Cisco Configuration Professional: зональный узел блокирования межсетевого экрана для пиринга с примером конфигурирования трафика

Содержание

Введение

Этот документ предоставляет пошаговый подход для настройки маршрутизатора Cisco IOS как зонального межсетевого экрана для блокирования Одноранговый (P2P) трафик при помощи Усовершенствованного мастера Конфигурации межсетевого экрана в Cisco Configuration Professional (CP Cisco).

Межсетевой экран политики на основе зон (также известный как межсетевой экран зональной политики или ZFW) обладает измененной конфигурацией межсетевого экрана: вместо старой модели на основе интерфейса теперь применяется более гибкая и понятная зональная модель. Интерфейсы присваиваются зонам, а политика проверки — трафику, передаваемому между зонами. Политика промежуточной зоны предлагает значительную гибкость и глубину детализации. Поэтому другой политике проверки можно примениться к несколько хостов группы, связанные с интерфейсом того жя маршрутизатор. Зоны устанавливают границы безопасности вашей сети. Зона определяет границу, где трафик, переходящий в другой регион вашей сети, подвержен ограничениям политики. Политика ZFW, выбранная по умолчанию между зонами, состоит в запрете всего трафика. Если ни одна политика не задана явным образом, блокируется весь трафик, перемещающийся между зонами.

Приложения P2P являются некоторыми наиболее широко использованными приложениями

в Интернете. Сети P2P могут действовать как conduit для злонамеренных угроз, таких как черви, предлагая легкий путь вокруг межсетевых экранов и вызывая опасения по поводу конфиденциальности и безопасности. Программное обеспечение Cisco IOS версии 12.4(9)T представило поддержку ZFW приложений P2P. Контроль P2P предлагает политику Уровня 4 и Уровня 7 для трафика приложения. Это означает, что ZFW может предоставить основную проверку трафика потоком для permit or deny трафика, а также гранулированного контроля за Уровнем 7 на определенных действиях в различных протоколах, так, чтобы определенные активности приложения были позволены, в то время как запрещены другие.

CP Cisco предлагает понятный, пошаговый подход для настройки Маршрутизатора IOS как зонального межсетевого экрана при помощи Усовершенствованного мастера Конфигурации межсетевого экрана.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Маршрутизатор IOS должен иметь версию программного обеспечения как 12.4 (9) T или позже.
- Для моделей Маршрутизатора IOS, которые поддерживают CP Cisco, обратитесь к Комментариям к выпуску CP Cisco.

Конфигурация маршрутизатора для выполнения CP Cisco

Примечание: Выполните эти действия настройки для выполнения CP Cisco на маршрутизаторе 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
```

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Маршрутизатор IOS Cisco 1841, который выполняет Выпуск ПО IOS 12.4 (15) T
- Cisco Configuration Professional (CP Cisco) выпуск 2.1

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

Для примера этого документа маршрутизатор настроен как зональный межсетевой экран для блокирования трафика P2P. Маршрутизатор ZFW имеет два интерфейса, внутренний (доверяемый) интерфейс в B зоне и внешний (недоверяемый) интерфейс в Зональном. Маршрутизатор ZFW блокирует приложения P2P, такие как edonkey, fasttrack, gnutella и kazaa2 с регистрацией действия для трафика, который проходит от B зоне до Зонального.

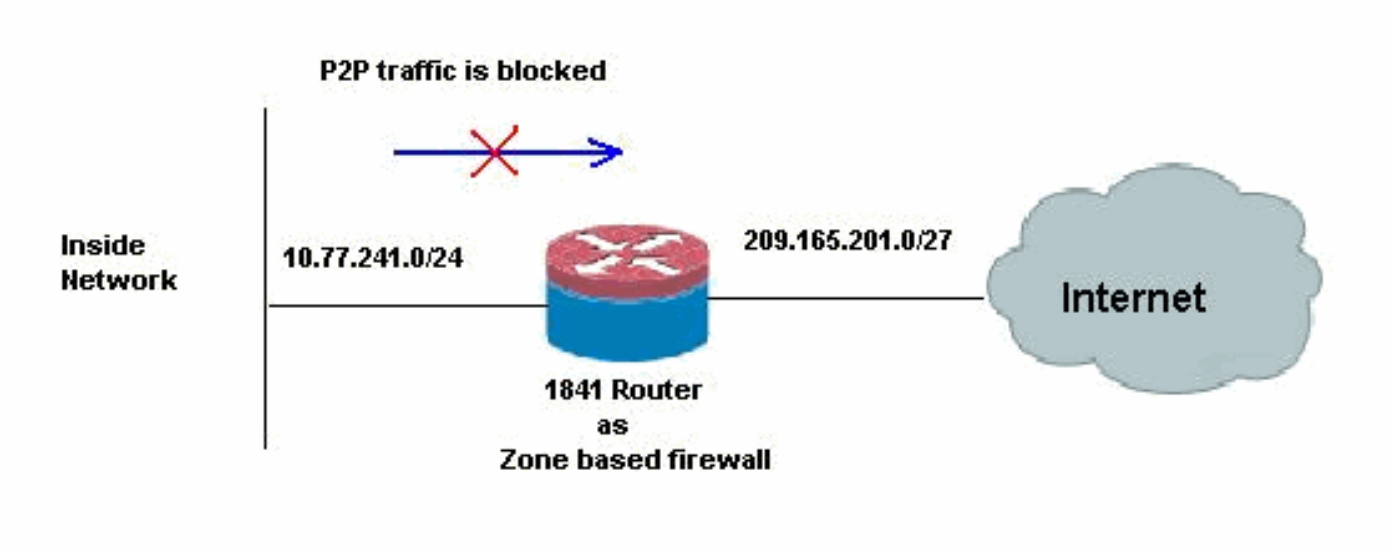
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:



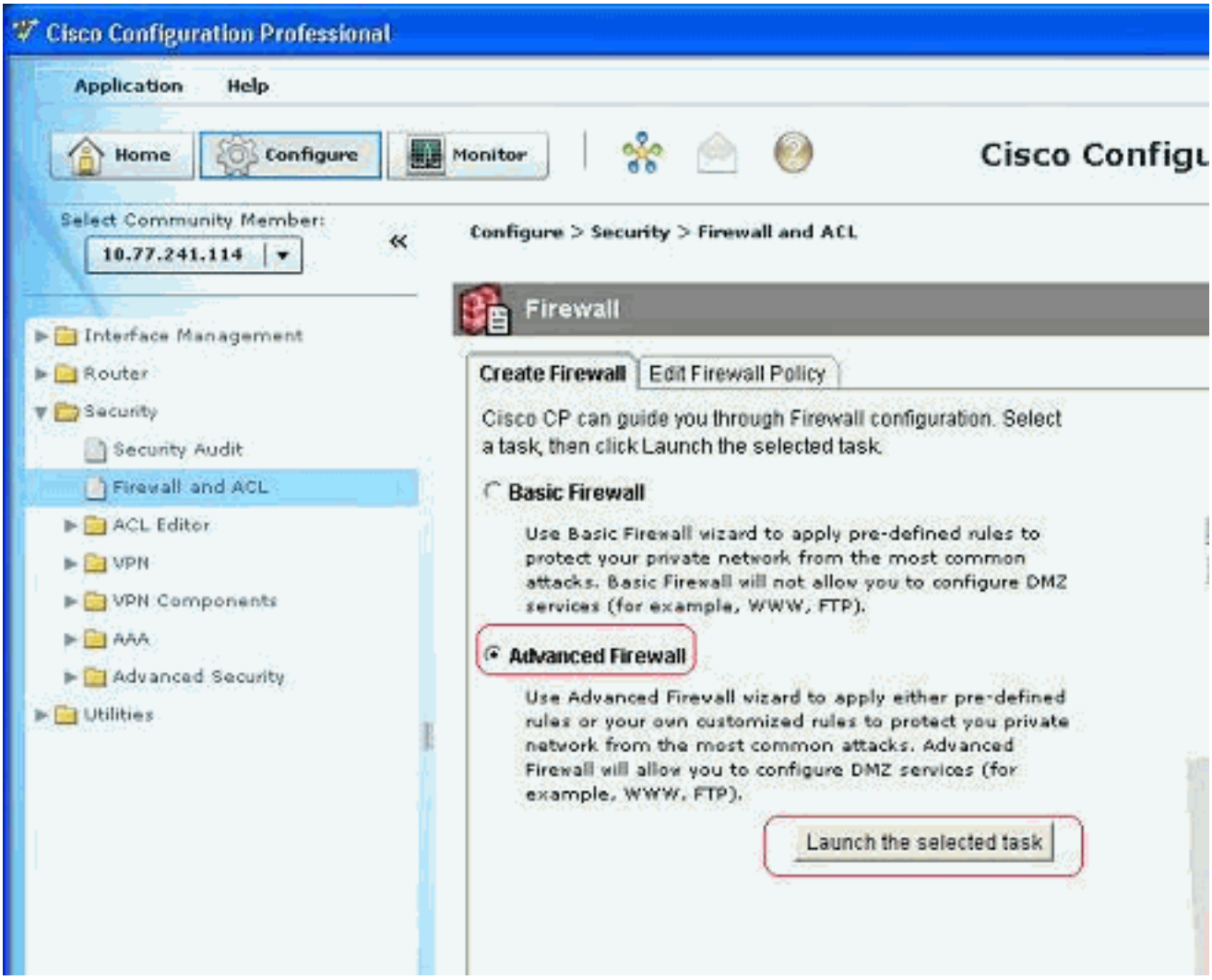
Конфигурация через Cisco Configuration Professional

Этот раздел содержит пошаговую процедуру о том, как использовать мастера для настройки Маршрутизатора IOS как зонального межсетевого экрана.

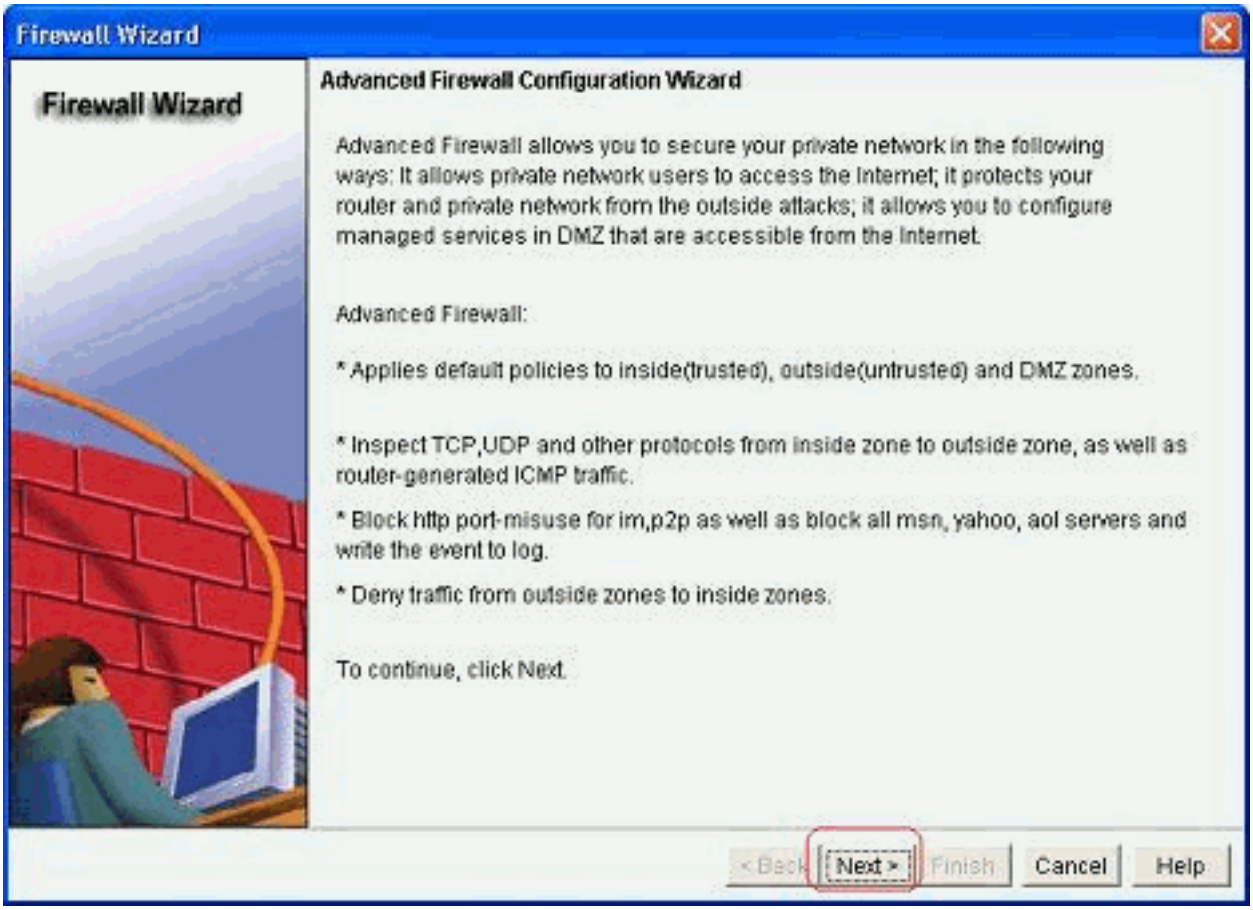
Выполните следующие действия:

1. Перейдите **Настраивают> Security> Межсетевой экран и ACL**. Затем выберите кнопку с

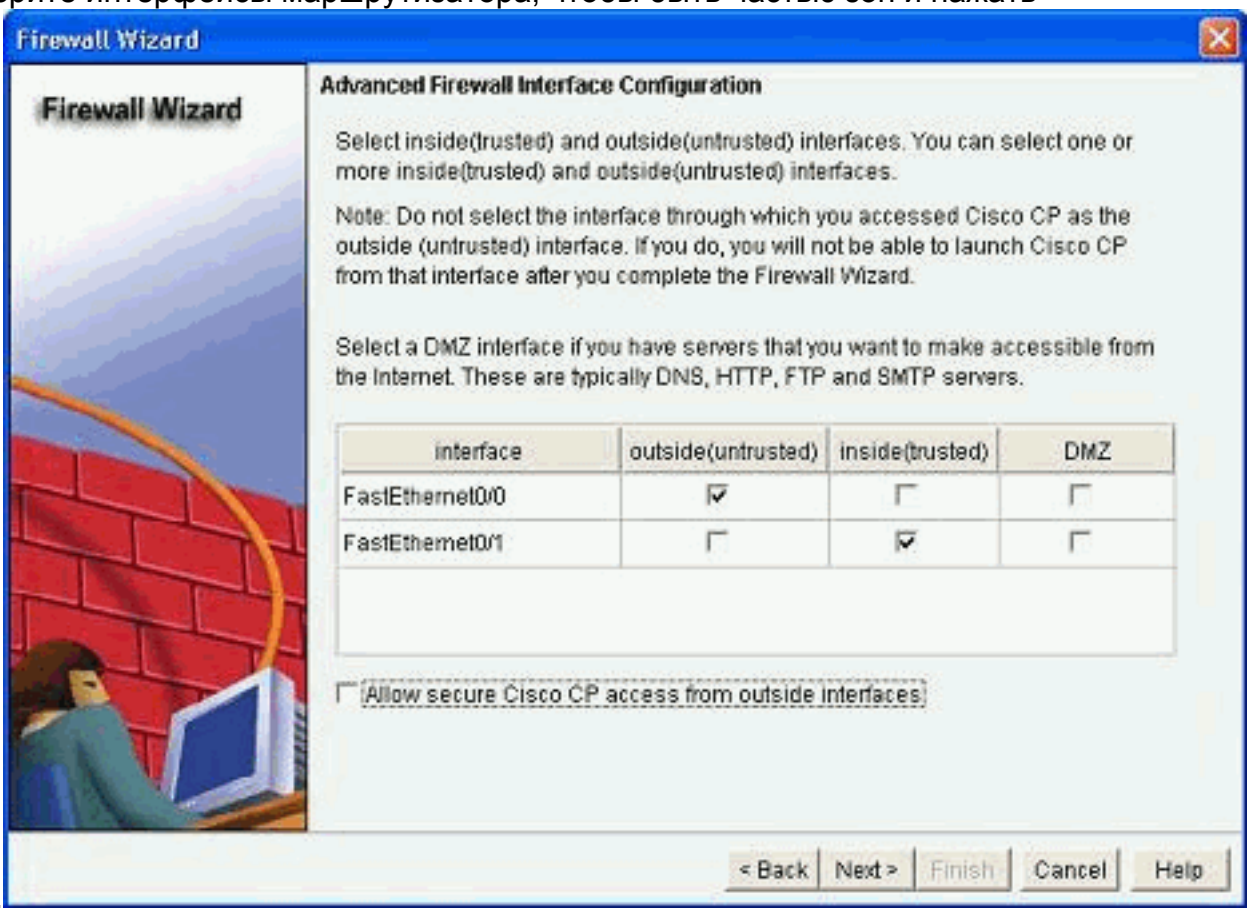
зависимой фиксацией **Advanced Firewall**. **Выберите Launch the selected task.**



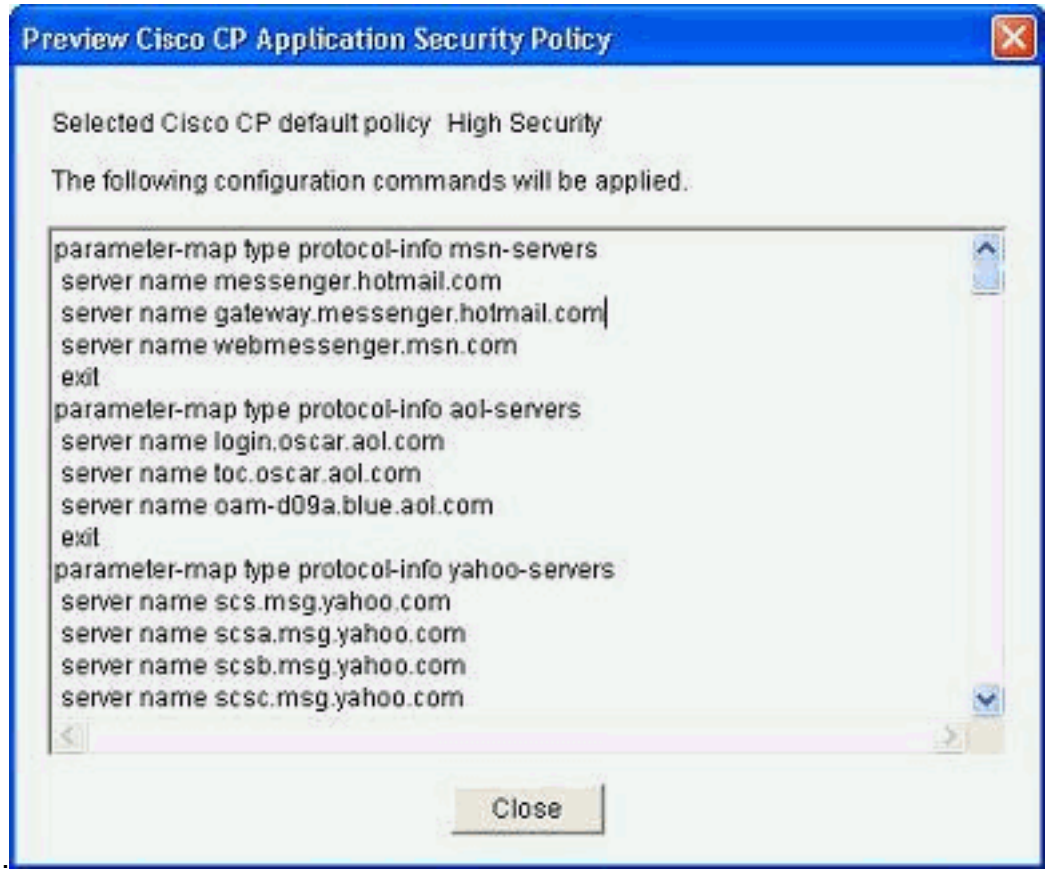
2. Этот следующий экран показывает краткое введение о Мастере Межсетевого экрана. Нажмите **Next**, чтобы начать настраивать межсетевой экран.



3. Выберите интерфейсы маршрутизатора, чтобы быть частью зон и нажать **Next**.

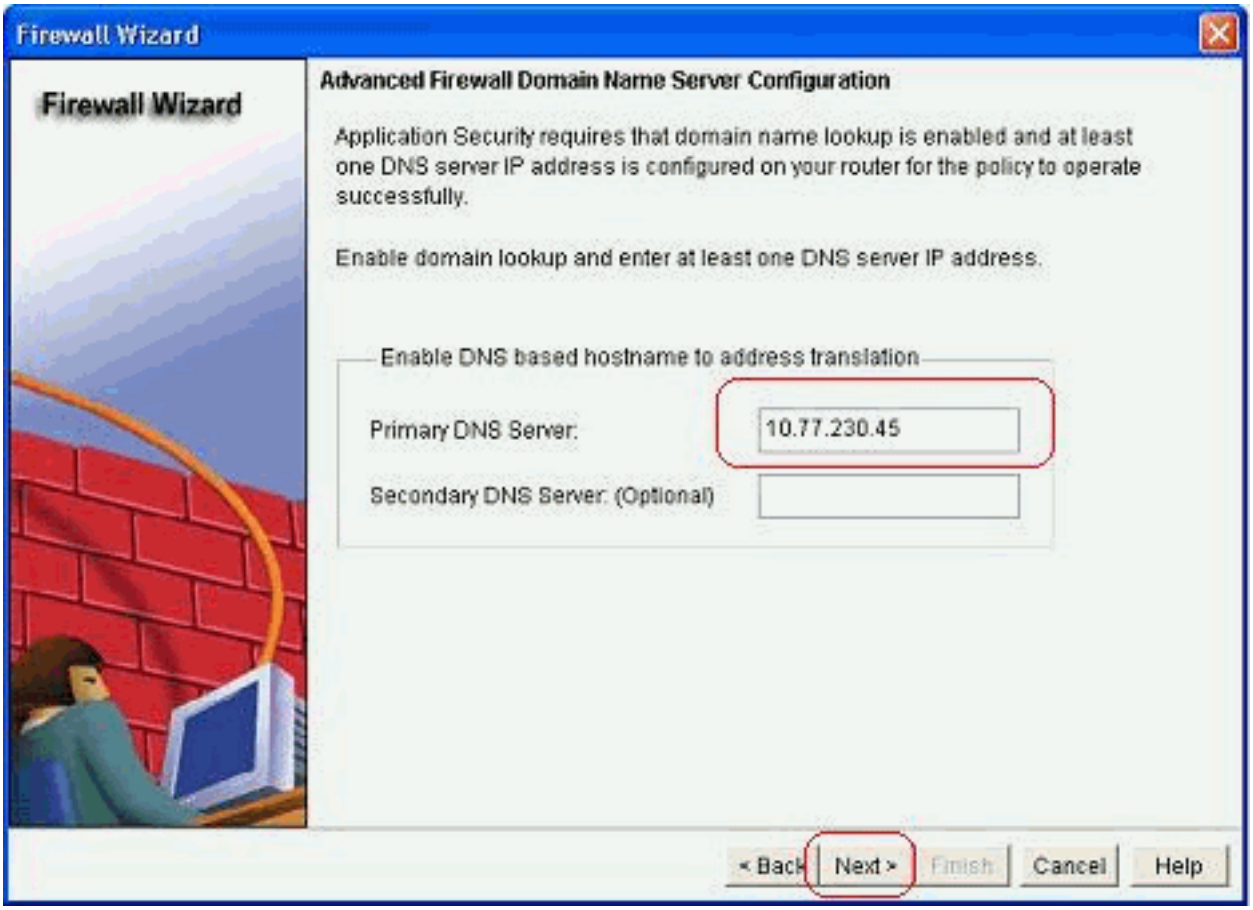


4. Политику по умолчанию с Высоким уровнем безопасности наряду с набором команд показывают в следующем окне. Нажмите **Close to**

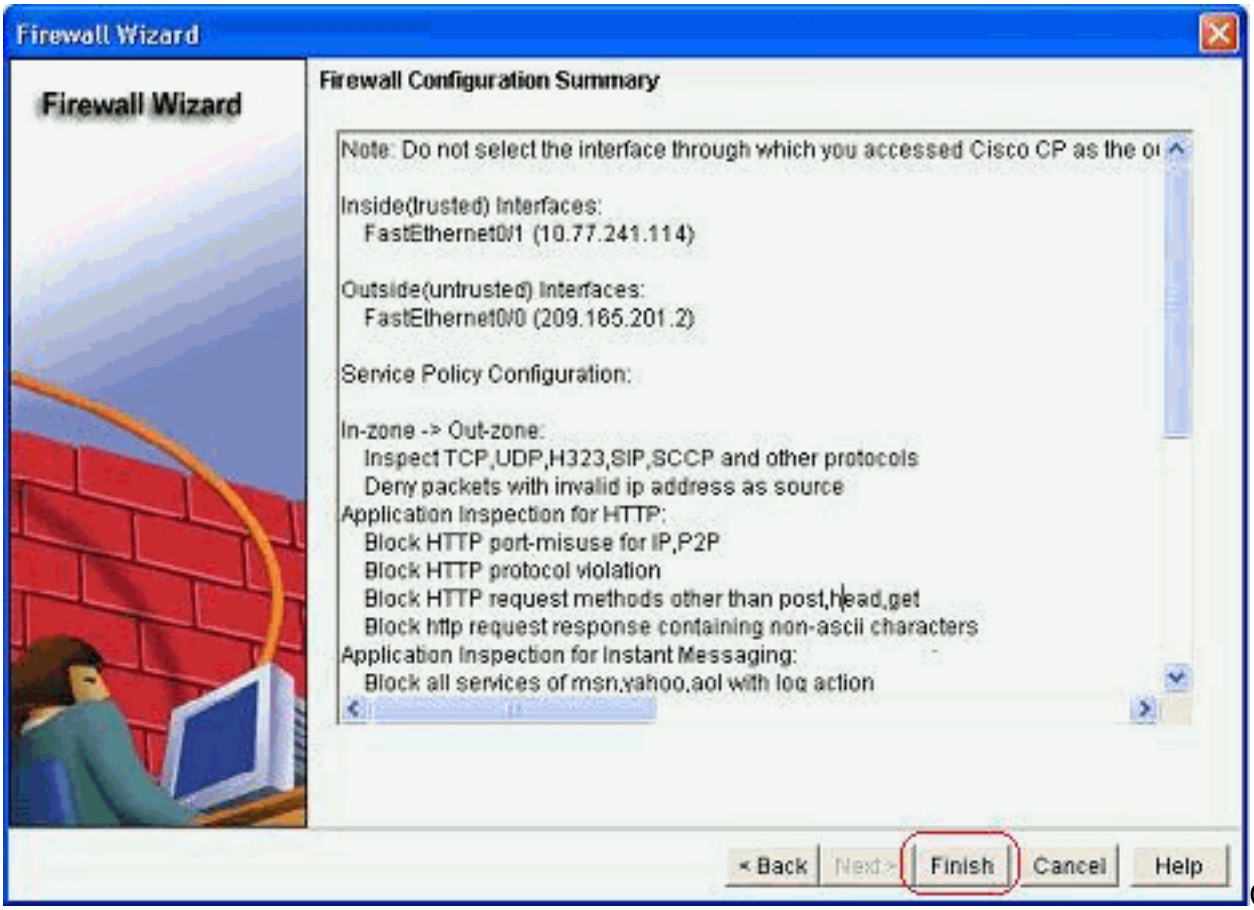


продолжаются.

5. Введите подробные данные Сервера DNS и нажмите **Next**.

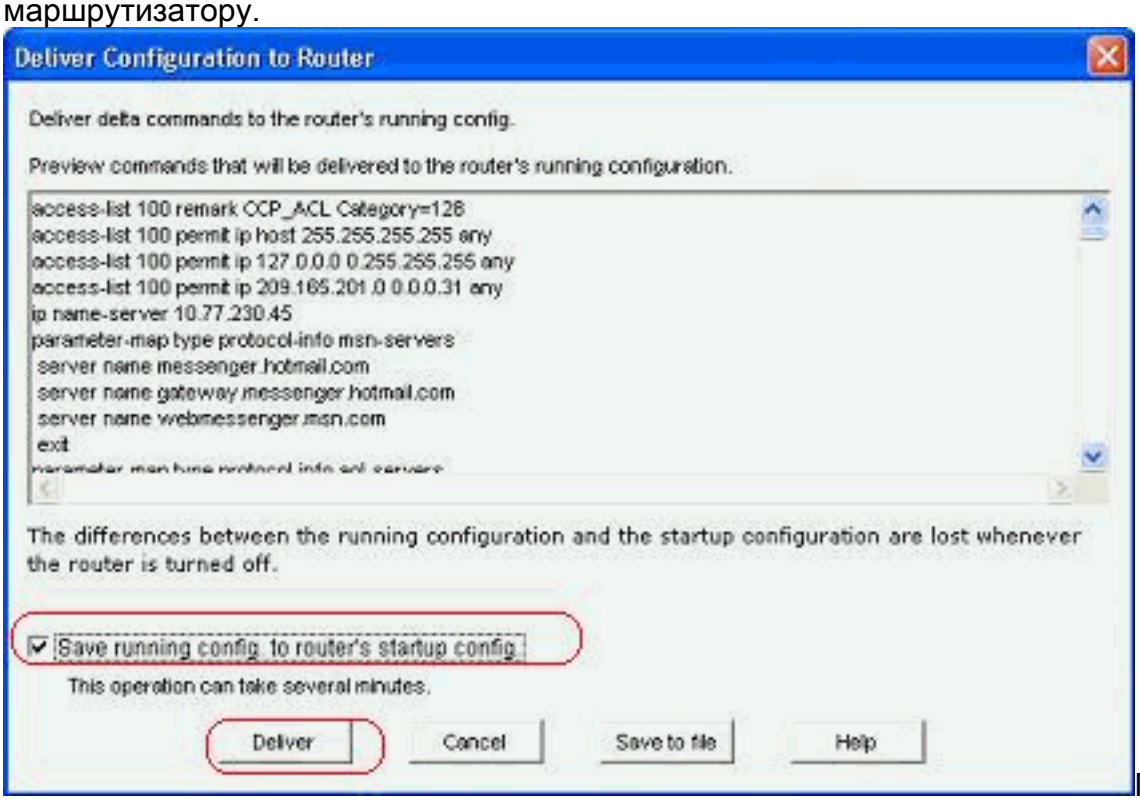


6. CP Cisco предоставляет сводку конфигурации такой как один показанный здесь. Нажмите **Finish** для завершения конфигурации.

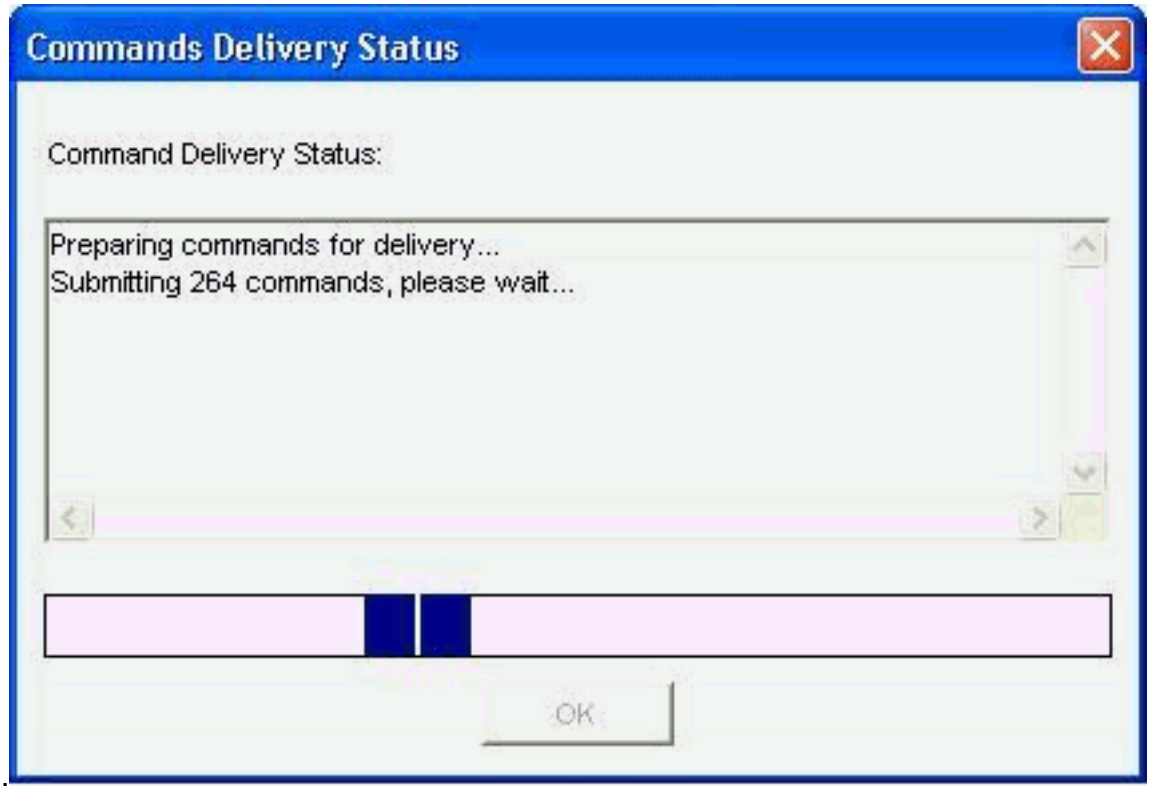


Сводка подробной конфигурации предоставлена в этой таблице. Это - конфигурация по умолчанию согласно политике Высокого уровня безопасности CP Cisco.

7. Проверьте **Сохранение рабочий config к** флажку **конфигурации запуска маршрутизатора**. Нажмите **Deliver** для передачи этой конфигурации к маршрутизатору.

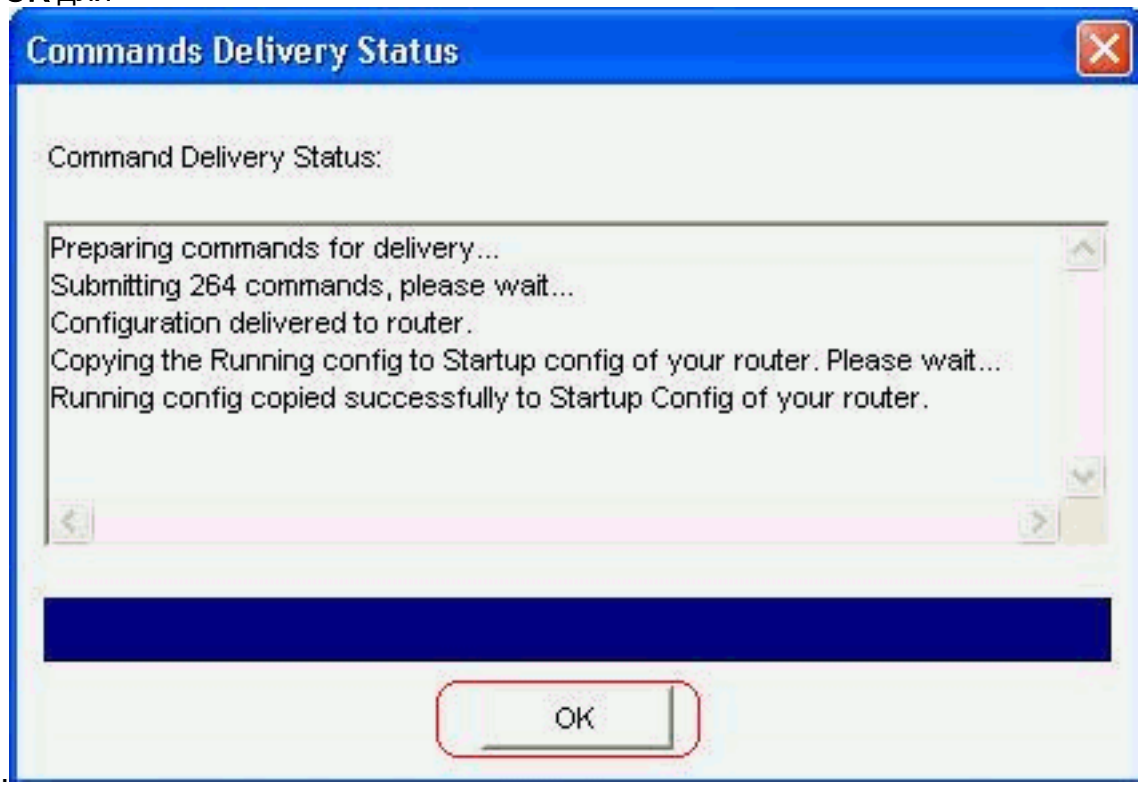


Полная конфигурация отправлена маршрутизатору. Это занимает время для



обработки.

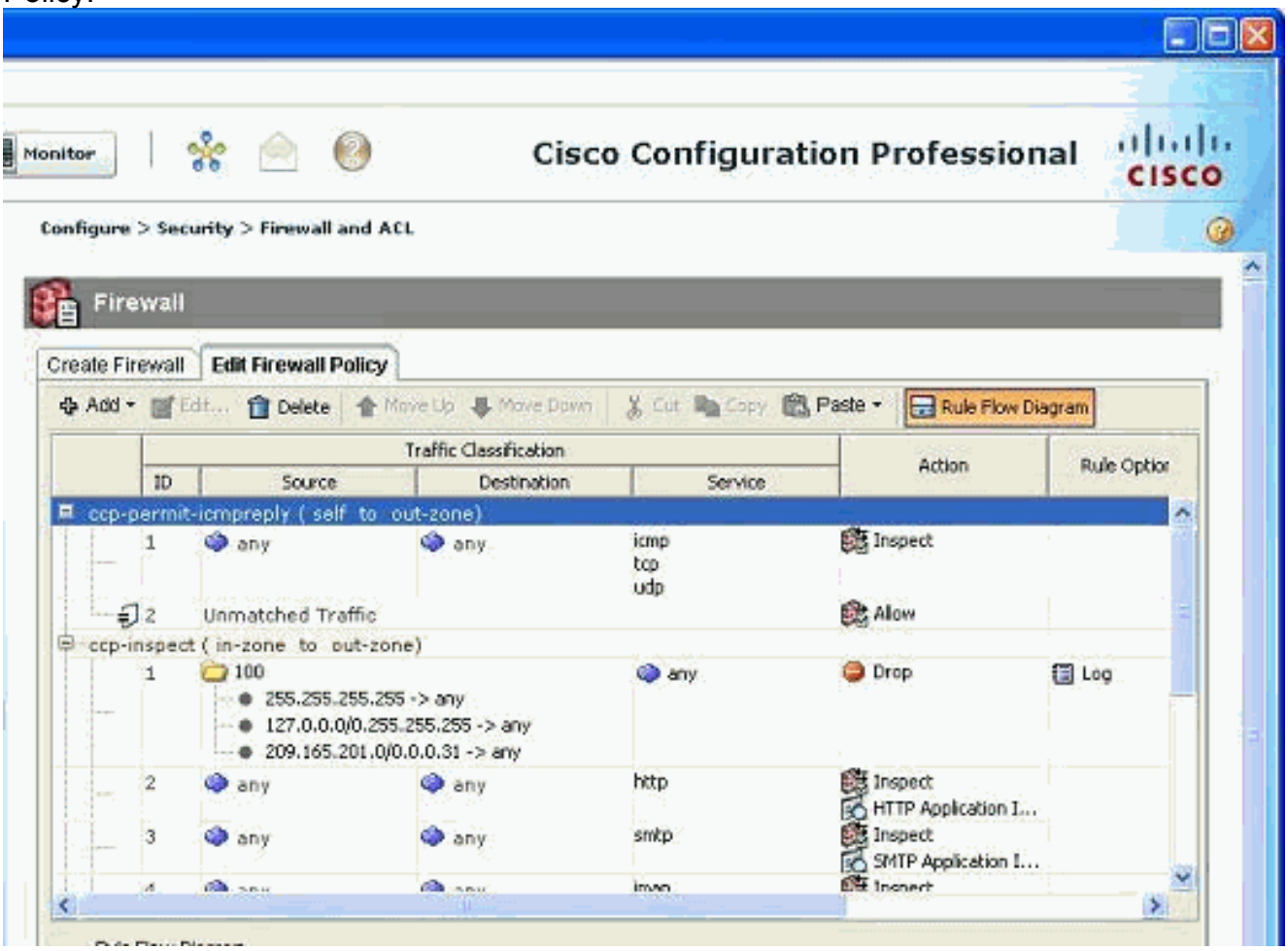
8. Нажмите **OK** для



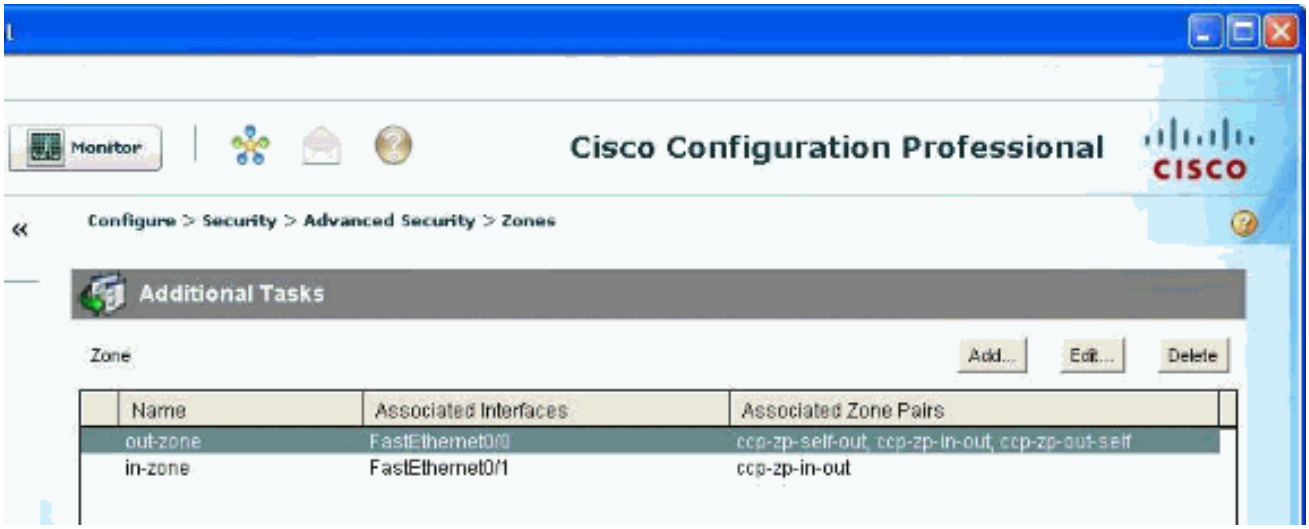
перехода.

9. Нажмите **OK**

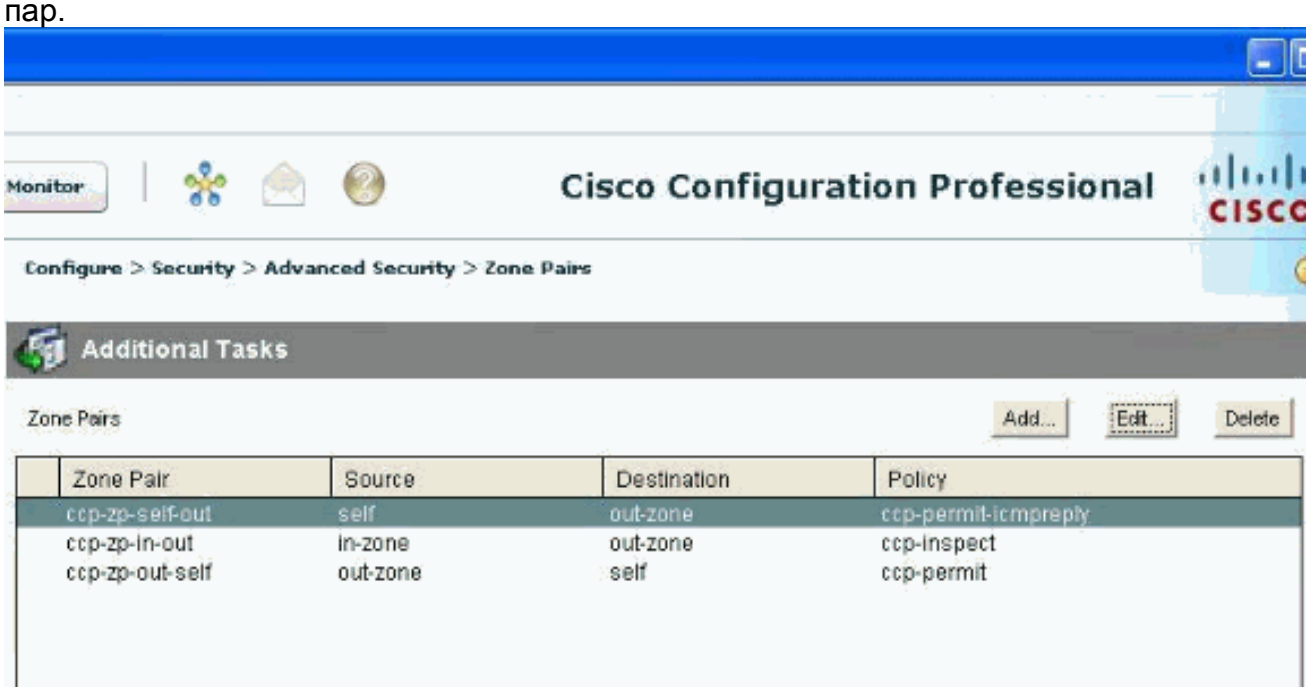
снова. Конфигурация теперь в действительности и показана как правила под вкладкой Firewall Policy.



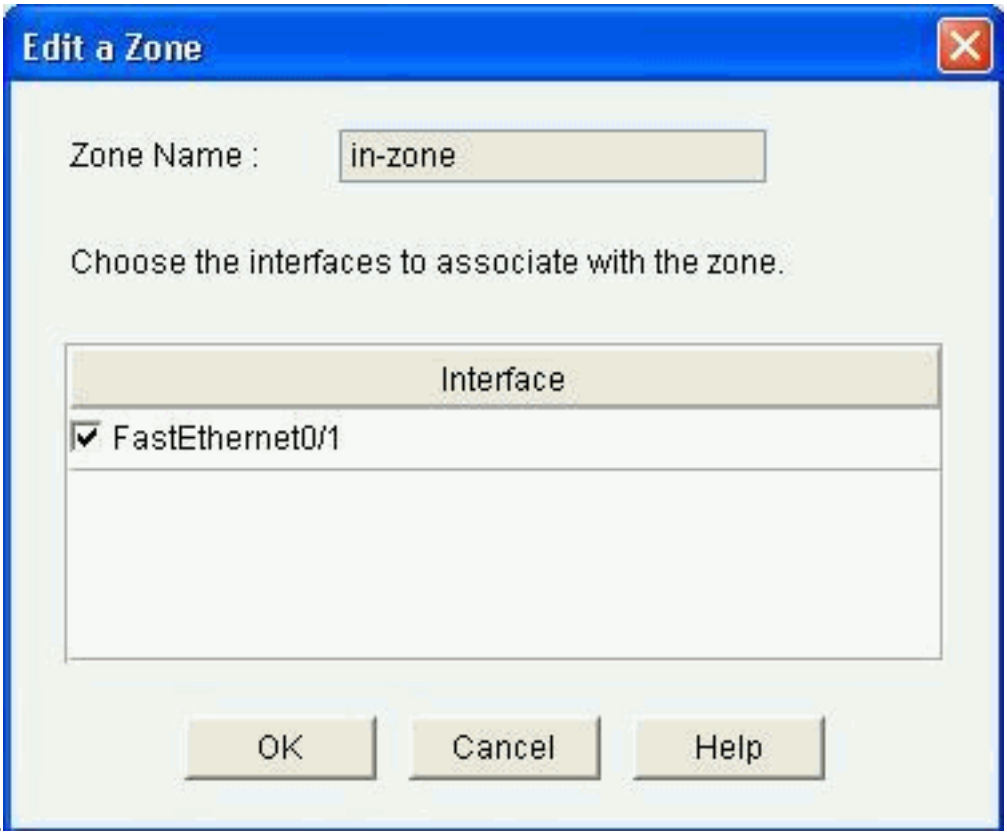
10. Зоны наряду с зональными парами, они привязаны, могут быть просмотрены, если вы переходите**, Настраивают> Security> Дополнительная безопасность> Зоны**. Можно также добавить новые зоны путем **нажмите Add** или модифицировать существующие зоны путем нажатия
Edit.



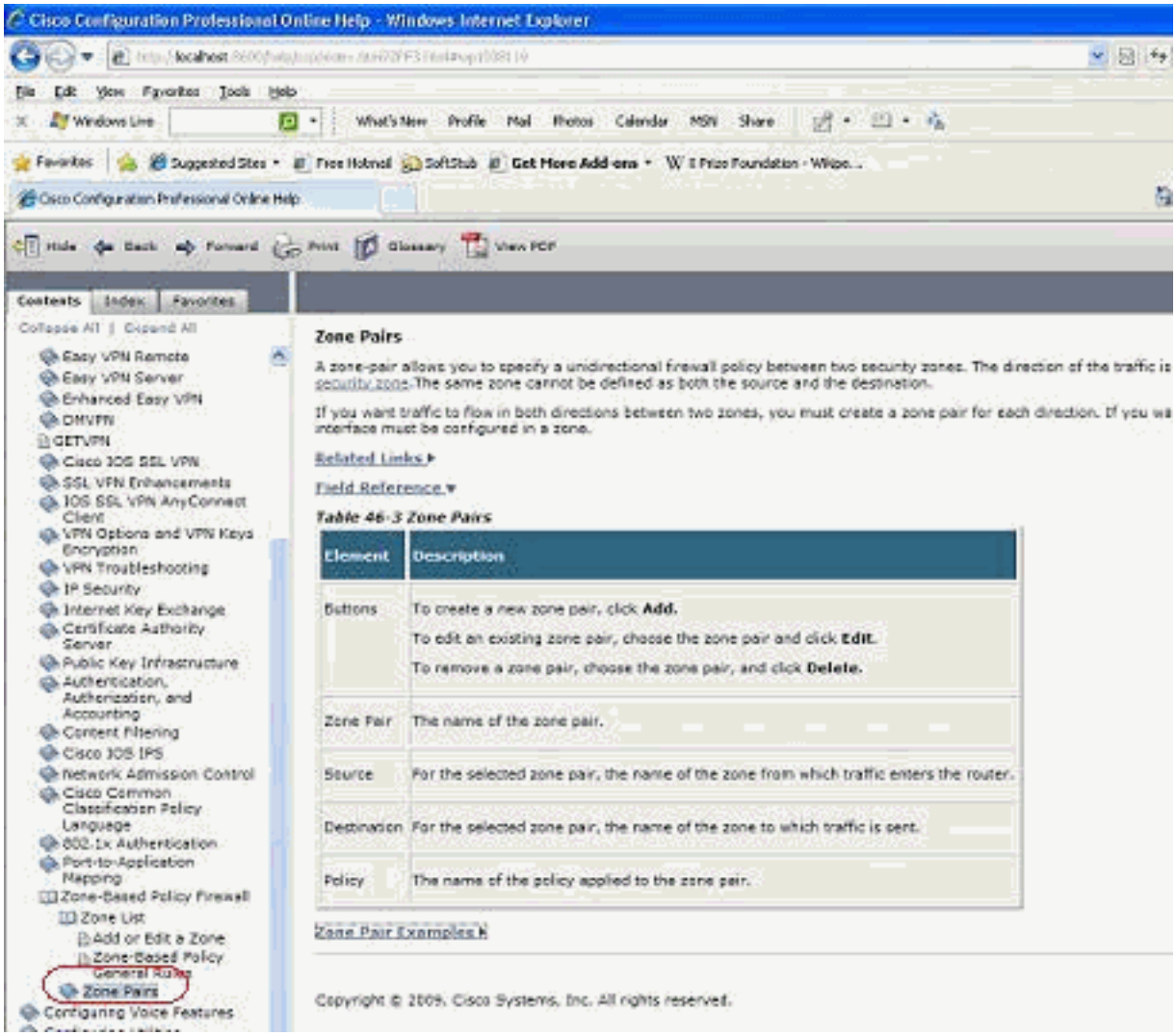
11. Перейдите **Настраивают> Security> Дополнительная безопасность> Зональные Пары**, чтобы посмотреть детали зональных
пар.



Мгновенная справка о том, как модифицировать/добавлять/удалять пар зон/зоны и другие дополнительные сведения, легко доступна со встроенными веб-страницами в CP

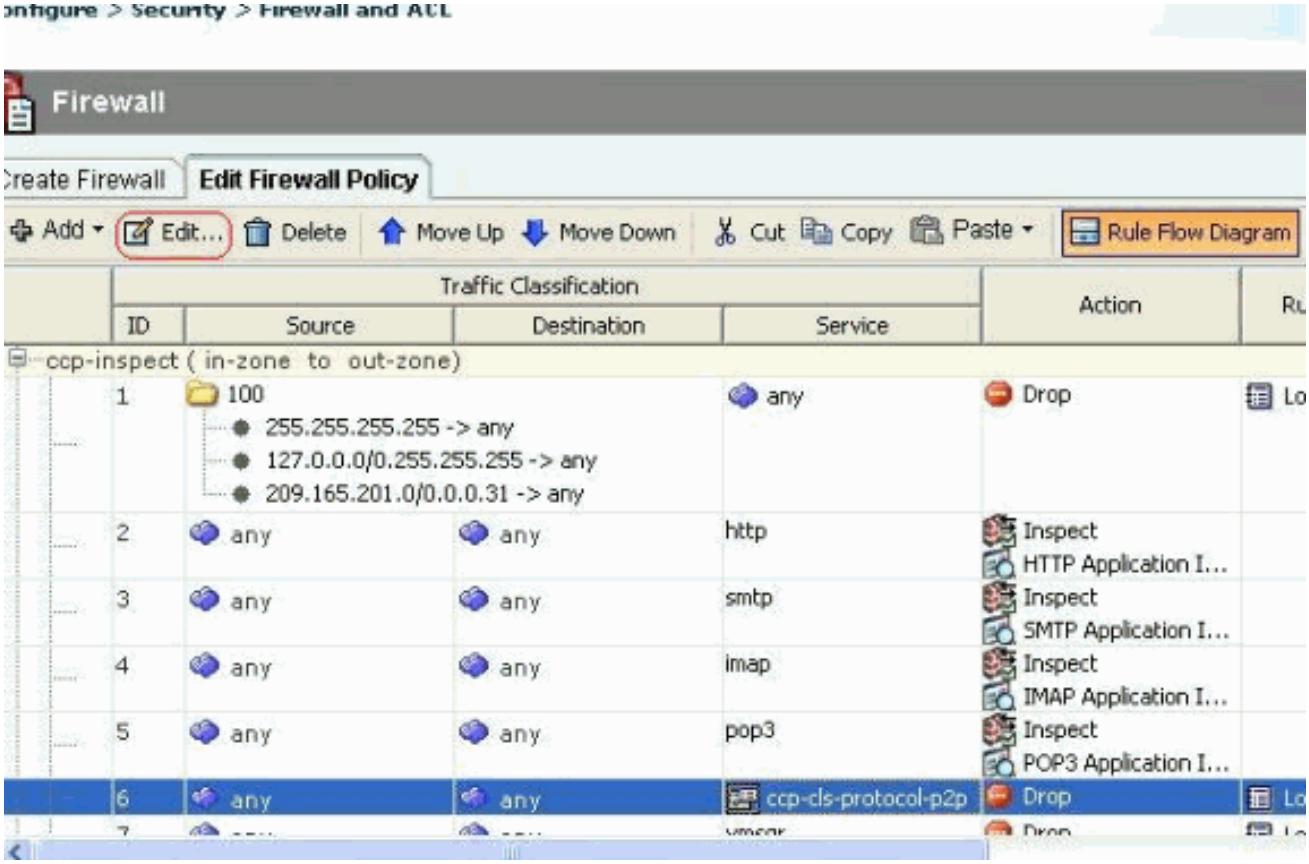


Cisco.

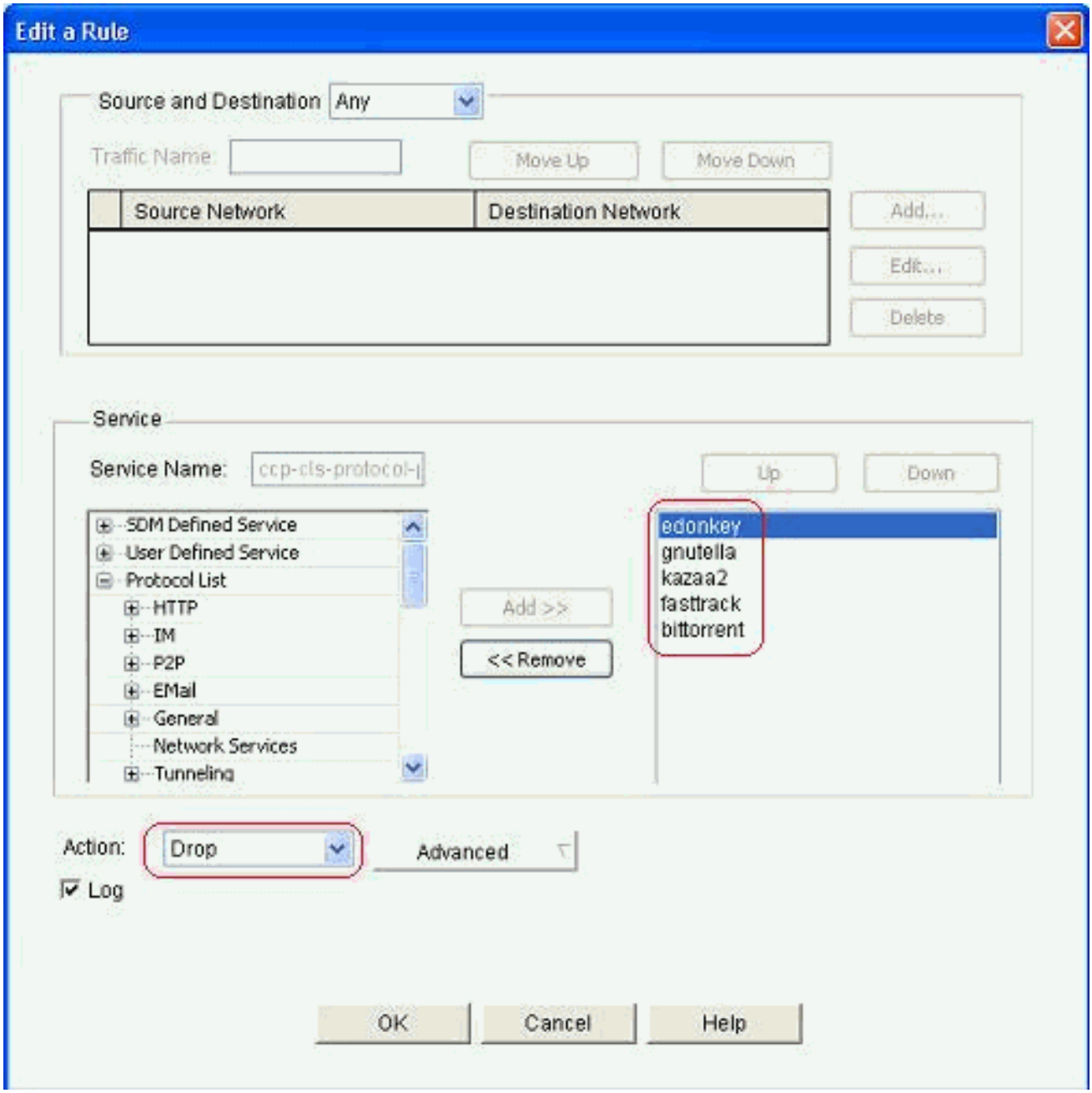


12. Для изменения специализированных инспекционных возможностей определенных приложений P2P перейдите **к> Security Конфигурации> Межсетевой экран и ACL**. Затем нажмите **Edit Firewall Policy** и выберите соответствующее правило в карте

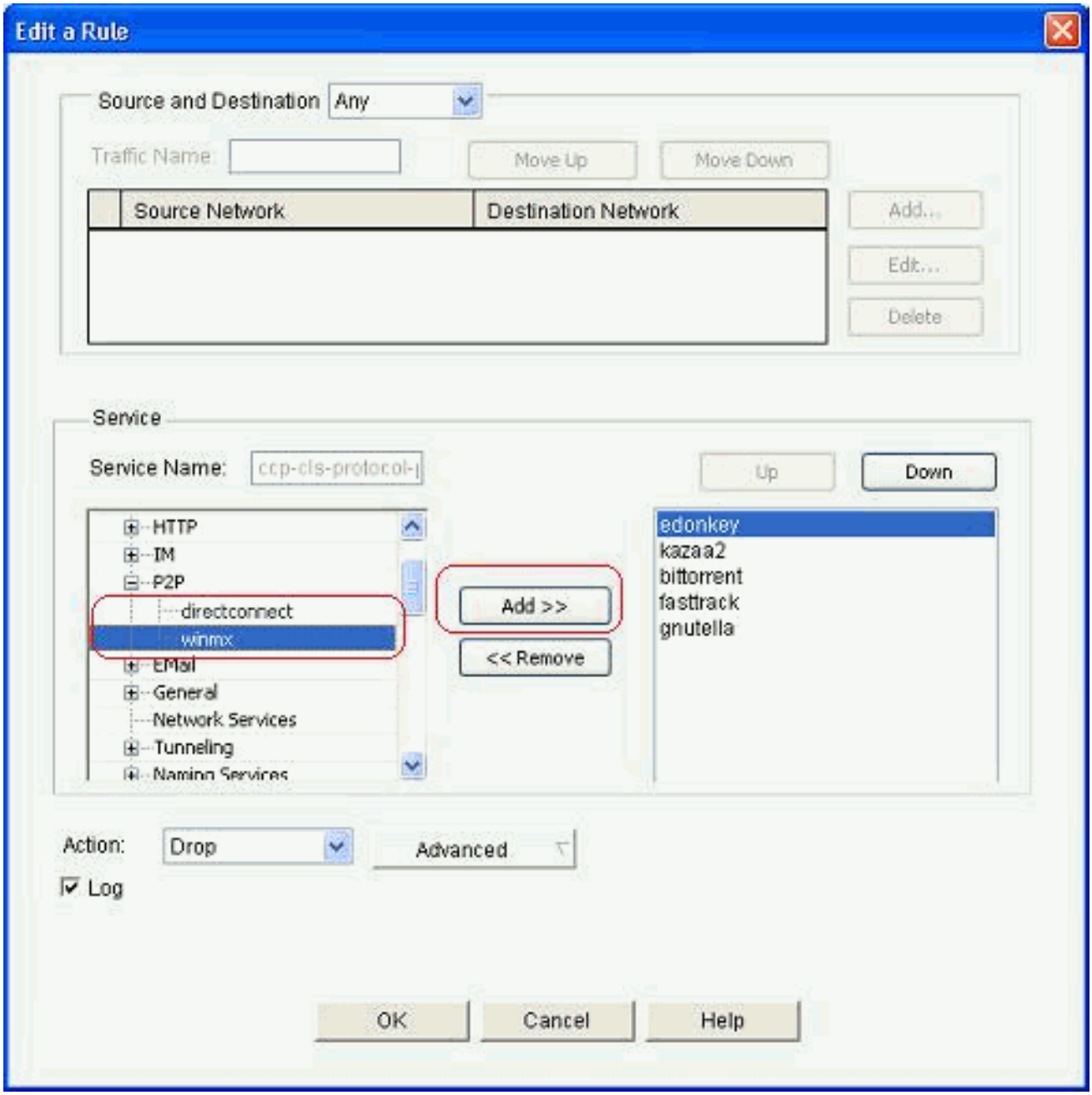
политик. **Нажмите**
Edit.

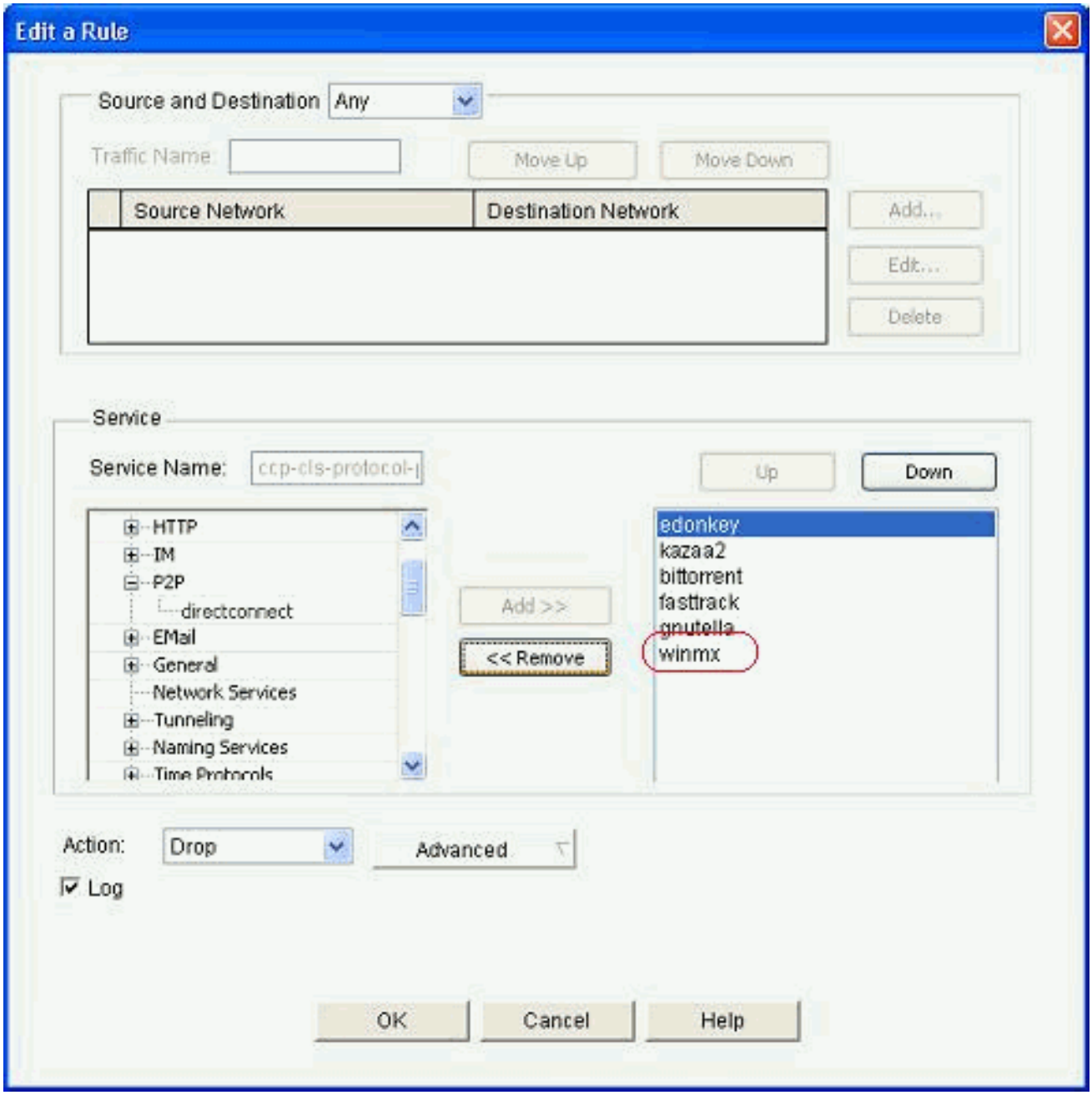


Это показывает текущие приложения P2P, которые будут заблокированный конфигурацией по
умолчанию.

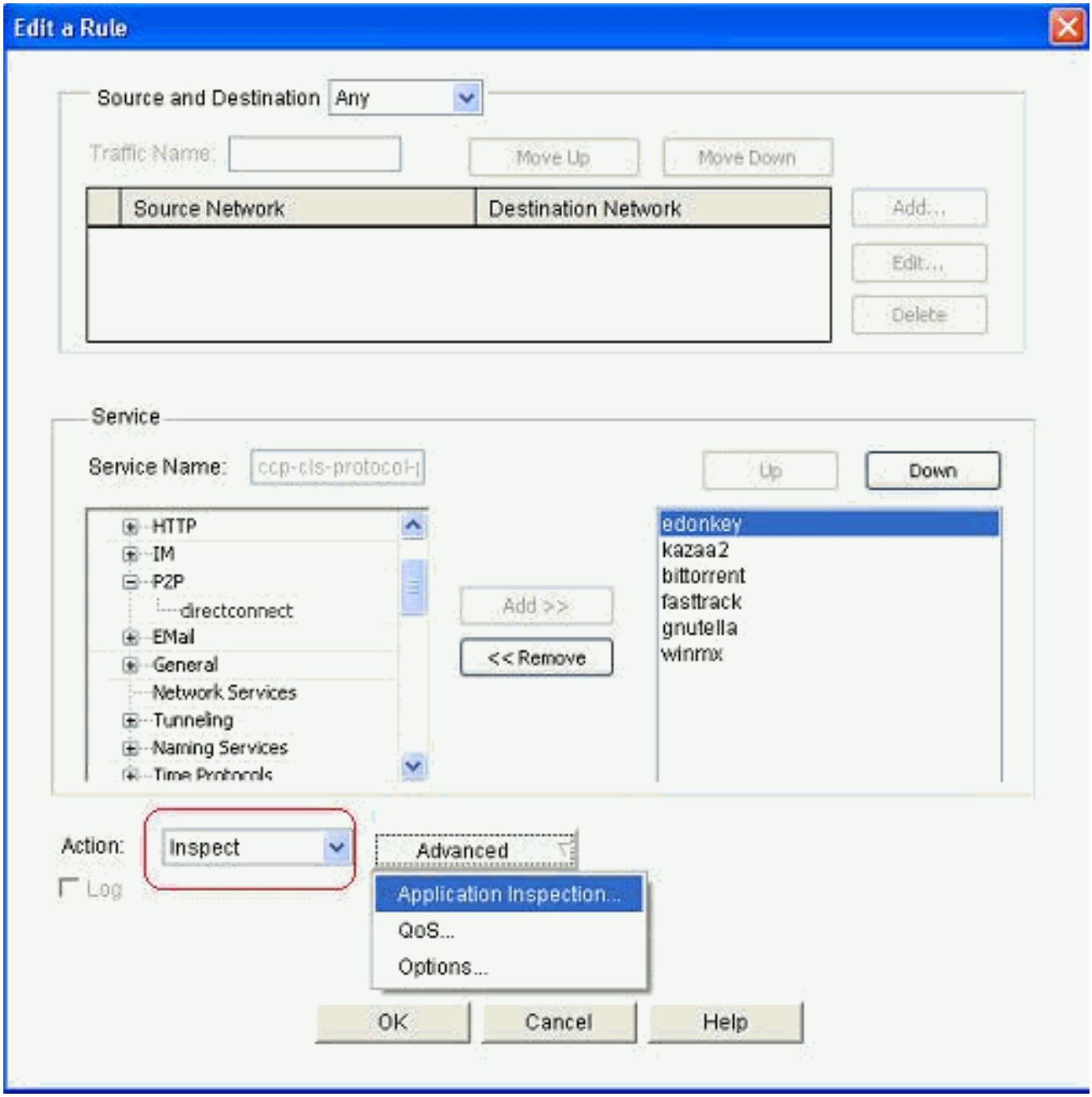


13. Можно использовать кнопки Add и Remove для добавления определенных приложений. Этот снимок экрана показывает, как добавить приложение winmx для блокирования
этого.


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

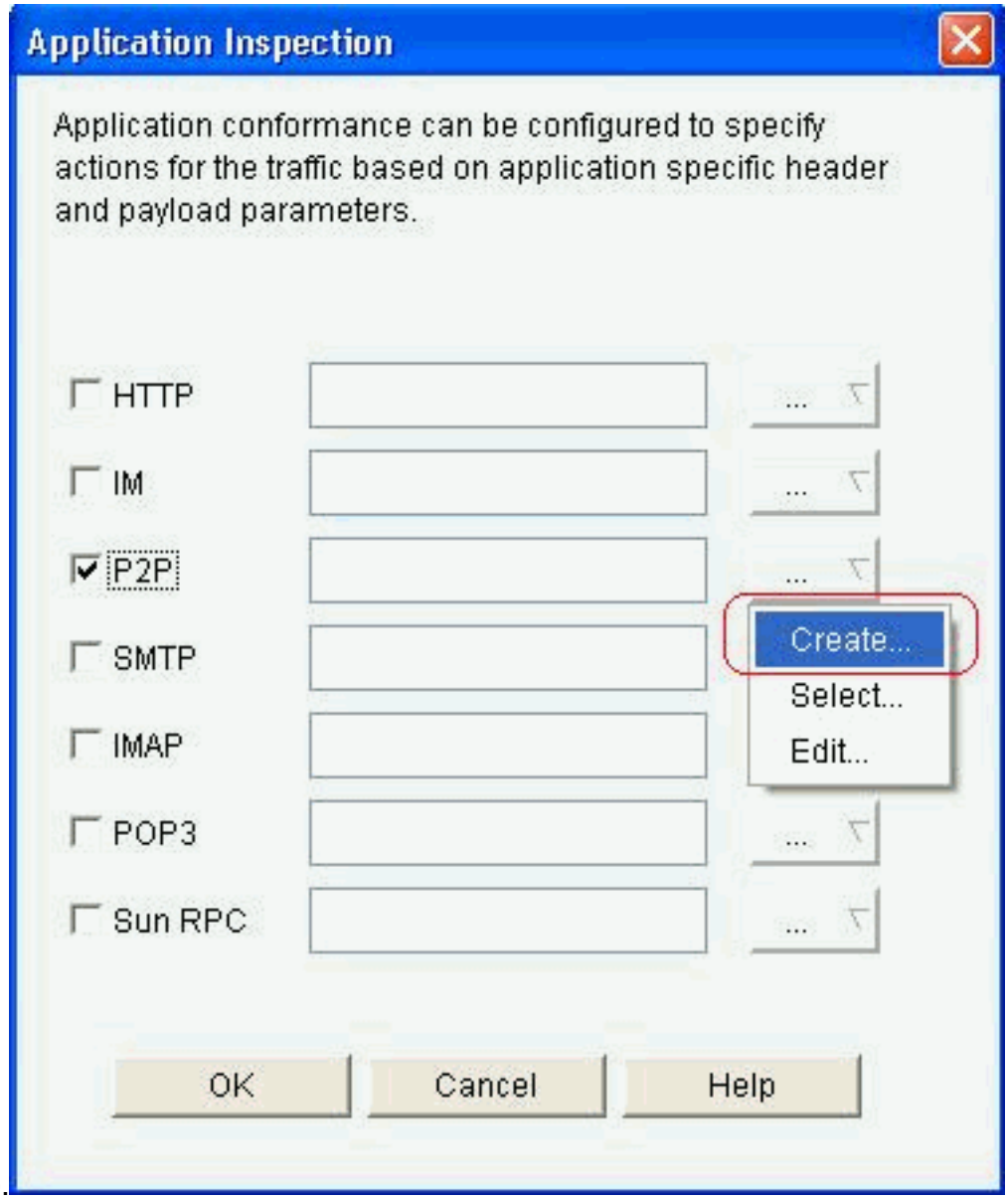


14. Вместо того, чтобы выбрать действие сброса, можно также выбрать действие Inspect для применения различных вариантов для глубокой проверки пакетов.



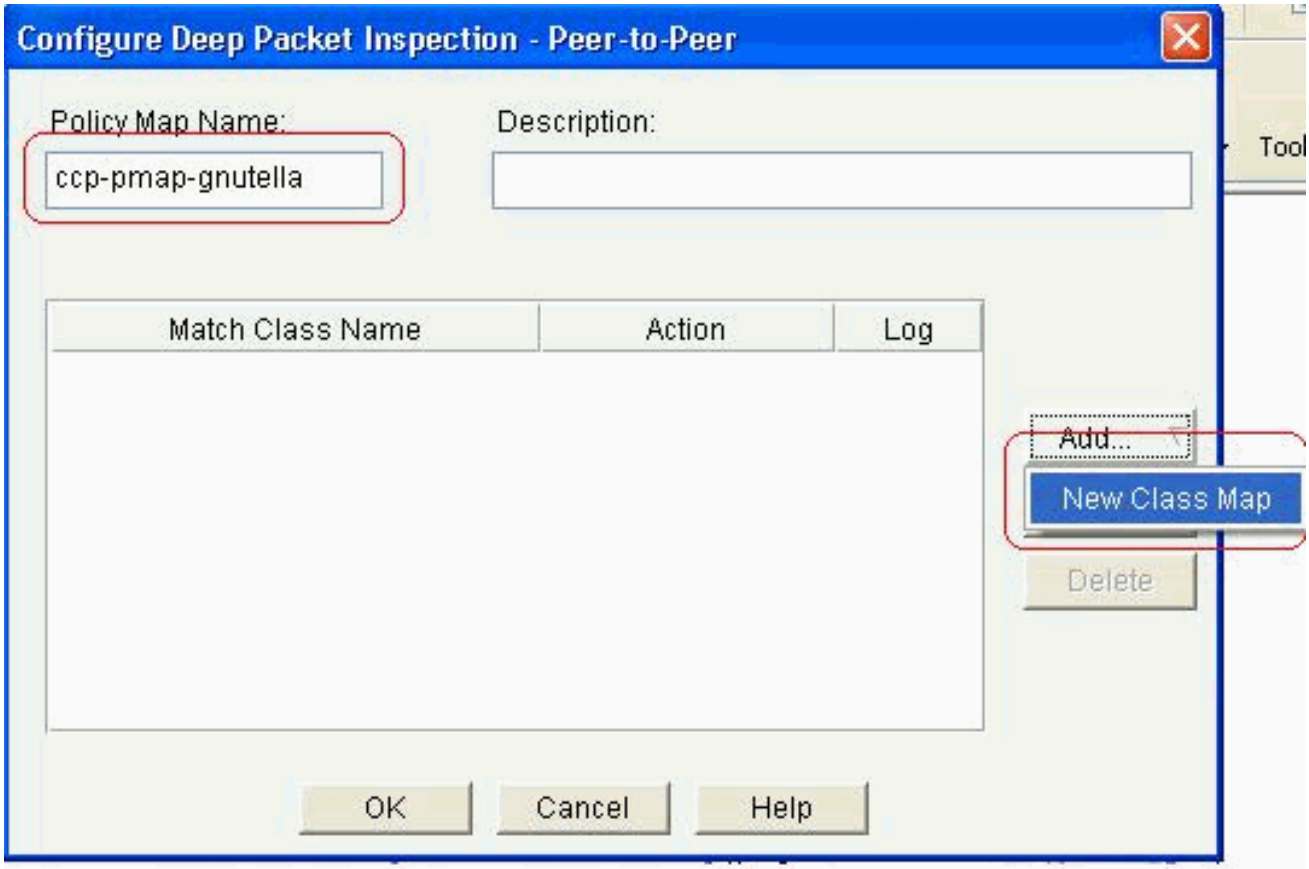
Контроль P2P предлагает политику Уровня 4 и Уровня 7 для трафика приложения. Это означает, что ZFW может предоставить основную проверку трафика потоком для permit or deny трафика, а также гранулированного контроля за Уровнем 7 на определенных действиях в различных протоколах, так, чтобы определенные активности приложения были позволены, в то время как запрещены другие. В этом контроле приложения можно применить различные типы определенных проверок уровня заголовка для приложений P2P. Пример для gnutella показывают затем.

15. Проверьте **опцию P2P** и нажмите **Create** для создания нового policy-map для

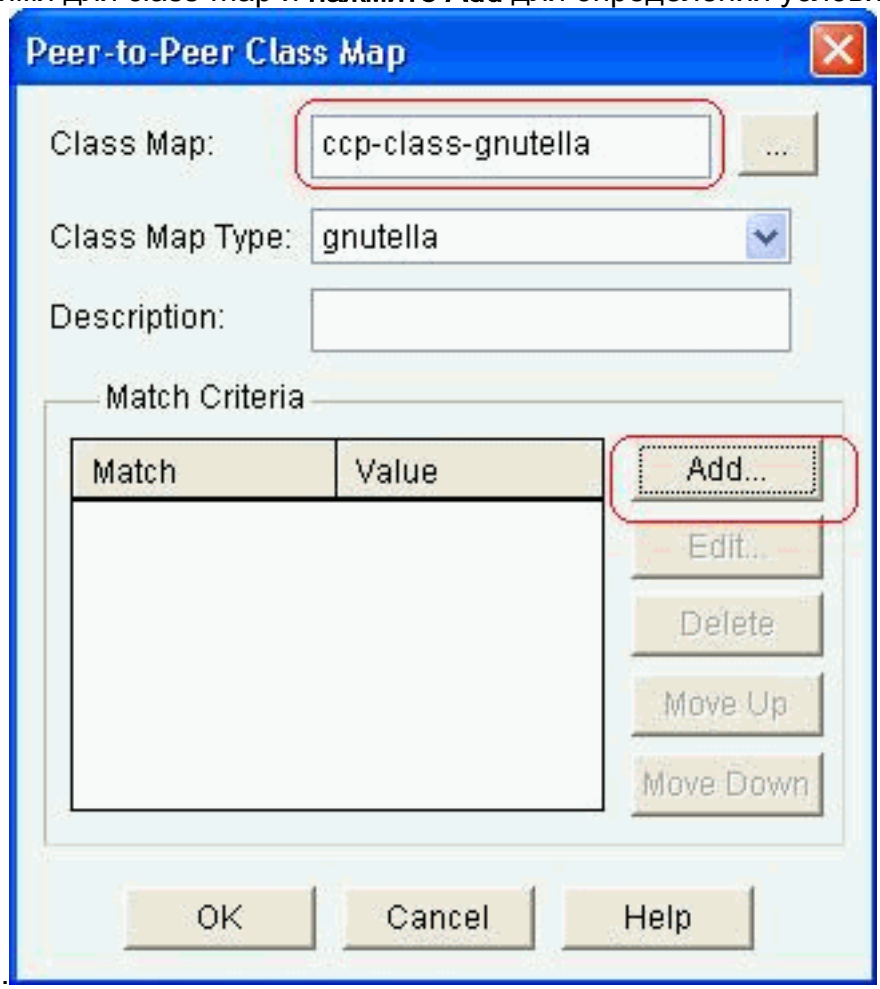


этого.

16. Создайте новый policy-map для глубокой проверки пакетов для протокола gnutella. **Нажмите Add** и затем выберите **New Class Map**.



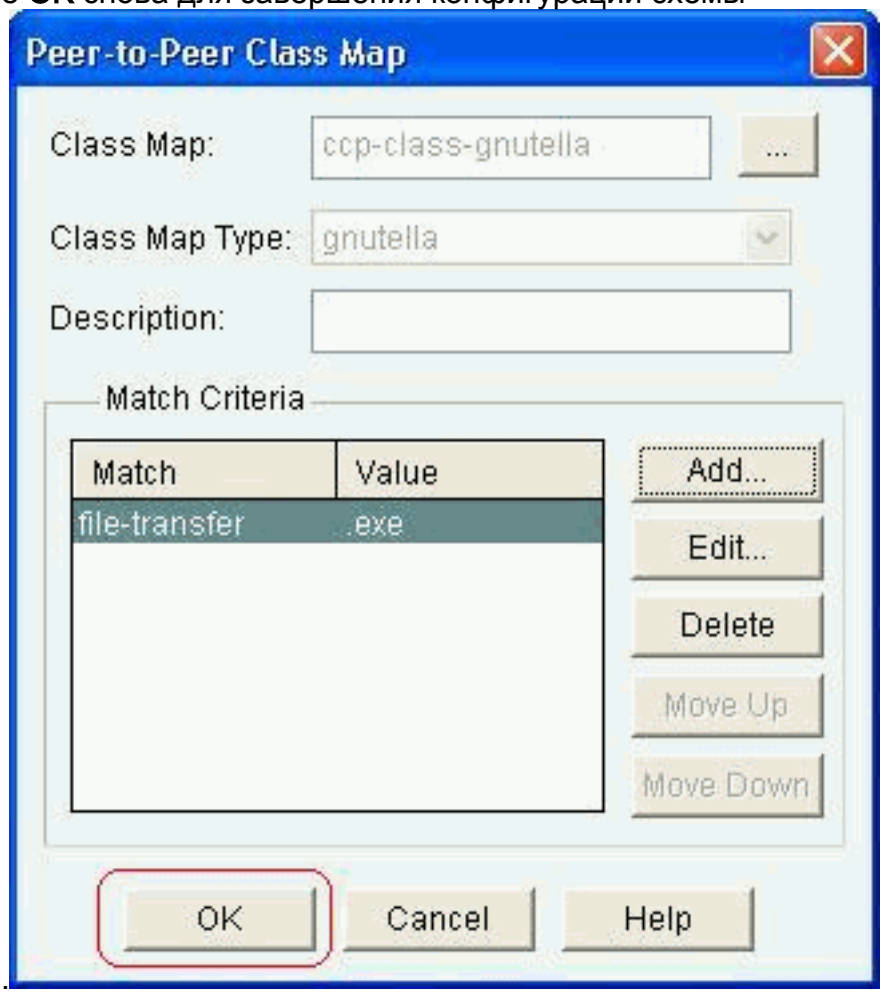
17. Дайте новое имя для class-map и **нажмите Add** для определения условий соответствия.



18. Используйте передачу файла в качестве критерия соответствия, и используемая строка является .exe. Это указывает что все соединения передачи файла gnutella, содержащие совпадение строки .exe для политики трафика. **Нажмите кнопку**

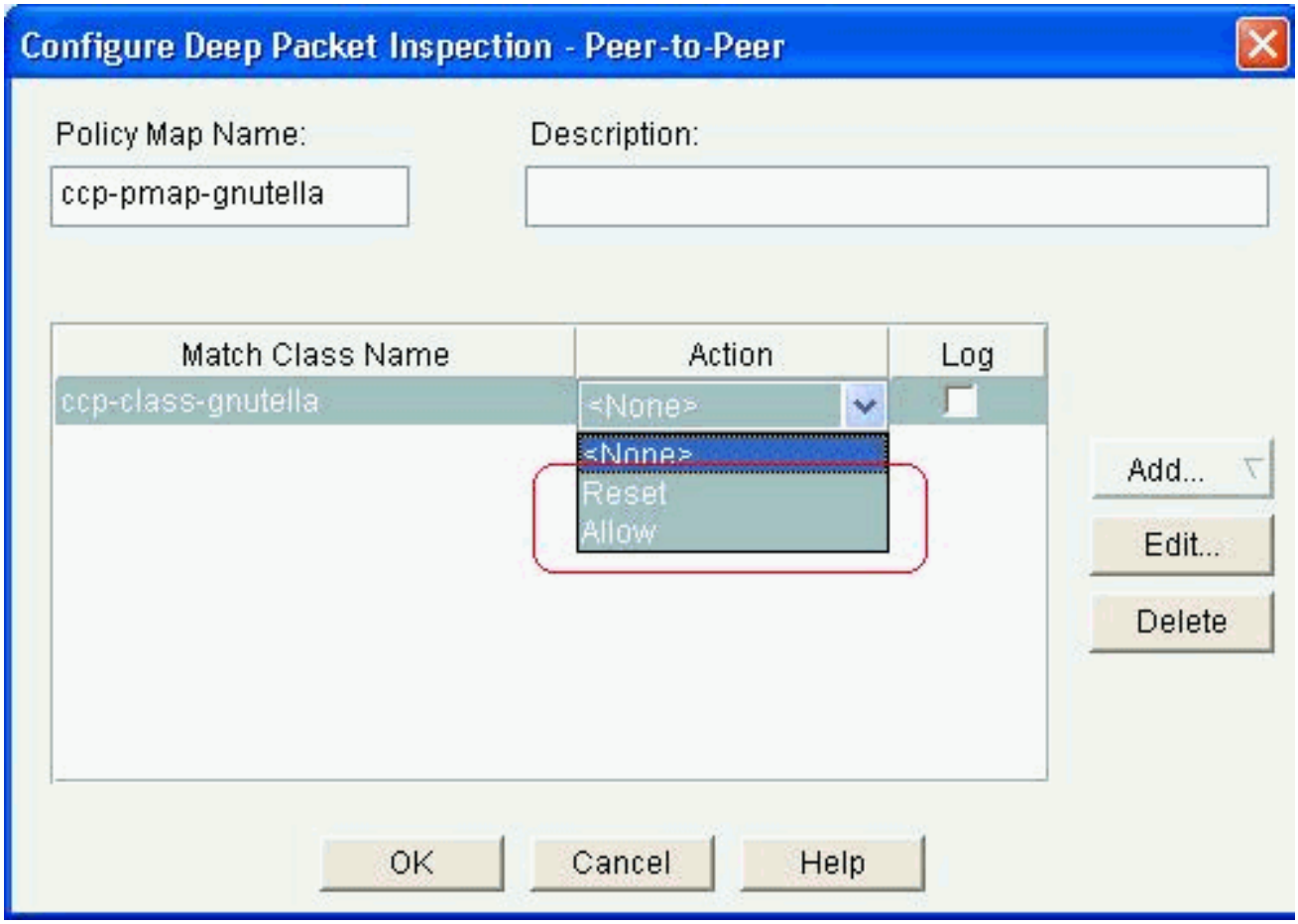
OK.

19. Нажмите **OK** снова для завершения конфигурации схемы



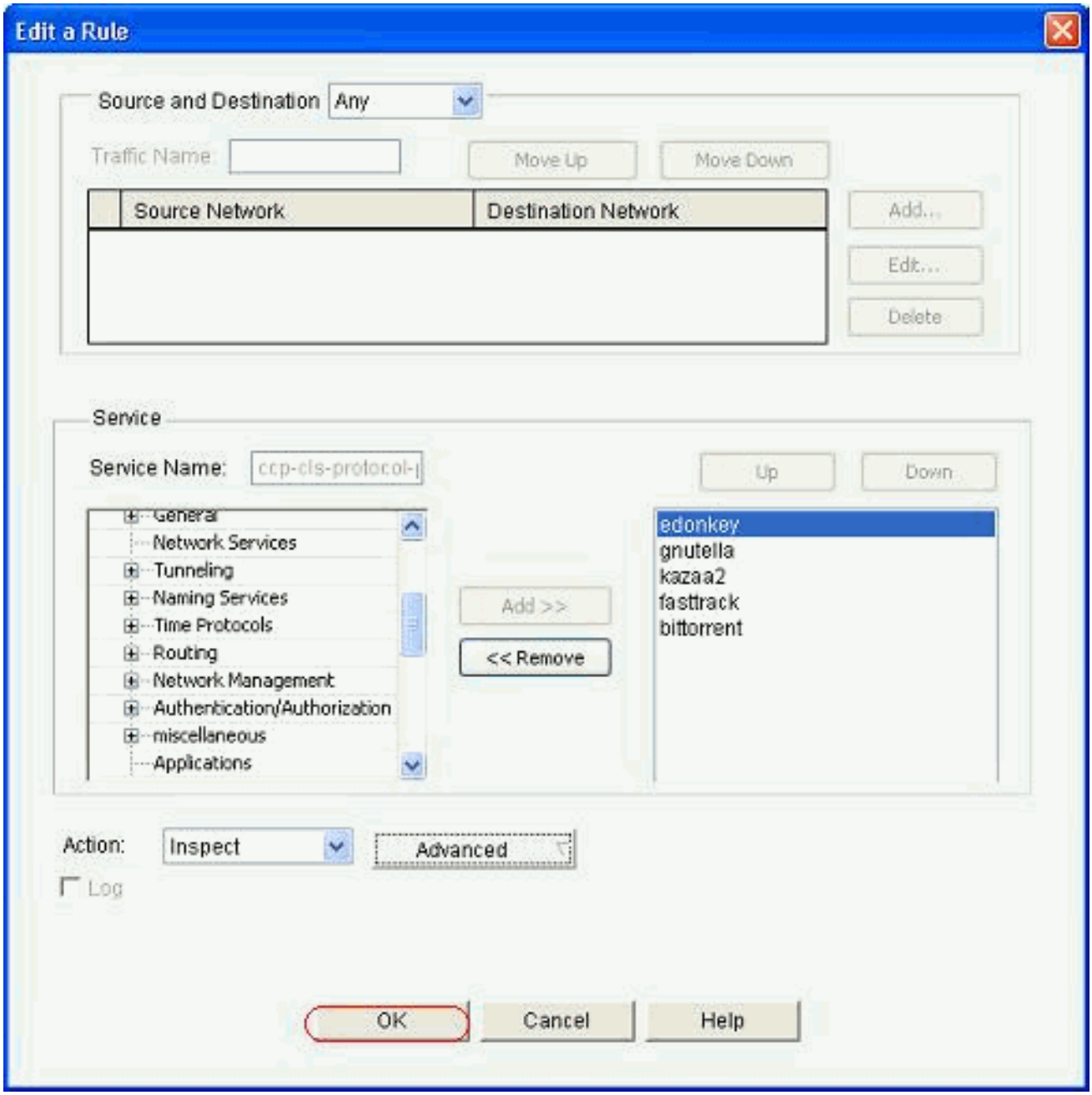
классов.

20. Выберите **Reset** или **опцию Allow**, которая зависит от Политики безопасности вашей компании. Нажмите **OK** для подтверждения действия с policy-map.



Этим тем же способом можно добавить другие policy-map для реализования глубоких инспекционных опций для других протоколов P2P путем определения других регулярных выражений как критерия соответствия.**Примечание:** Приложения для обмена данными в одноранговой сети особенно сложно обнаружить из-за смены портов и других уловок для избегания обнаружения, а также из-за проблем, вызванных быстрыми изменениями и обновлениями таких приложений, которые модифицируют поведение протоколов. ZFW комбинирует собственную проверку трафика потоком межсетевого экрана с возможностями распознавания трафика Сетевого распознавания приложений (NBAR) отправить управление приложениями P2P.**Примечание:** Проверка приложений для обмена данными в одноранговой сети обладает возможностями приложения, предназначенными для набора приложений, который можно проверить на уровне 4:edonkeyfasttrackgnutellakazaa2**Примечание:** В настоящее время ZFW не имеет опции для осмотра трафика приложения "BitTorrent". Клиенты BitTorrent обычно обмениваются данными с так называемыми “трекерами” (серверами одноранговых каталогов) с помощью протокола http, использующего какой-либо нестандартный порт. Обычно это порт TCP 6969, но, возможно, потребуется проверить порт, специально предназначенный для трекера. Если вы хотите позволить BitTorrent, лучший метод для размещения дополнительного порта должен настроить HTTP как одного из match protocol и добавить TCP 6969 к HTTP с помощью этой команды ip port-map: **порт tcp 6969 http ip port-map**. При этом потребуется определить http и bittorrent как критерии соответствия, применяемые в карте классов.

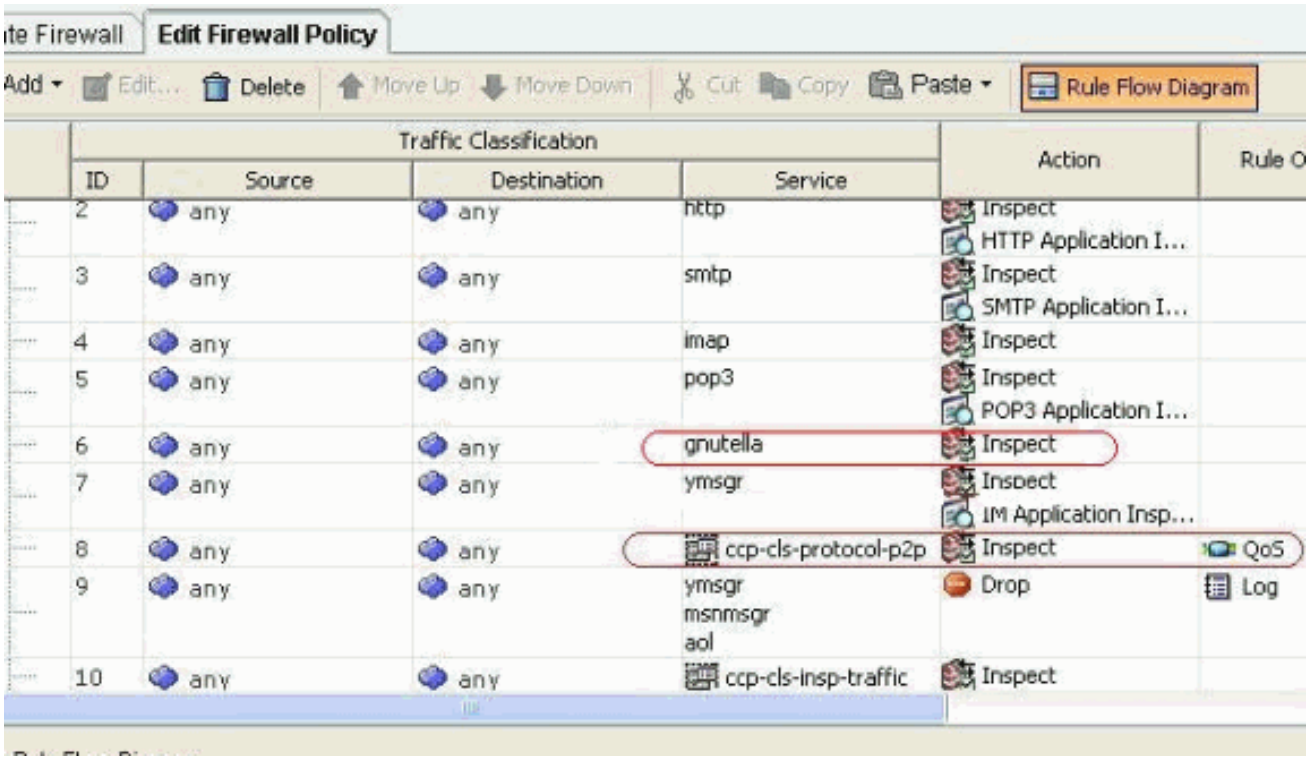
21. Нажмите **OK** для завершения Усовершенствованной Инспекционной конфигурации.



Соответствующий набор команд отправлен маршрутизатору.

22. Нажмите **OK** для завершения копирования набора команд к маршрутизатору.

23. Можно заметить, что новые правила, имеющие место от вкладки Firewall Policy Редактирования под, **Настраивают> Security> Межсетевой экран и ACL**.



Конфигурация командной строки маршрутизатора ZFW

Конфигурация в предыдущем разделе от CP Cisco приводит к этой конфигурации на маршрутизаторе ZFW:

Маршрутизатор 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#
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- **Policy-map type inspect ZBF-Router#show зонально-парные сеансы** — Отображают время выполнения, осматривает статистику policy-map типа для всех существующих

зональных пар.

Дополнительные сведения

- Дизайн и руководство по Zone-Based Policy межсетевому экрану
- Классический брандмауэр Cisco IOS и пример конфигурации приложения зонального виртуального брандмауэра
- Домашняя страница Cisco Configuration Professional
- Руководство пользователя Cisco Configuration Professional
- Cisco Systems – техническая поддержка и документация