Cisco Configuration Professional: Konfigurationsbeispiel für Peer-to-Peer-Datenverkehr durch eine zonenbasierte Firewall blockieren

Inhalt

Einführung

Dieses Dokument enthält eine schrittweise Anleitung zur Konfiguration eines Cisco IOS-Routers als zonenbasierte Firewall, um Peer-to-Peer (P2P)-Datenverkehr zu blockieren. Hierzu wird der erweiterte Firewall-Konfigurationsassistent im Cisco Configuration Professional (Cisco CP) verwendet.

Zonenbasierte Richtlinien-Firewall (auch als Zone-Policy Firewall oder ZFW bezeichnet) wandelt die Firewall-Konfiguration vom älteren schnittstellenbasierten Modell in ein flexibleres, besser verständliches zonenbasiertes Modell um. Schnittstellen werden Zonen zugewiesen, und die Überprüfungsrichtlinie wird auf Datenverkehr angewendet, der zwischen den Zonen fließt. Richtlinien für die Zonenübergreifende Zusammenarbeit bieten beträchtliche Flexibilität und Präzision. Aus diesem Grund können verschiedene Inspektionsrichtlinien auf mehrere Hostgruppen angewendet werden, die mit derselben Router-Schnittstelle verbunden sind. Zonen definieren die Sicherheitsgrenzen Ihres Netzwerks. Eine Zone definiert eine Grenze, an der der Datenverkehr Richtlinienbeschränkungen unterliegt, wenn er eine andere Region Ihres Netzwerks durchquert. Die ZFW-Standardrichtlinie zwischen Zonen lautet "Deny All" (Alle ablehnen). Wenn keine Richtlinie explizit konfiguriert ist, wird der gesamte Datenverkehr zwischen Zonen blockiert.

P2P-Anwendungen gehören zu den am häufigsten genutzten Anwendungen im Internet. P2P-Netzwerke können als Kanal für bösartige Bedrohungen wie Würmer fungieren und einen

einfachen Pfad um Firewalls anbieten, der Bedenken hinsichtlich Datenschutz und Sicherheit hervorruft. Mit der Cisco IOS Software-Version 12.4(9)T wurde die ZFW-Unterstützung für P2P-Anwendungen eingeführt. P2P Inspection bietet Layer-4- und Layer-7-Richtlinien für Anwendungsdatenverkehr. Das bedeutet, dass die ZFW eine grundlegende Stateful Inspection bereitstellen kann, um den Datenverkehr zuzulassen oder abzulehnen, sowie eine präzise Layer-7-Kontrolle bestimmter Aktivitäten in den verschiedenen Protokollen, sodass bestimmte Anwendungsaktivitäten zugelassen werden, während andere abgelehnt werden.

Cisco CP bietet einen einfachen, schrittweisen Ansatz zur Konfiguration des IOS-Routers als zonenbasierte Firewall mithilfe des erweiterten Firewall-Konfigurationsassistenten.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Die Softwareversion des IOS-Routers muss 12.4(9)T oder höher sein.
- Informationen zu IOS-Router-Modellen, die Cisco CP unterstützen, finden Sie in den Cisco CP-Versionshinweisen.

Routerkonfiguration zum Ausführen des Cisco CP

Hinweis: Führen Sie folgende Konfigurationsschritte durch, um Cisco CP auf einem Cisco Router auszuführen:

```
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
```

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco 1841 IOS-Router mit IOS-Softwareversion 12.4(15)T
- Cisco Configuration Professional (Cisco CP) Version 2.1

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Im Beispiel dieses Dokuments ist der Router als zonenbasierte Firewall konfiguriert, um den P2P-Datenverkehr zu blockieren. Der ZFW-Router verfügt über zwei Schnittstellen: eine interne(vertrauenswürdige) Schnittstelle in der In-Zone und eine externe (nicht vertrauenswürdige) Schnittstelle in der Out-Zone. Der ZFW-Router blockiert P2P-Anwendungen wie edonkey, fasttrack, gnutella und kazaa2 mit Protokollierungsaktionen für den Datenverkehr, der von In-Zone zur Out-Zone fließt.

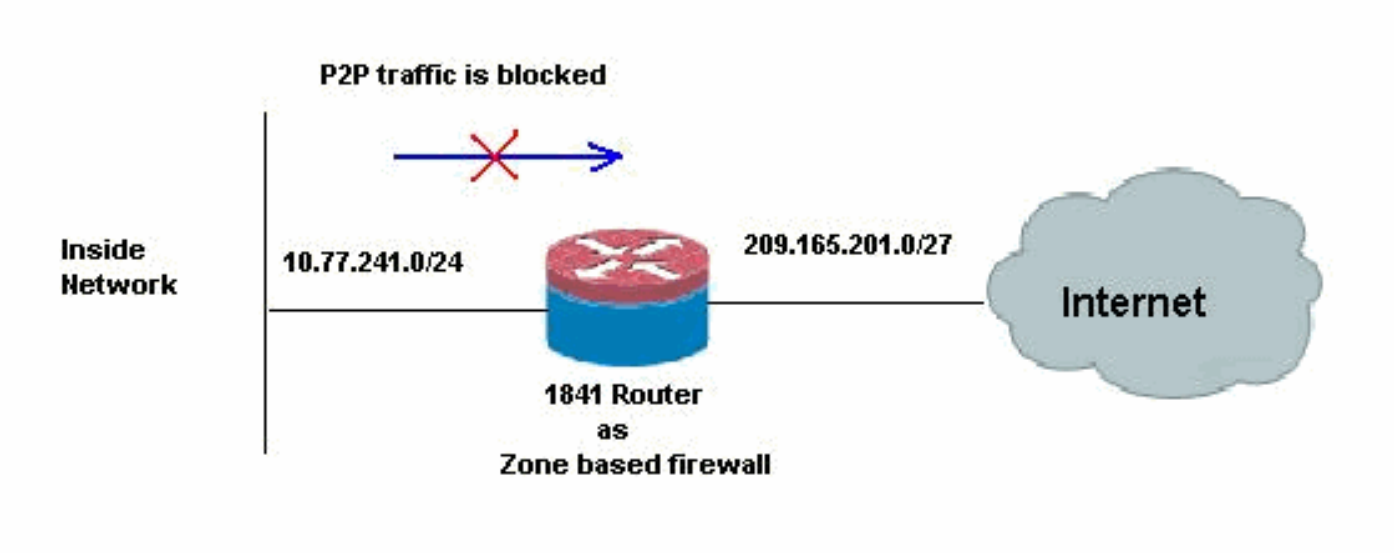
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

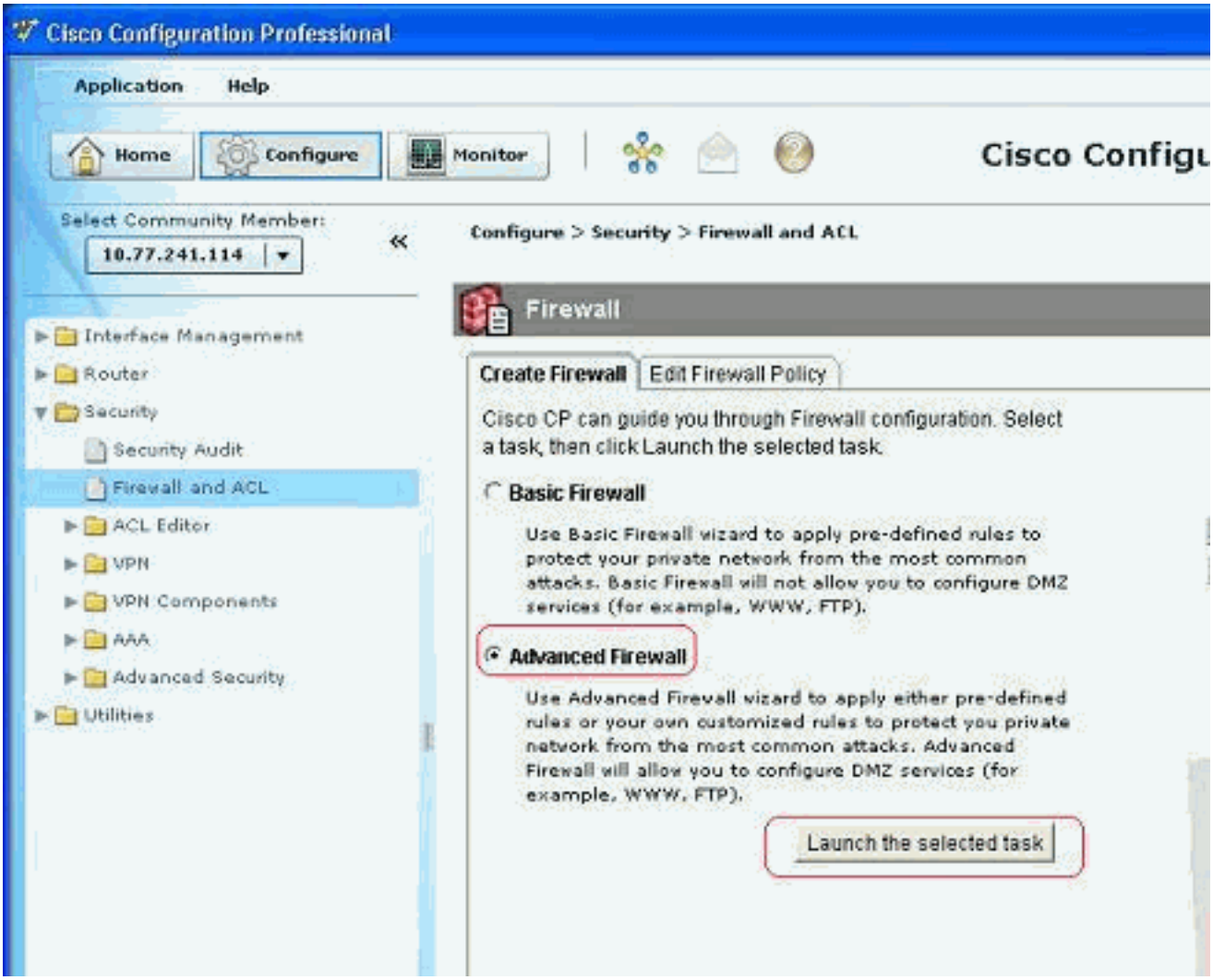


Konfiguration über Cisco Configuration Professional

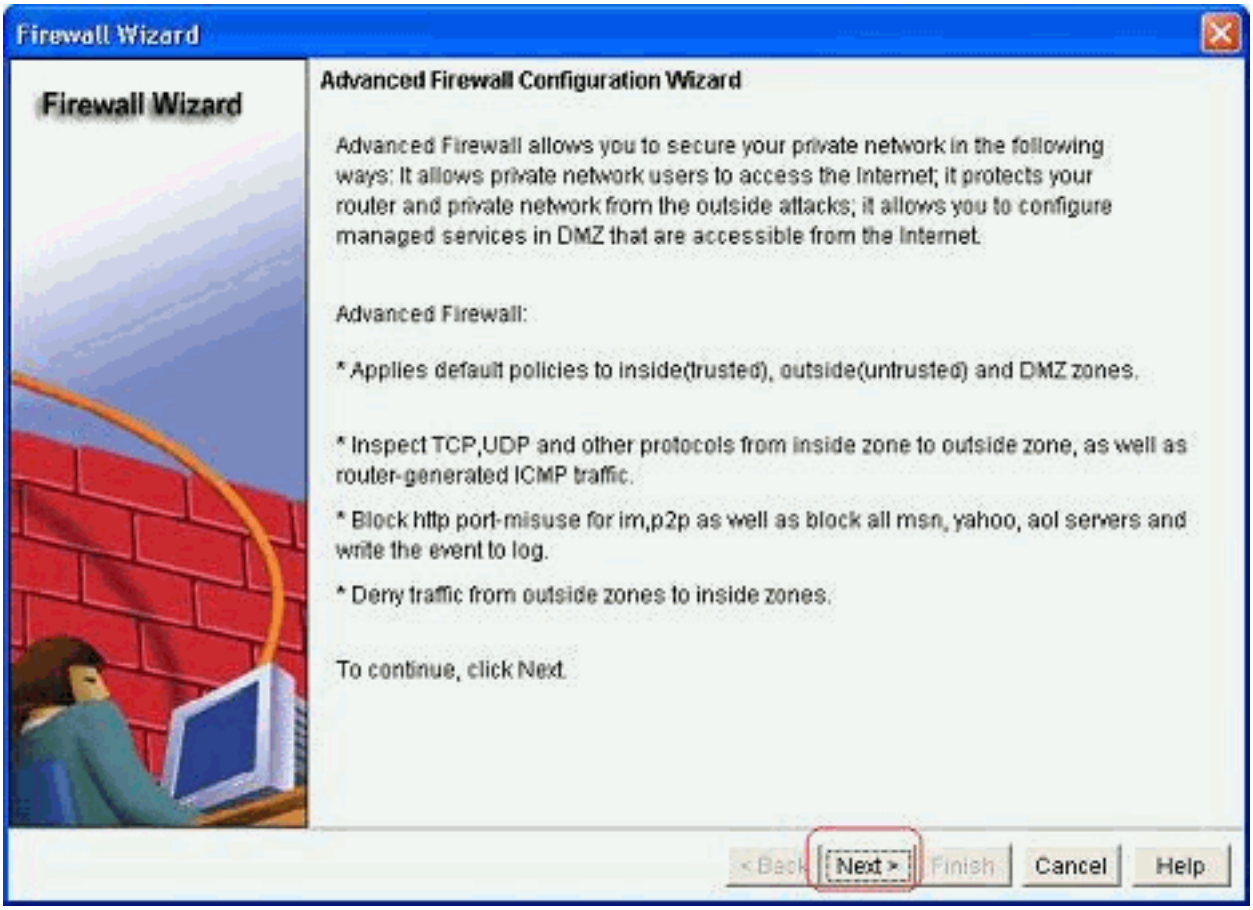
Dieser Abschnitt enthält eine schrittweise Anleitung zur Verwendung des Assistenten zum Konfigurieren des IOS-Routers als zonenbasierte Firewall.

Gehen Sie wie folgt vor:

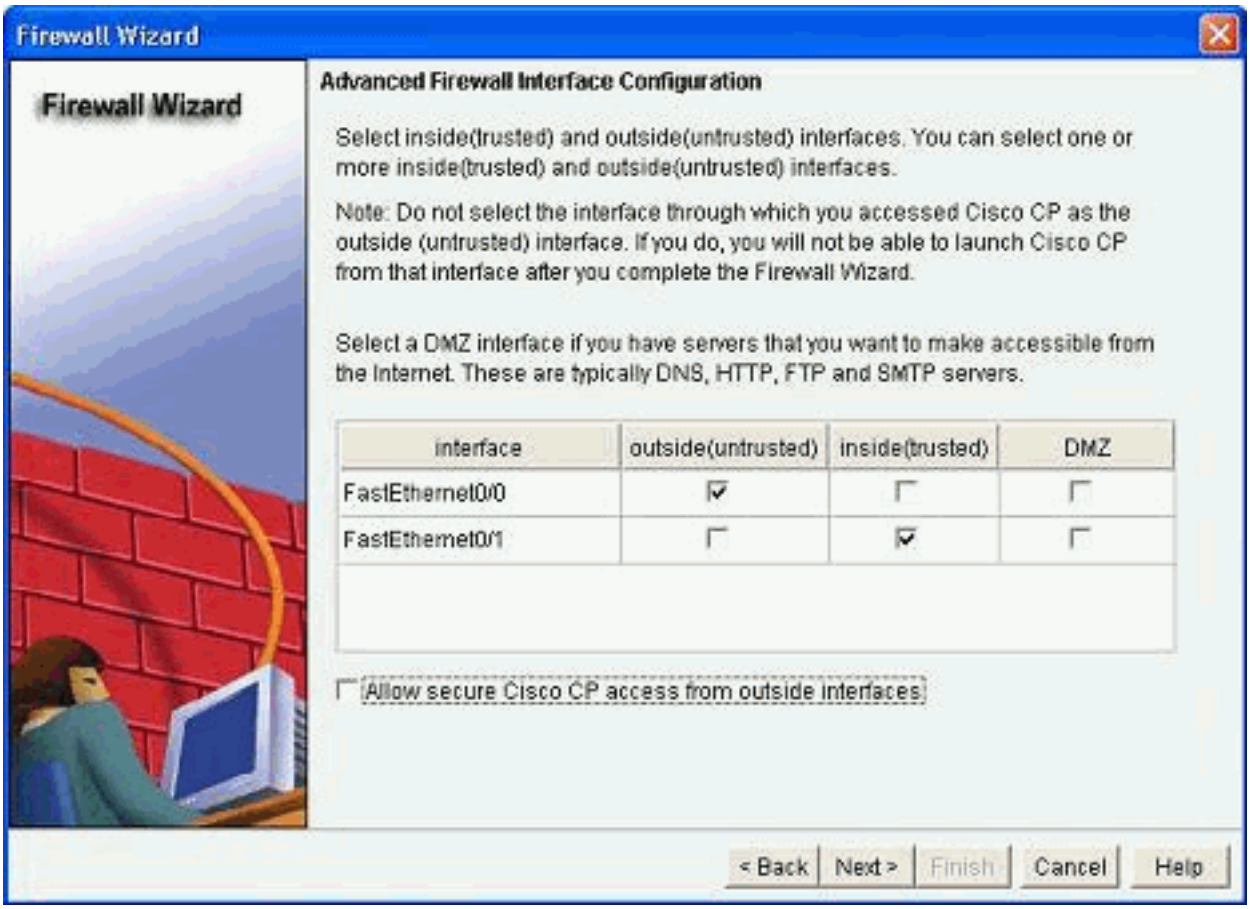
1. Gehen Sie zu **Konfigurieren > Sicherheit > Firewall und ACL**. Wählen Sie anschließend das Optionsfeld **Erweiterte Firewall**. Klicken Sie auf **Ausgewählte Aufgabe starten**.



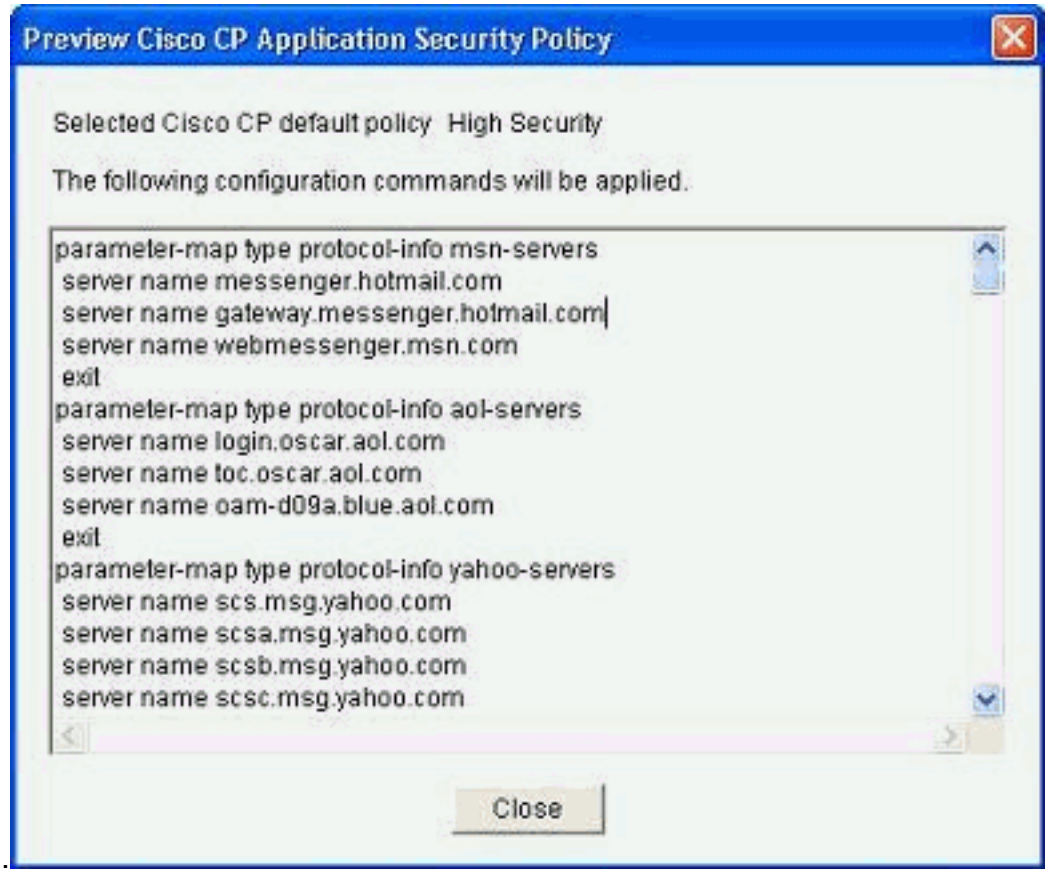
2. Im nächsten Bildschirm wird eine kurze Einführung zum Firewall-Assistenten angezeigt. Klicken Sie auf **Weiter**, um die Konfiguration der Firewall zu starten.



3. Wählen Sie die Schnittstellen des Routers aus, der zu Zonen gehören soll, und klicken Sie auf
Weiter.

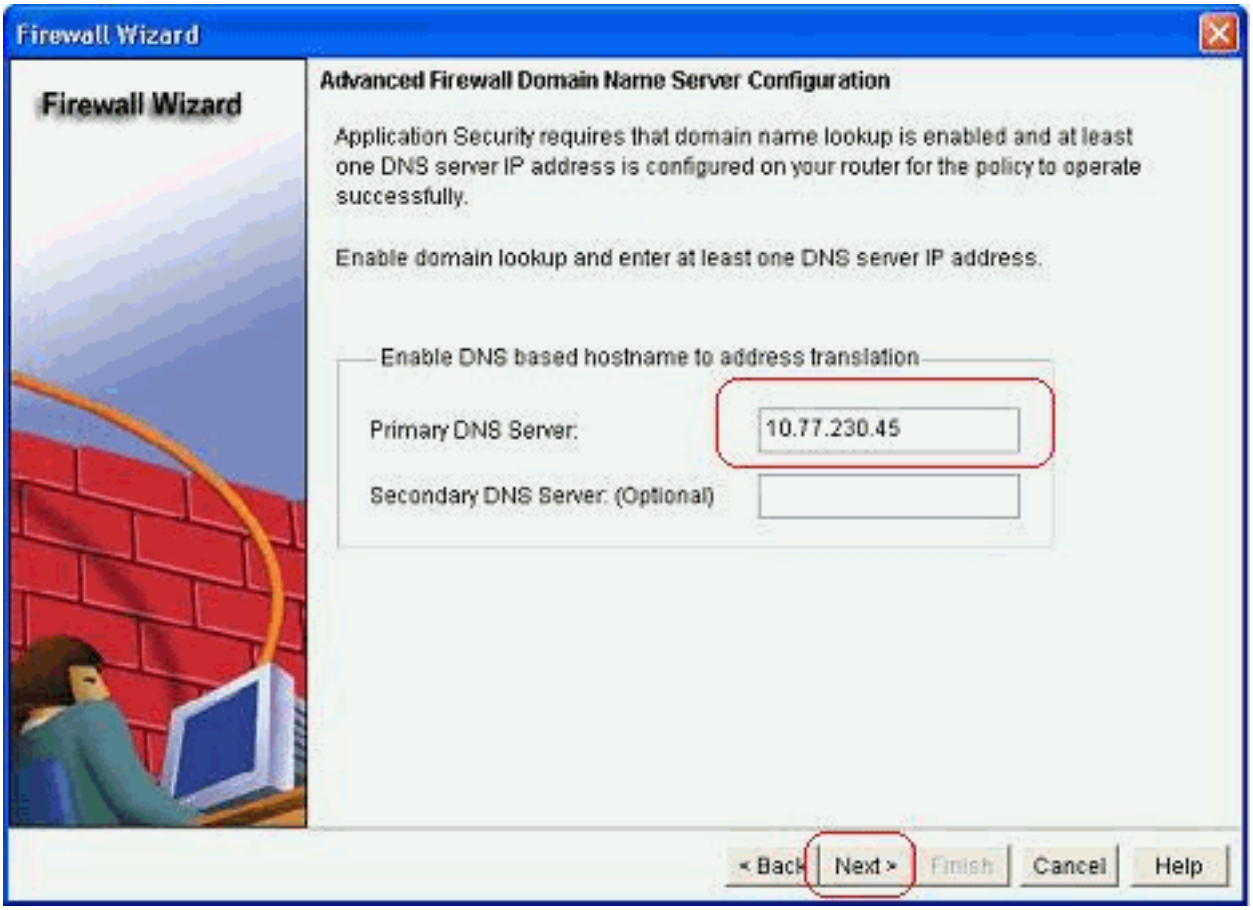


4. Im nächsten Fenster wird die Standardrichtlinie mit hoher Sicherheit zusammen mit dem Befehlssatz angezeigt. Klicken Sie auf **Schließen**, um

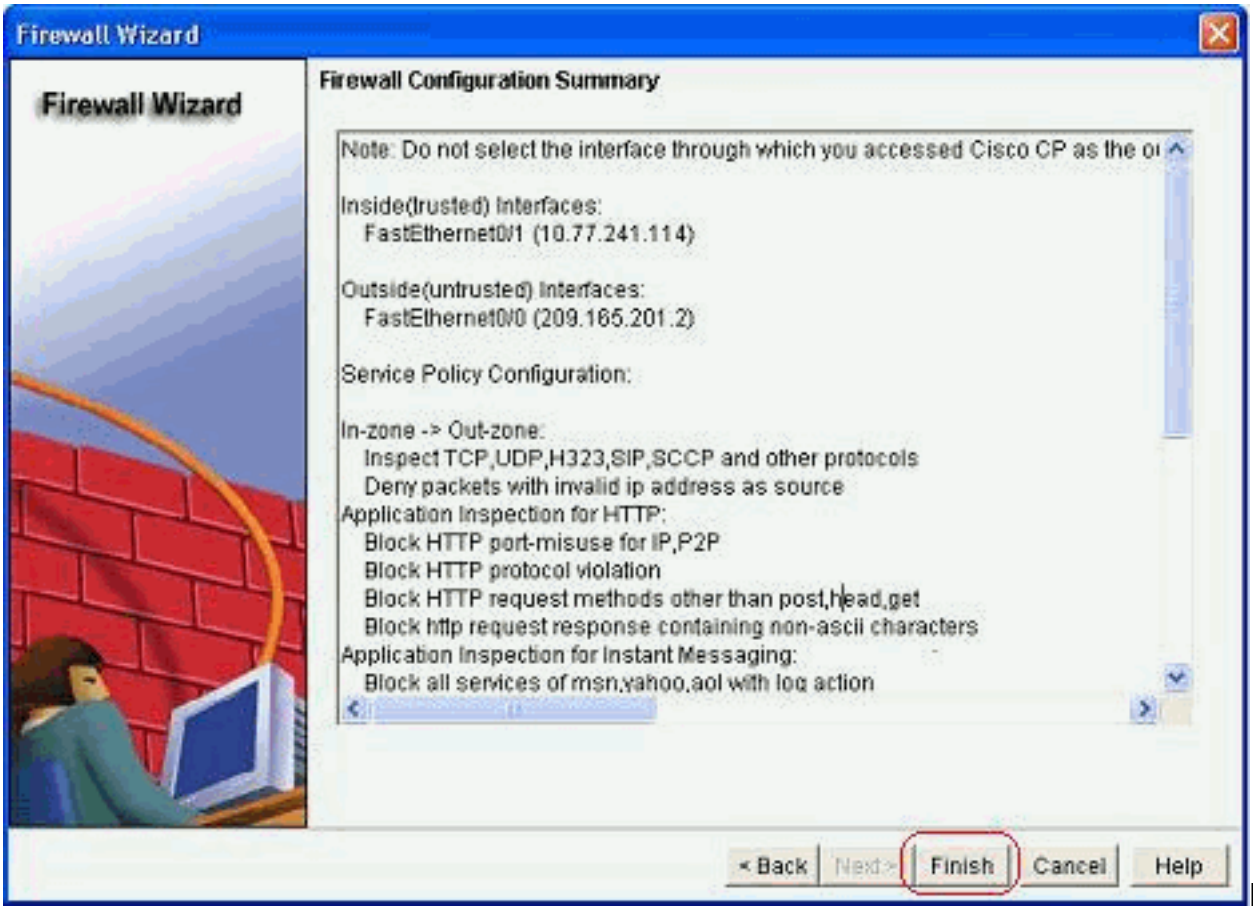


fortzufahren.

5. Geben Sie die Details des DNS-Servers ein, und klicken Sie auf **Weiter**.

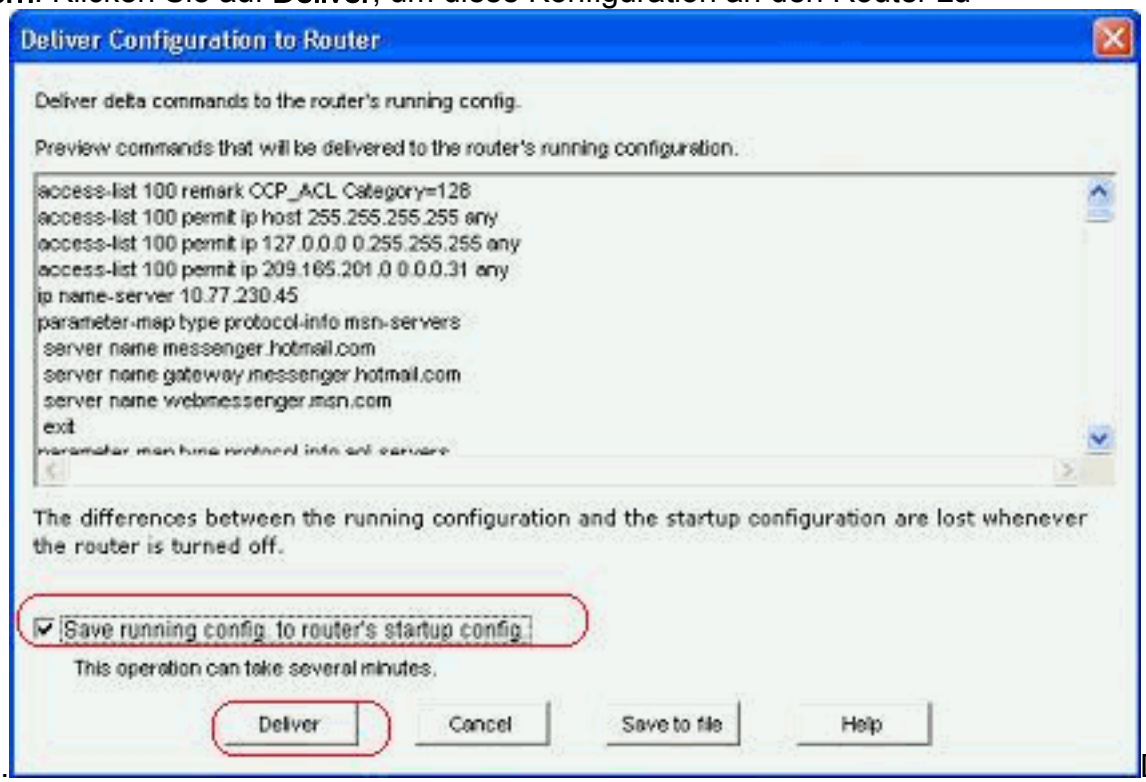


6. Der Cisco CP bietet eine Konfigurationsübersicht, wie hier gezeigt. Klicken Sie auf **Fertig stellen**, um die Konfiguration abzuschließen.

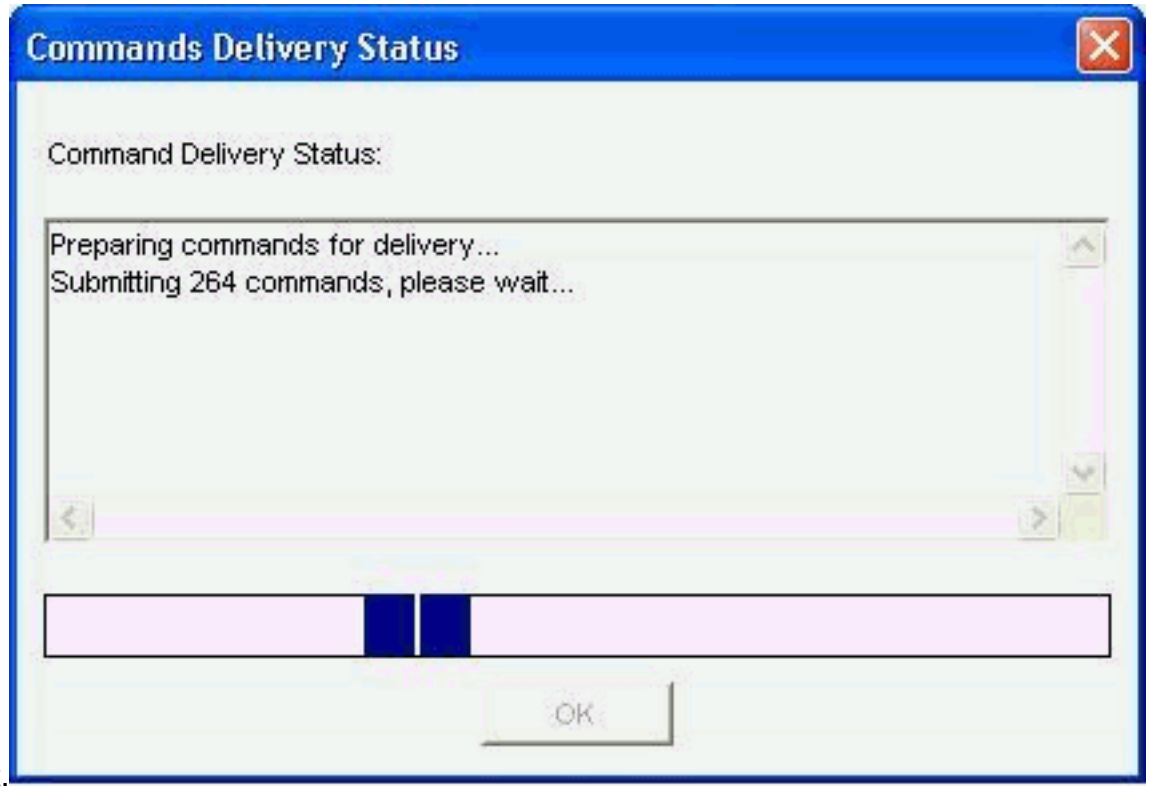


Die detaillierte Konfigurationsübersicht ist in dieser Tabelle enthalten. Dies ist die Standardkonfiguration gemäß der High Security Policy des Cisco CP.

7. Aktivieren Sie das Kontrollkästchen **Laufende Konfiguration in Startkonfiguration des Routers speichern**. Klicken Sie auf **Deliver**, um diese Konfiguration an den Router zu senden.

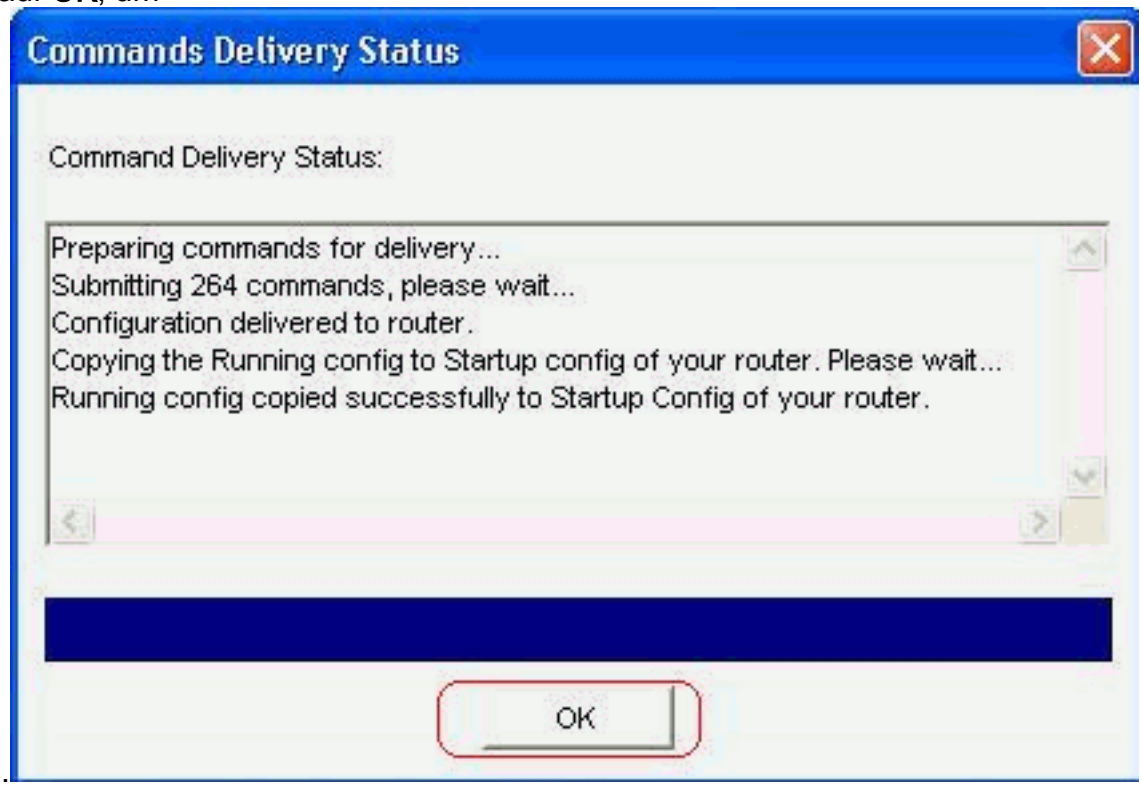


Die gesamte Konfiguration wird an den Router übermittelt. Dies erfordert einige



Zeit.

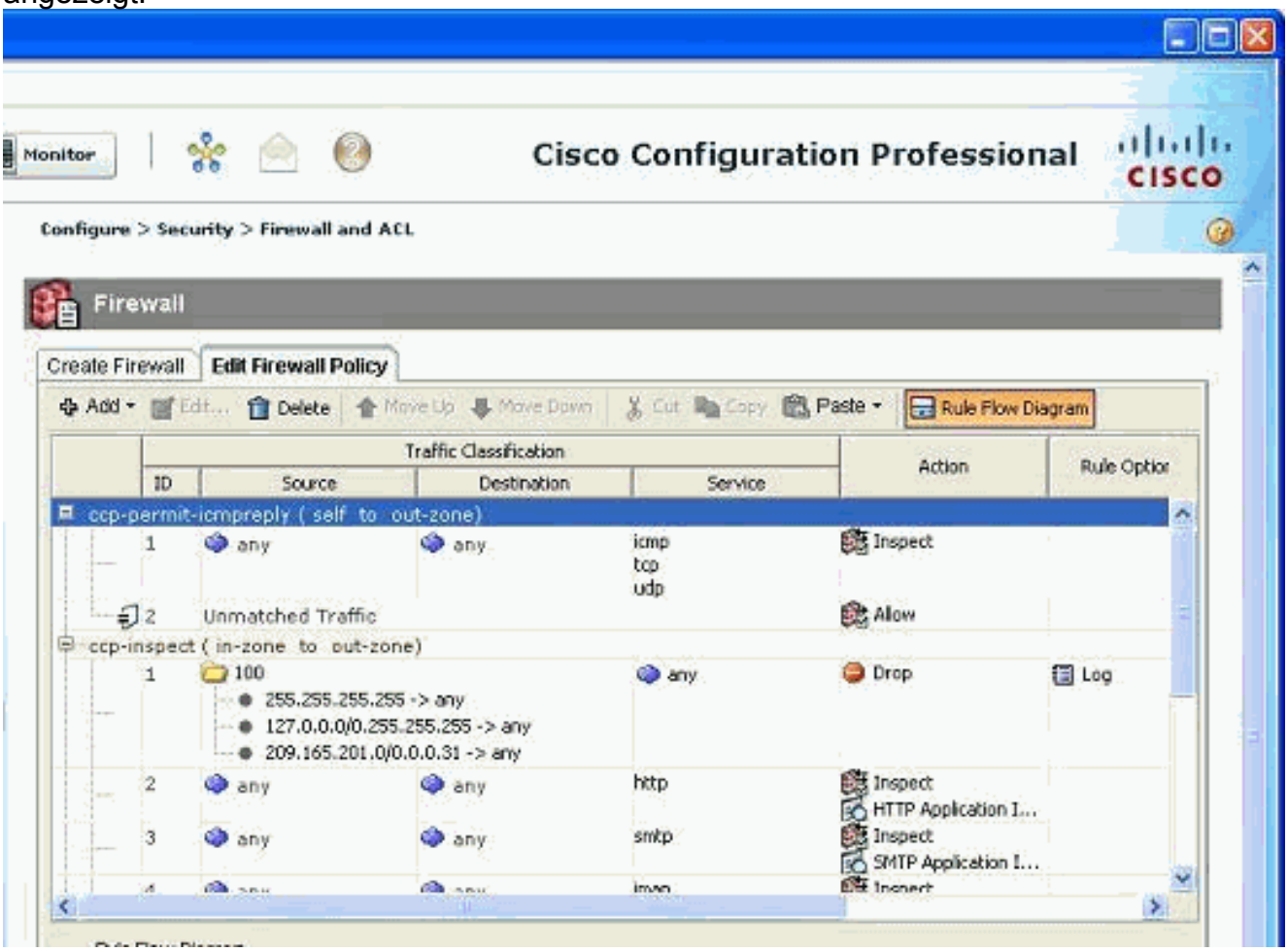
8. Klicken Sie auf **OK**, um



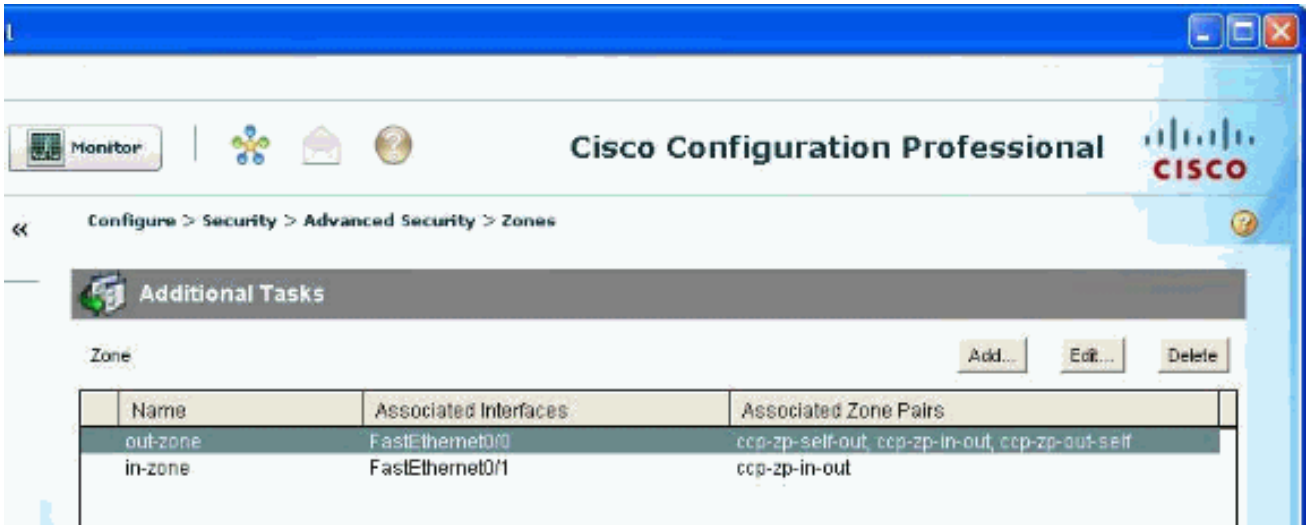
fortzufahren.

9. Klicken Sie erneut auf

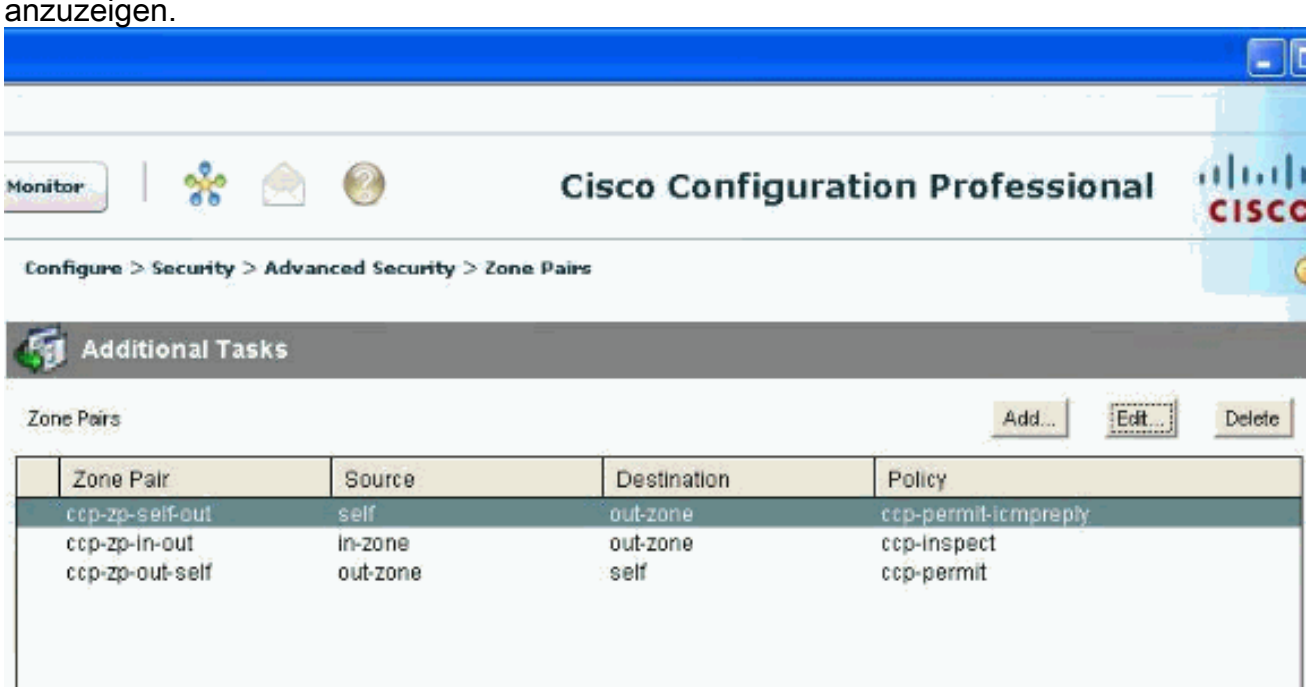
OK.Die Konfiguration ist nun in Kraft und wird als Regeln auf der Registerkarte "Firewall Policy" (Firewall-Richtlinien)
angezeigt.



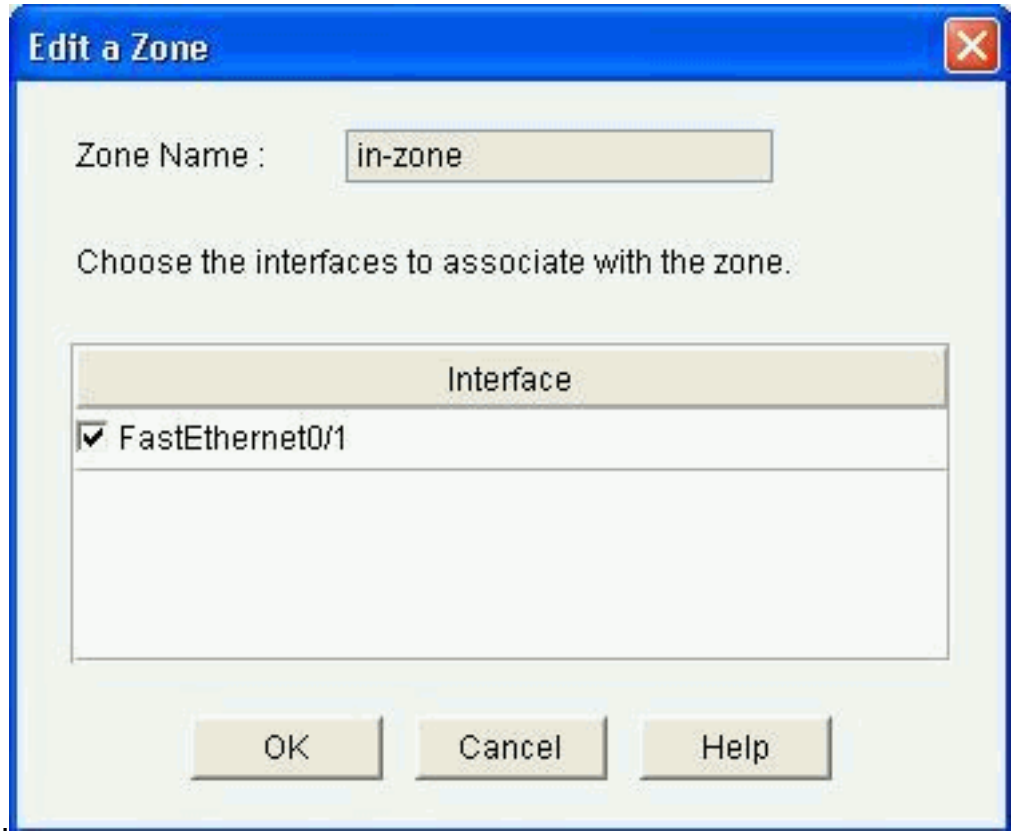
10. Die Zonen und die Zonenpaare, denen sie zugeordnet sind, können angezeigt werden, wenn Sie **Configure > Security > Advanced Security > Zones** wählen. Sie können auch neue Zonen hinzufügen, indem Sie auf **Hinzufügen** klicken, oder die vorhandenen Zonen ändern, indem Sie auf **Bearbeiten**
klicken.



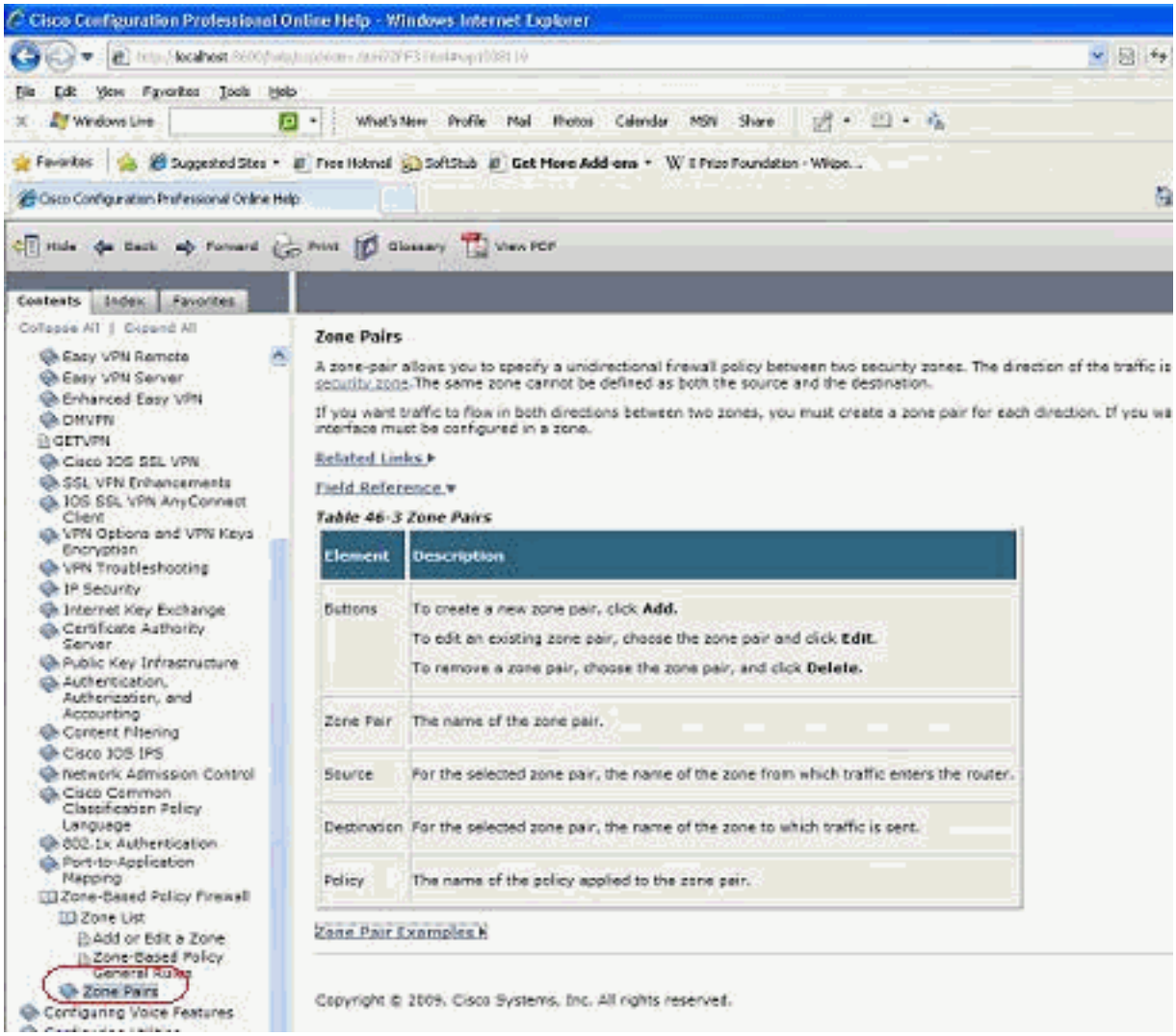
11. Gehen Sie zu **Konfigurieren > Sicherheit > Erweiterte Sicherheit > Zonenpaare**, um die Details der Zonenpaare anzuzeigen.



Auf den integrierten Webseiten im Cisco CP finden Sie sofortige Hilfe zum Ändern/Hinzufügen/Löschen von Zonen/Zonenpaaren und anderen verwandten

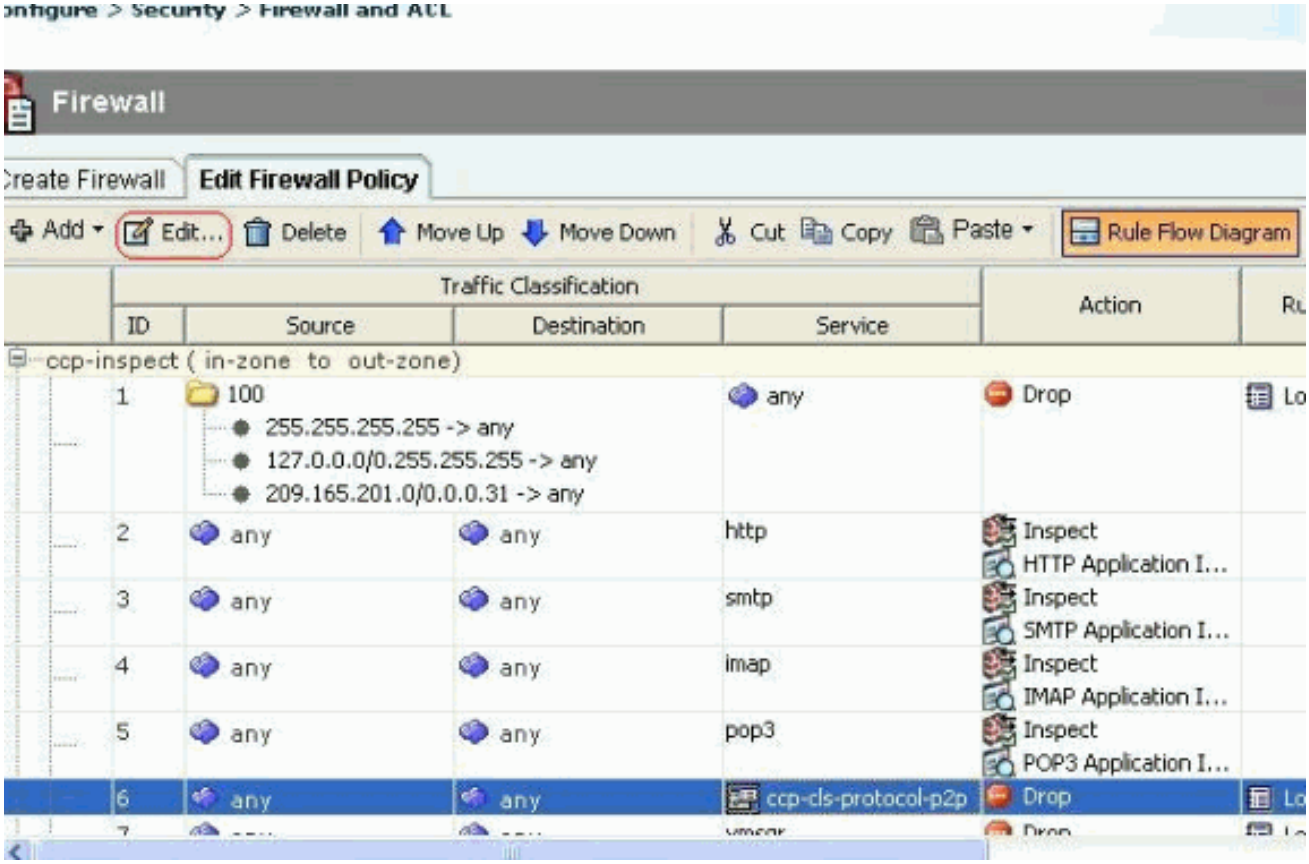


Informationen.

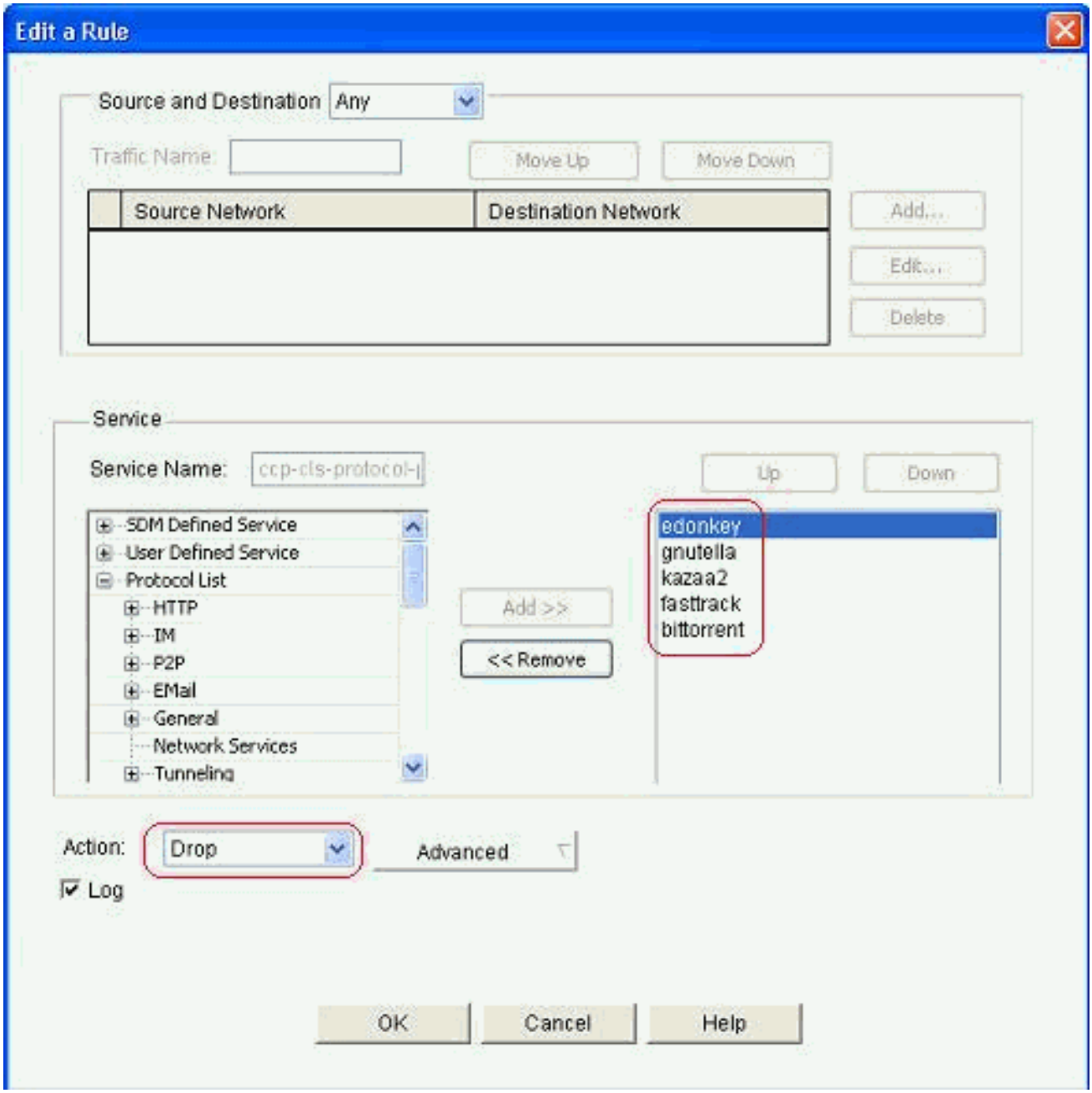


12. Um die anwendungsspezifischen Prüffunktionen für bestimmte P2P-Anwendungen zu ändern, gehen Sie zu **Konfiguration > Sicherheit > Firewall und ACL**. Klicken Sie dann auf **Firewall-Richtlinie bearbeiten** und wählen Sie die entsprechende Regel in der

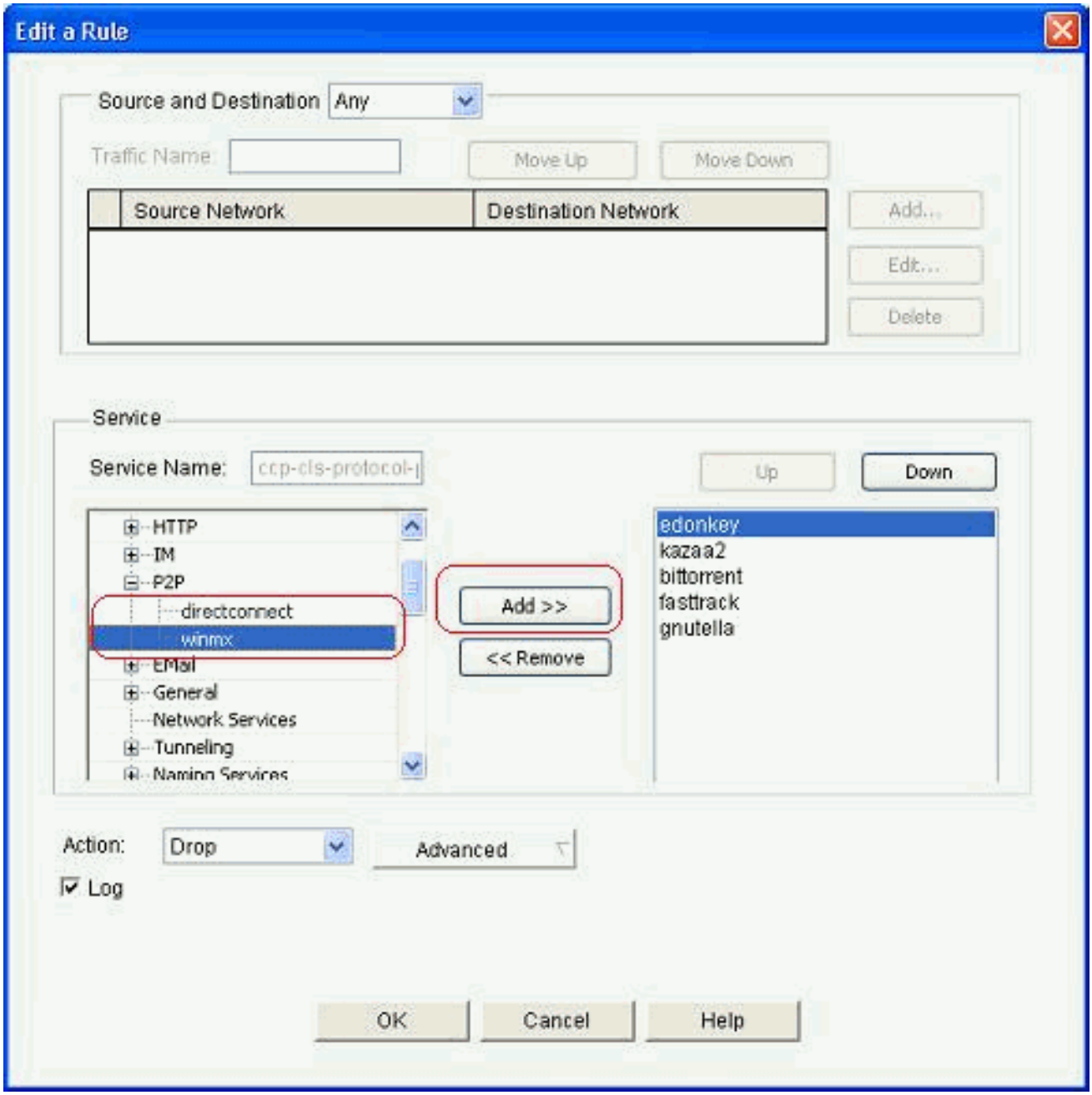
Richtlinienzuordnung aus. Klicken Sie auf **Bearbeiten**.

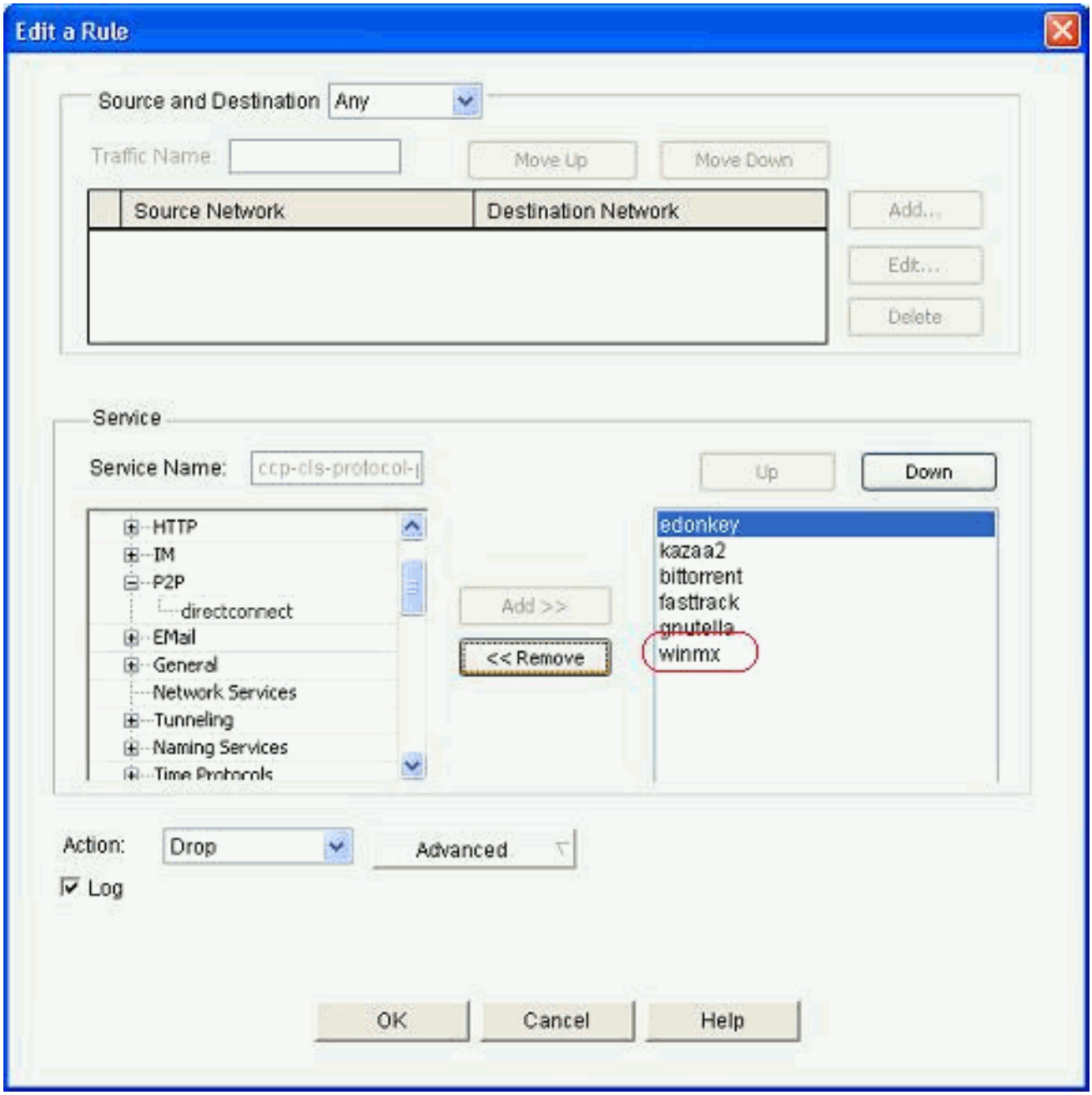


Dies zeigt die aktuellen P2P-Anwendungen, die durch die Standardkonfiguration blockiert werden.

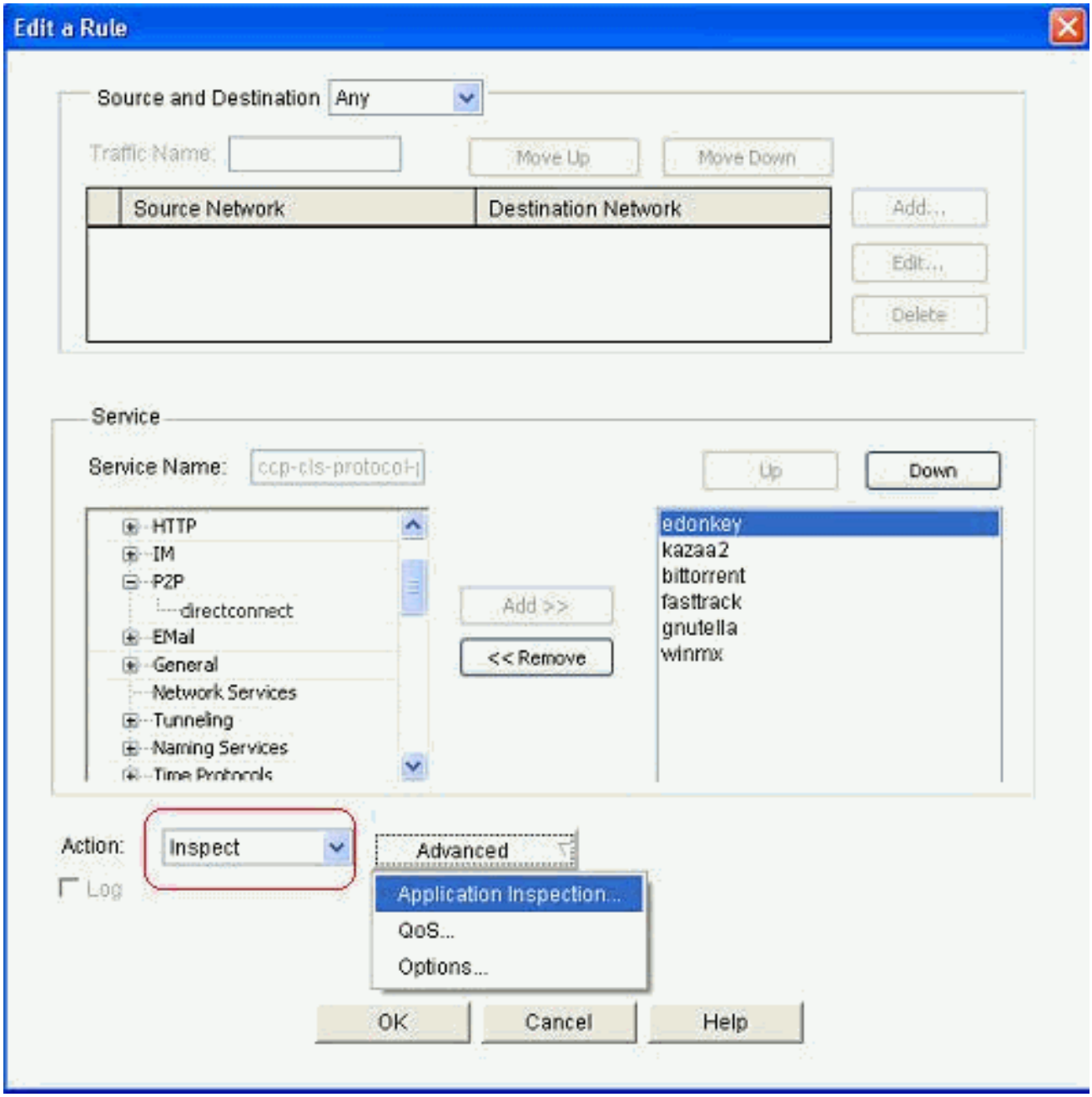


13. Sie können die Schaltflächen Hinzufügen und Entfernen verwenden, um bestimmte Anwendungen hinzuzufügen bzw. zu entfernen. Dieser Screenshot zeigt, wie Sie die winmx-Anwendung hinzufügen, um dies zu blockieren.


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

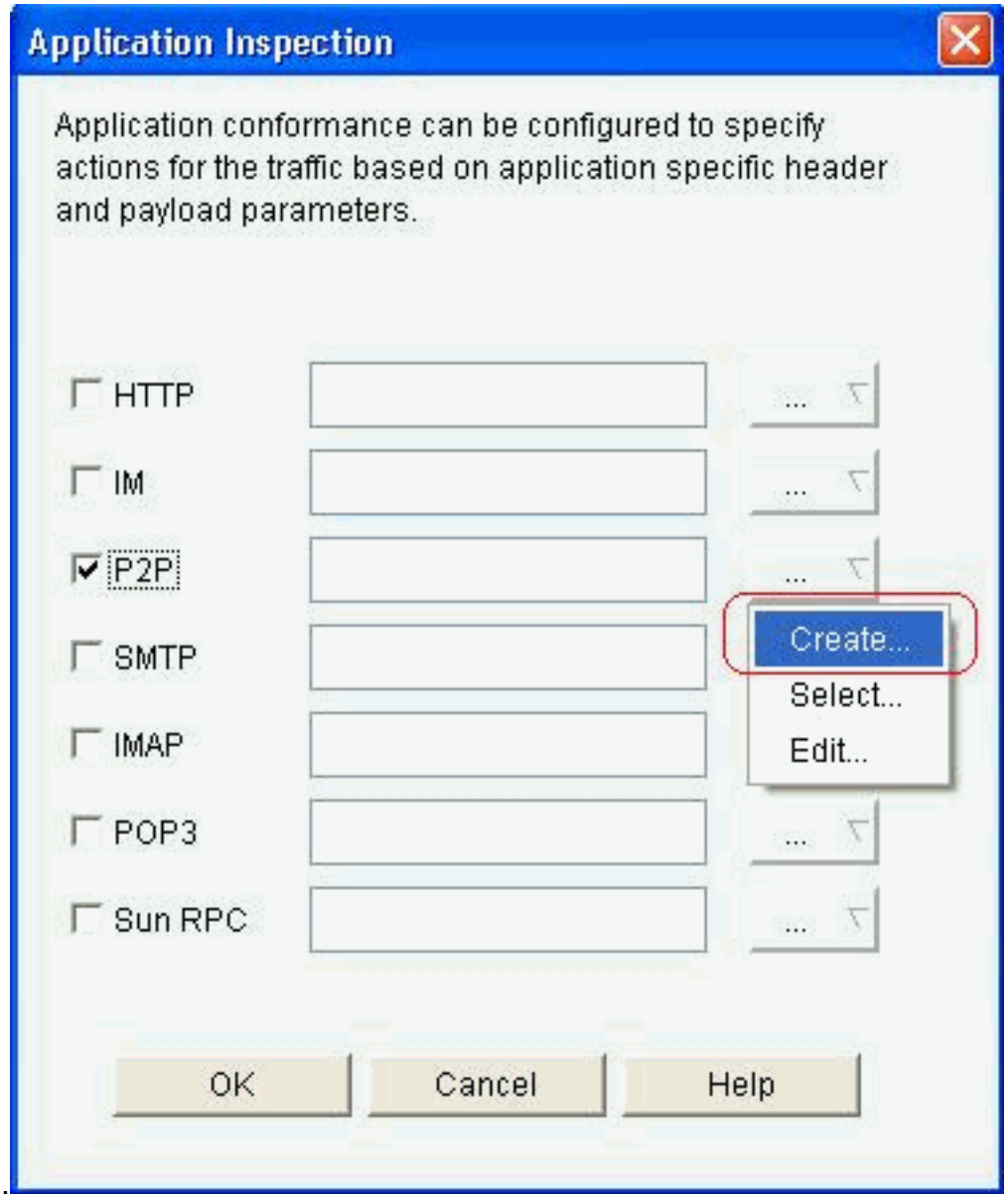


14. Anstatt die Drop-Aktion auszuwählen, können Sie auch die Inspect-Aktion auswählen, um verschiedene Optionen für die Deep Packet Inspection anzuwenden.



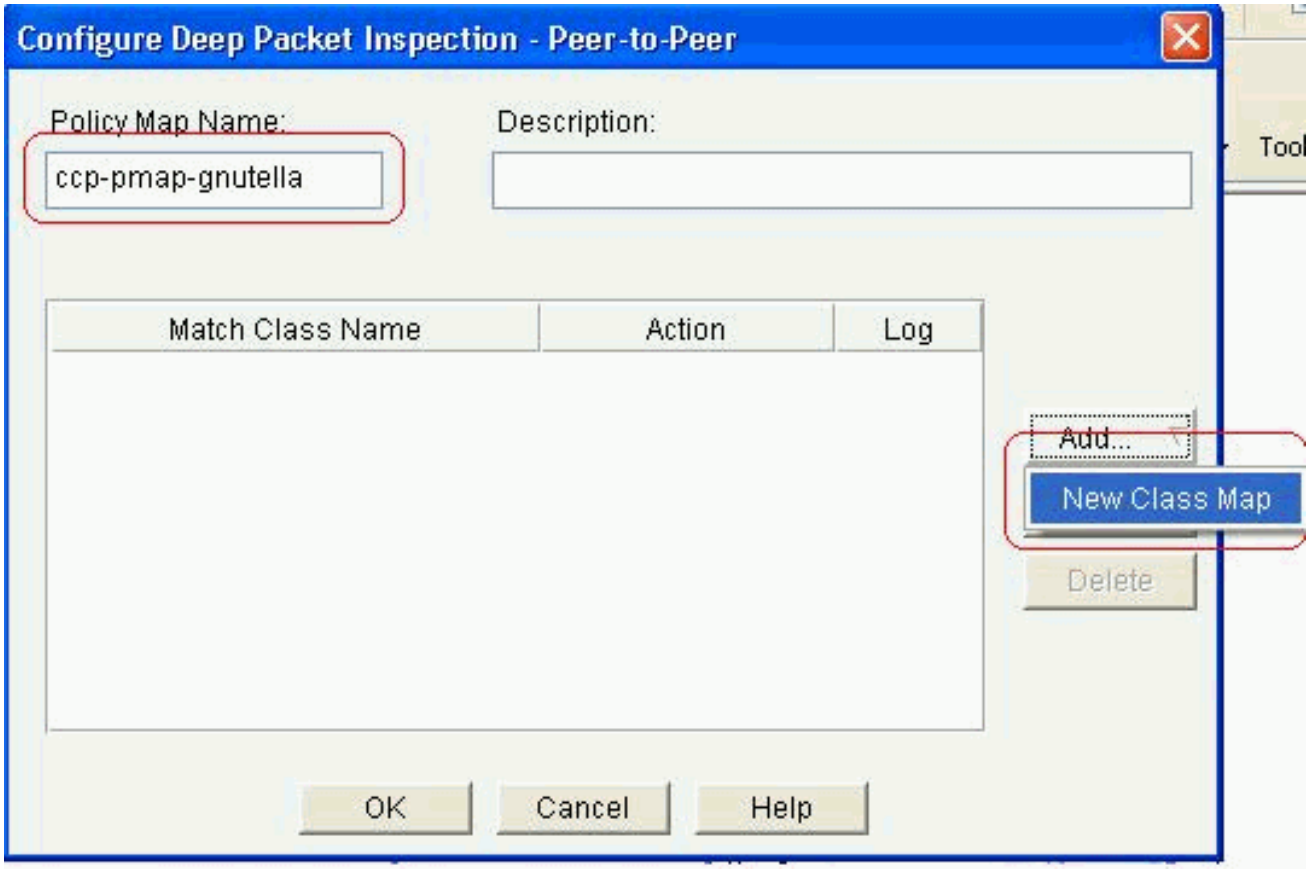
P2P Inspection bietet Layer-4- und Layer-7-Richtlinien für Anwendungsdatenverkehr. Das bedeutet, dass die ZFW eine grundlegende Stateful Inspection bereitstellen kann, um den Datenverkehr zuzulassen oder abzulehnen, sowie eine präzise Layer-7-Kontrolle bestimmter Aktivitäten in den verschiedenen Protokollen, sodass bestimmte Anwendungsaktivitäten zugelassen werden, während andere abgelehnt werden. Bei dieser Anwendungsinspektion können Sie für P2P-Anwendungen verschiedene Arten von spezifischen Überprüfungen auf Kopfzeilenebene anwenden. Ein Beispiel für die Gnutella wird nachfolgend gezeigt.

15. Aktivieren Sie die **P2P-**Option, und klicken Sie auf **Erstellen**, um eine neue Richtlinienzuweisung zu

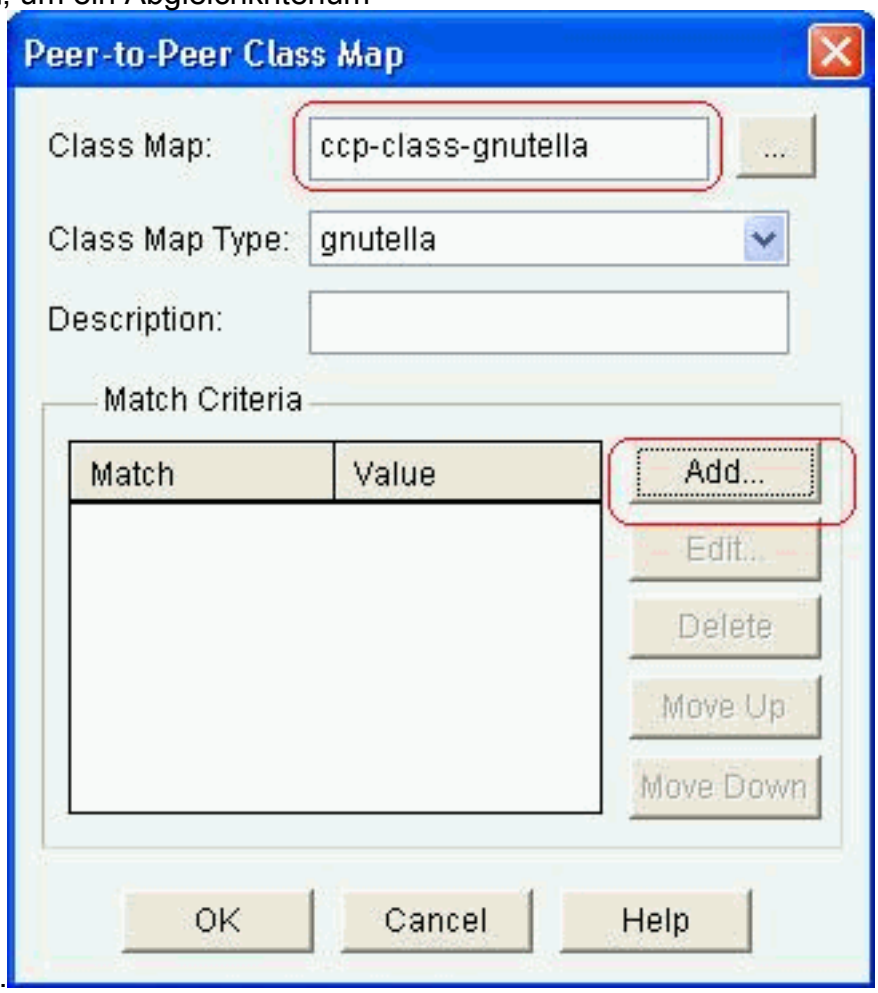


erstellen.

16. Erstellen Sie eine neue Policy-Map für die Deep Packet Inspection für das gnutella-Protokoll. Klicken Sie auf **Hinzufügen** und wählen Sie dann **Neue Klassenzuordnung**.



17. Geben Sie einen neuen Namen für die Klassenzuordnung an, und klicken Sie auf **Hinzufügen**, um ein Abgleichkriterium anzugeben.

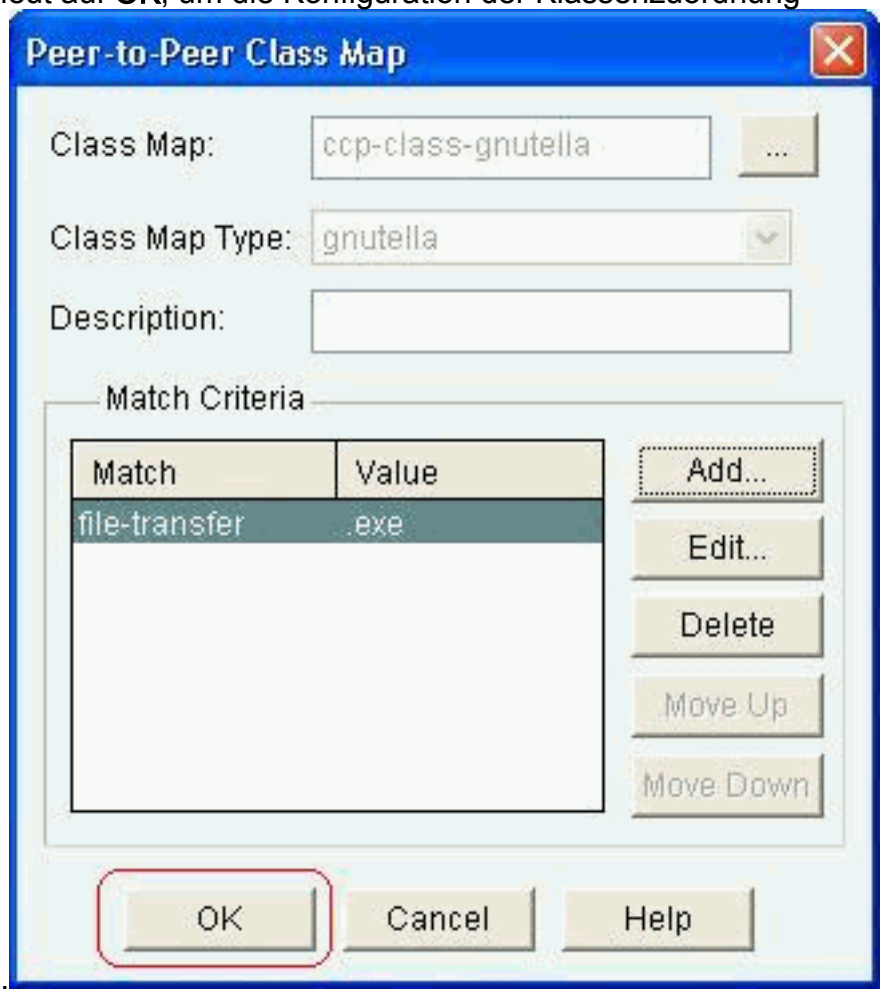


18. Verwenden Sie die Dateiübertragung als Übereinstimmungskriterium, und die verwendete Zeichenfolge ist .exe. Dies zeigt an, dass alle GNUELLA-Dateiübertragungsverbindungen,

die die .exe-Zeichenfolge enthalten, mit der Datenverkehrsrichtlinie übereinstimmen.

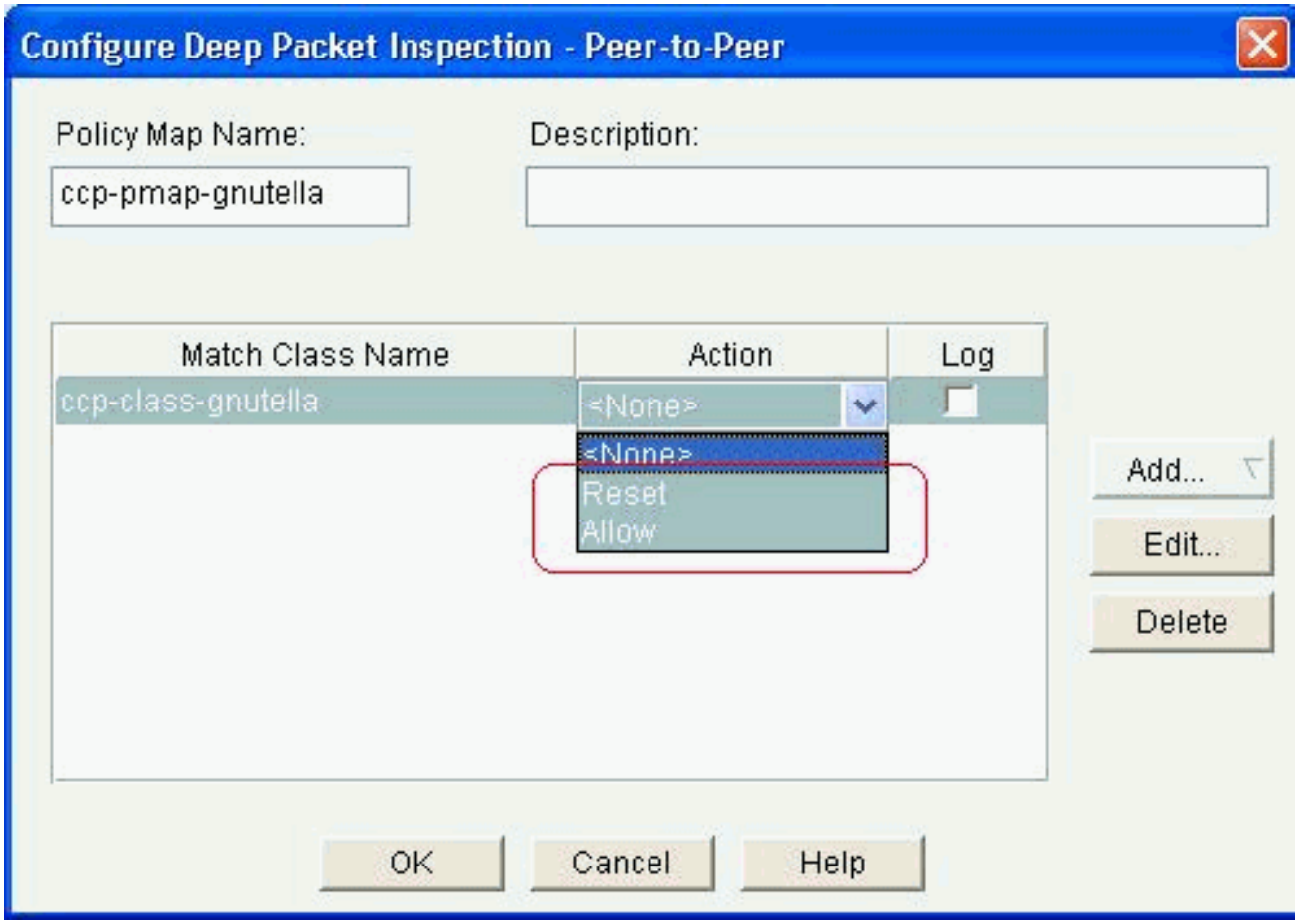
Klicken Sie auf **OK**.

19. Klicken Sie erneut auf **OK**, um die Konfiguration der Klassenzuordnung



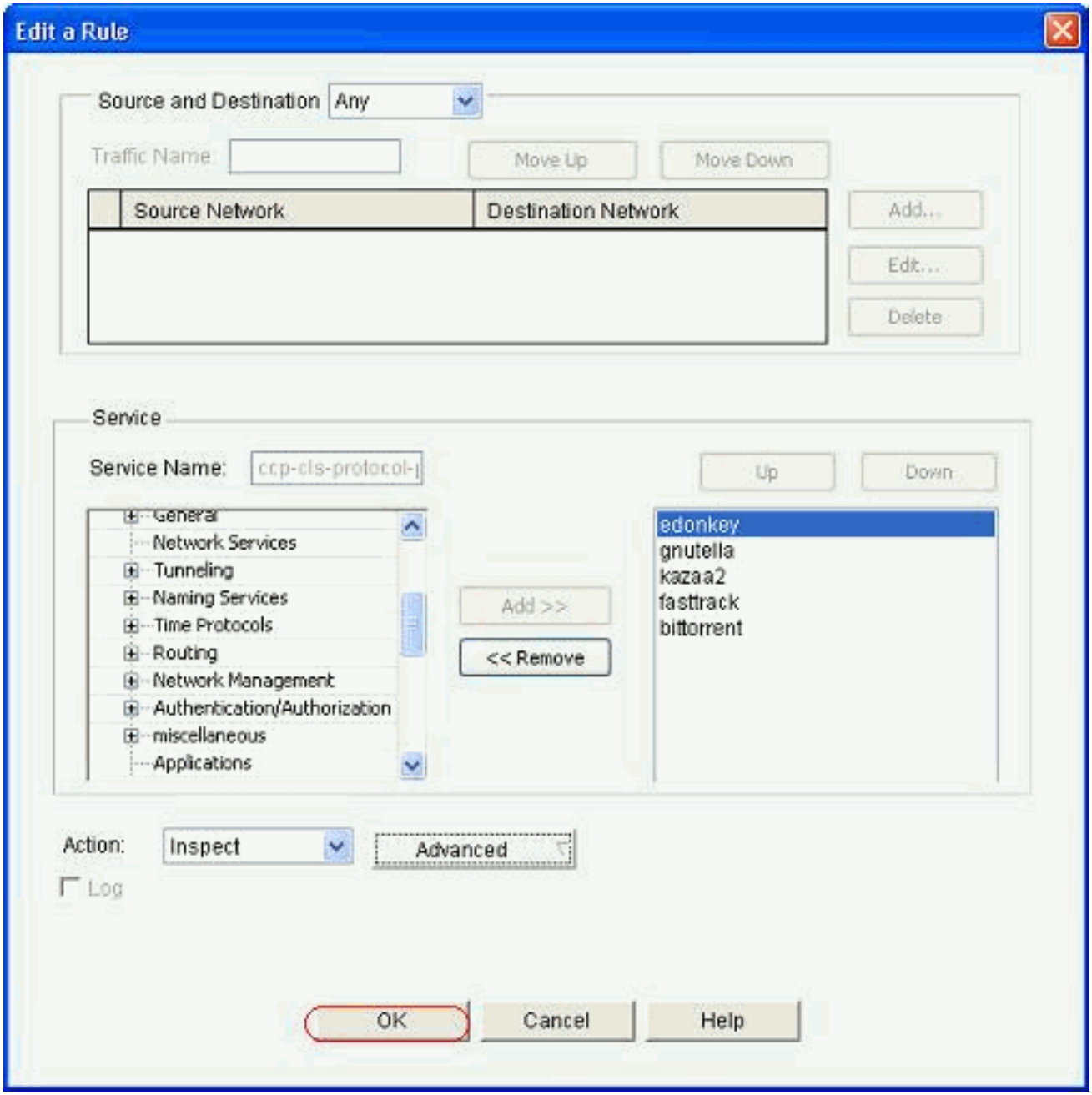
abzuschließen.

20. Wählen Sie die Option **Reset** oder **Allow (Zurücksetzen)** aus, die von den Sicherheitsrichtlinien Ihres Unternehmens abhängt. Klicken Sie auf **OK**, um die Aktion in der Richtlinienzuordnung zu bestätigen.



Auf diese Weise können Sie weitere Richtlinienzuordnungen hinzufügen, um tief greifende Inspektionsfunktionen für andere P2P-Protokolle zu implementieren, indem Sie unterschiedliche reguläre Ausdrücke als Anpassungskriterium angeben.**Hinweis:** P2P-Anwendungen sind aufgrund des "Port-Hopping"-Verhaltens und anderer Tricks zur Vermeidung von Erkennungen besonders schwer zu erkennen, ebenso wie Probleme, die durch häufige Änderungen und Aktualisierungen von P2P-Anwendungen entstehen, die das Verhalten der Protokolle ändern. Die ZFW kombiniert native Stateful Inspection-Prozesse mit Network-Based Application Recognition (NBAR)-Funktionen zur Erkennung des Datenverkehrs und bietet so eine P2P-Anwendungskontrolle.**Hinweis:** P2P Application Inspection bietet anwendungsspezifische Funktionen für einen Teil der Anwendungen, die von Layer 4 Inspection unterstützt werden:EtonschlüsselSchnellspurGnutellaKazaa2**Hinweis:** Zurzeit hat die ZFW keine Möglichkeit, den "Bittorrent"-Anwendungsdatenverkehr zu überprüfen. BitTorrent-Clients kommunizieren normalerweise mit Trackern (Peer-Directory-Server) über HTTP, das auf einem nicht standardmäßigen Port ausgeführt wird. Dies ist normalerweise TCP 6969, aber Sie müssen möglicherweise den torrent-spezifischen Tracker-Port überprüfen. Wenn Sie BitTorrent zulassen möchten, ist die beste Methode für den zusätzlichen Port, HTTP als eines der Übereinstimmungsprotokolle zu konfigurieren und TCP 6969 mit dem folgenden Befehl ip port-map zu HTTP hinzuzufügen: **ip port-map http port tcp 6969**. Sie müssen http und bitTorrent als die in der Klassenzuordnung angewendeten Anpassungskriterien definieren.

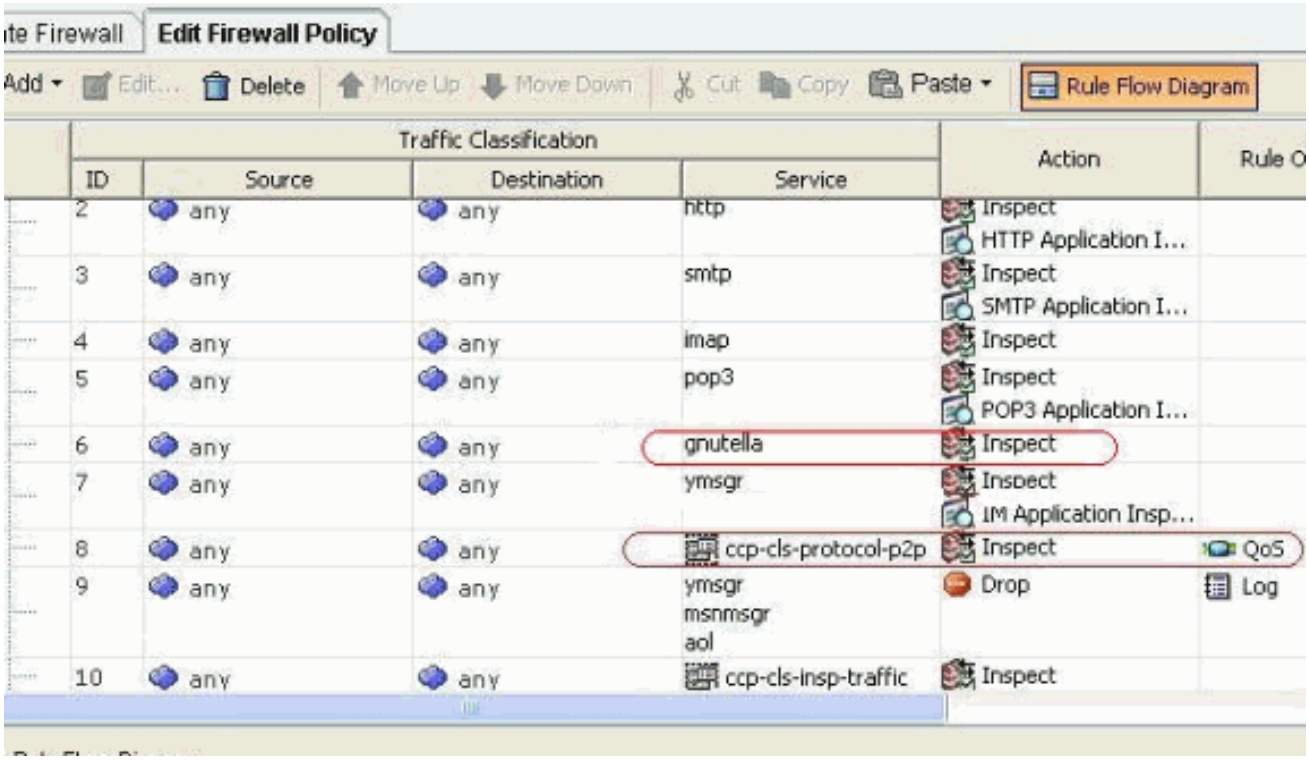
21. Klicken Sie auf **OK**, um die Konfiguration der erweiterten Überprüfung abzuschließen.



Der entsprechende Befehlssatz wird an den Router übermittelt.

22. Klicken Sie auf **OK**, um das Kopieren der Befehlssätze auf den Router abzuschließen.

23. Sie können die neuen Regeln auf der Registerkarte "Edit Firewall Policy" (Firewall-Richtlinie bearbeiten) unter **Configure (Konfigurieren) > Security (Sicherheit) > Firewall (Firewall) und ACL (Zugriffskontrollliste)**
beobachten.



Befehlszeilenkonfiguration des ZFW-Routers

Die Konfiguration im vorherigen Abschnitt des Cisco CP führt zu dieser Konfiguration auf dem ZFW-Router:

ZBF-Router

```
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#
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- ZBF-Router#**show policy-map type inspect zone-pair sessions** - Zeigt die Statistiken zur

Typrichtlinienzuordnung der Laufzeit für alle vorhandenen Zonenpaare an.

Zugehörige Informationen

- Firewall-Design und Anwendungshandbuch für zonenbasierte Richtlinien
- Konfigurationsbeispiel für die klassische und zonenbasierte virtuelle Firewall der Cisco IOS Firewall
- Cisco Configuration Professional - Startseite