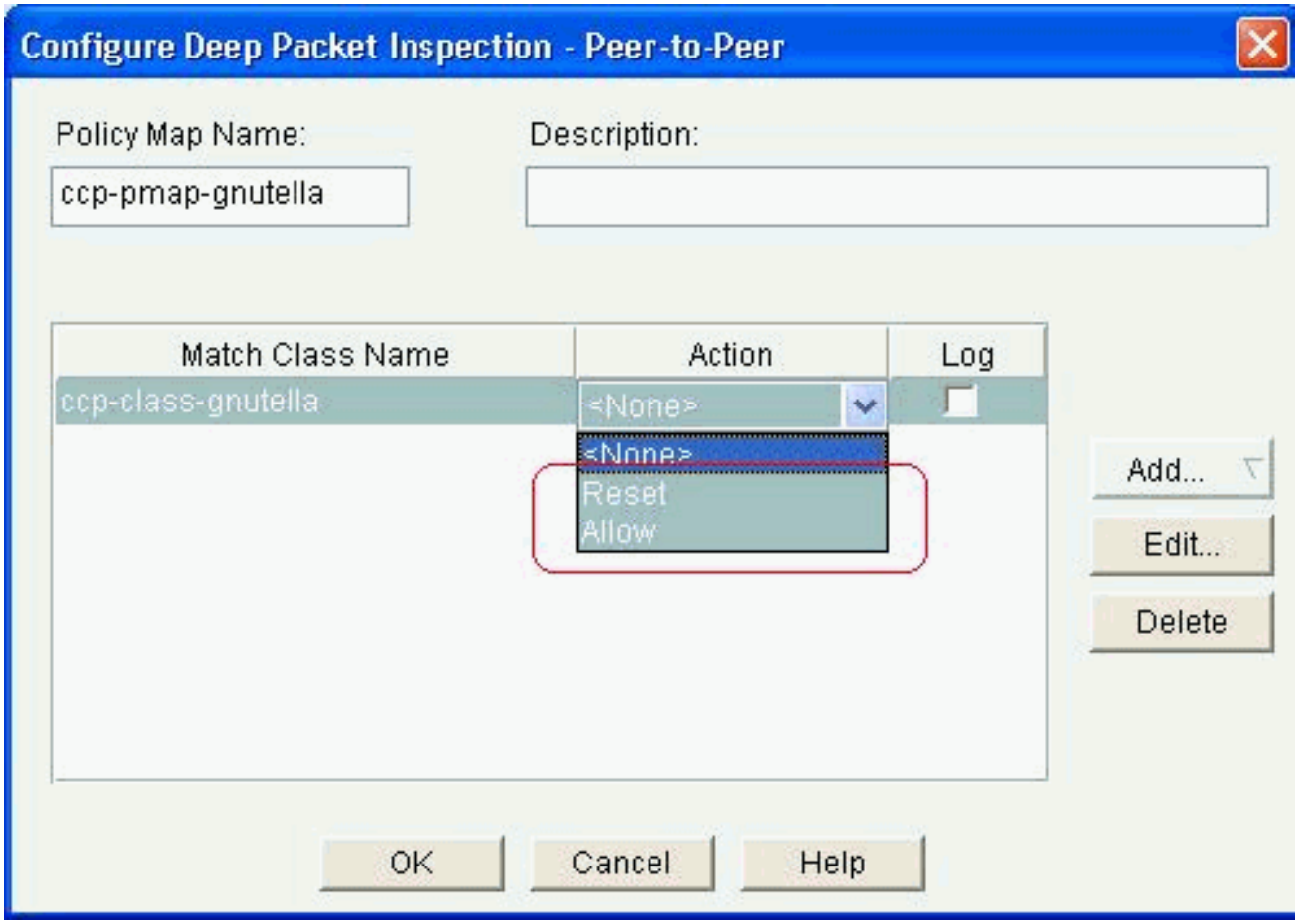


18. Utilice la transferencia de archivos pues el criterio de la coincidencia y la cadena usados es .exe. Esto indica que todas las conexiones de la transferencia de archivos del gnutella que contienen la correspondencia de cadenas del .exe para la política de tráfico. Haga clic en

OK. 

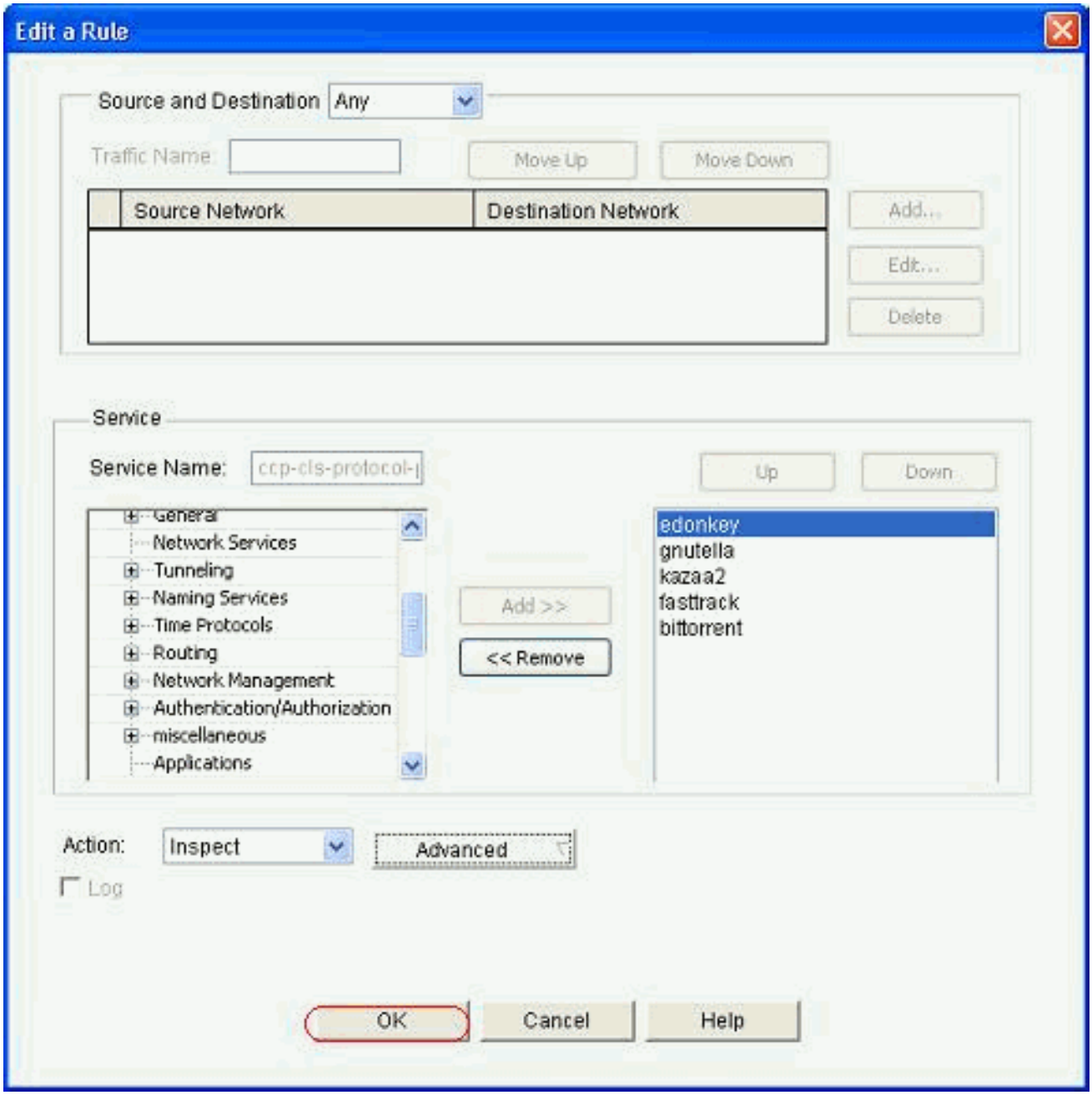
19. Haga Click en OK otra vez para completar el configuración class-map. 

20. Elija la **restauración** o **permita la** opción, que depende de la política de seguridad de su compañía. Haga Click en OK para confirmar la acción con el directiva-mapa.



De esta misma manera usted puede agregar otras correspondencias de políticas para implementar las características profundas del examen para otros protocolos P2P especificando diversas expresiones normales como el criterio del emparejamiento.**Nota:** Las aplicaciones P2P son determinado difíciles de detectar, como resultado del comportamiento de la “puerto-lupulización” y de otros trucos para evitar la detección, así como de los problemas introducidos por los cambios y las actualizaciones frecuentes a las aplicaciones P2P que modifican los comportamientos de los protocolos. ZFW combina la inspección con estado nativa del Firewall con capacidades del tráfico-reconocimiento s del Network-Based Application Recognition (NBAR) las 'para entregar el control de la aplicación P2P.**Nota:** La Inspección de la aplicación P2P ofrece las capacidades específicas a la aplicación para un subconjunto de las aplicaciones soportadas por el examen de la capa 4:edonkeyvía rápidagnutellakazaa2**Nota:** Actualmente, ZFW no tiene una opción para examinar el tráfico de aplicación “bittorrent”. Los clientes de BitTorrent comunican generalmente con los perseguidores (Servidores del directorio del par) vía el HTTP que se ejecuta en algún puerto no estándar. Éste es típicamente TCP 6969, pero usted puede ser que necesite marcar el puerto torrente-específico del perseguidor. Si usted desea permitir BitTorrent, el mejor método para acomodar el puerto adicional es configurar el HTTP como uno de los protocolos de la coincidencia y agregar TCP 6969 al HTTP usando este comando ip port-map: **puerto tcp 6969 HTTP del port-map del IP**. Usted necesitará definir el HTTP y bitTorrent como los criterios de concordancia aplicados en el clase-mapa.

21. Haga Click en OK para completar la configuración avanzada del examen.

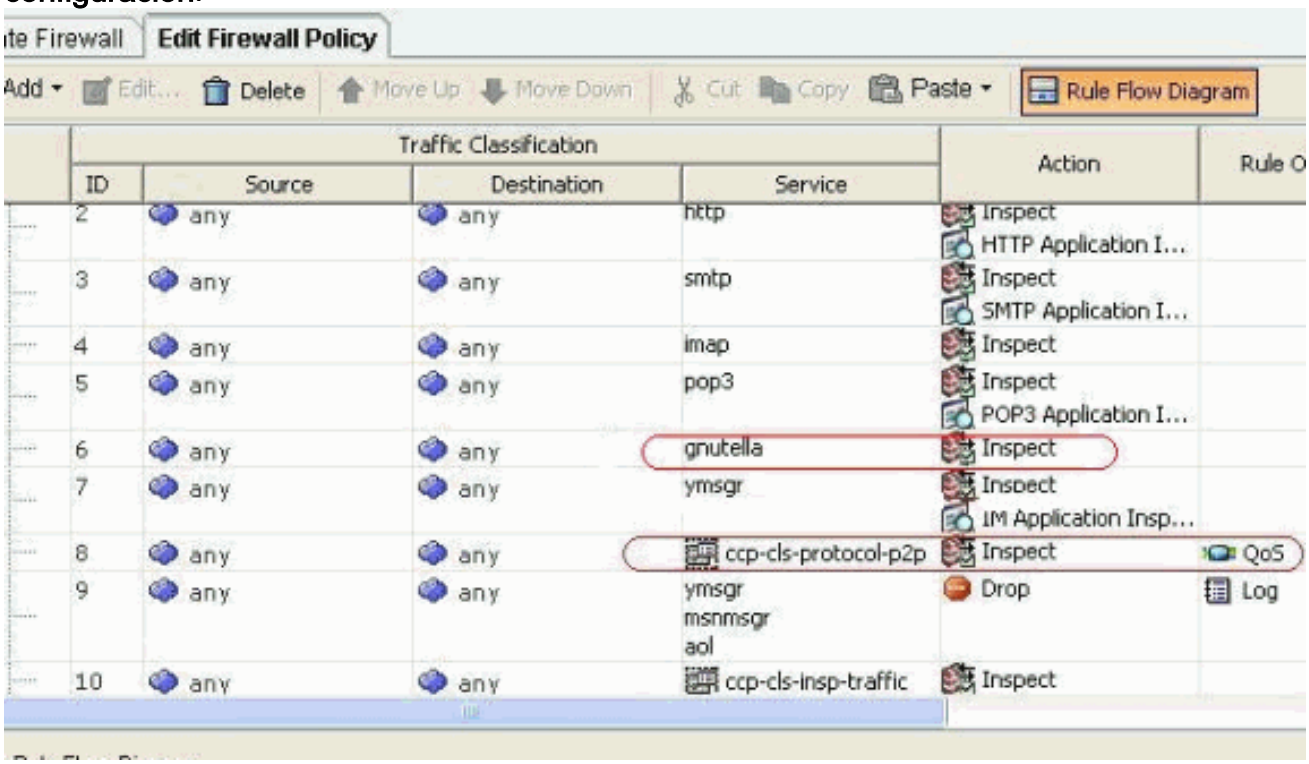


El conjunto de comandos correspondiente se entrega al router.

22. Haga Click en OK a completar copiando el conjunto de comandos al

router.

23. Usted puede observar las nuevas reglas el ocurrir de la lengueta de las políticas del firewall del editar bajo el **> Security (Seguridad) > el Firewall y el ACL de la configuración**.



Comando line configuration del router ZFW

La configuración en la sección anterior de Cisco CP da lugar a esta configuración en el router ZFW:

Router 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#
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **El tipo del directiva-mapa de** ZBF-Router#show **examina las sesiones de los zona-pares** — Visualiza el tiempo de ejecución examinan las estadísticas del directiva-mapa del tipo para saber si hay todos los pares existentes de la zona.

Información Relacionada

- Diseño del Firewall de la directiva y guía Zona-basados de la aplicación
- Ejemplo virtual clásico y Zona-basado del Firewall Cisco IOS del Firewall de la configuración de aplicación
- Home Page del Cisco Configuration Professional
- Guía del usuario del Cisco Configuration Professional
- Soporte Técnico y Documentación - Cisco Systems