ASA 8.3 en later: Stel SSH/telnet/HTTP-verbinding in met behulp van MPF-configuratievoorbeeld

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor Cisco adaptieve security applicatie (ASA) met versie 8.3(1) en hoger van een tijdelijke oplossing die specifiek is voor een bepaalde toepassing zoals SSH/telnet/HTTP, in tegenstelling tot een applicatie die van toepassing is op alle toepassingen. Dit configuratievoorbeeld gebruikt het modulaire beleidskader (MPF) dat in Cisco adaptieve security applicatie (ASA) versie 7.0 is geïntroduceerd. Raadpleeg het modulaire beleidskader gebruiken voor meer informatie.

In deze voorbeeldconfiguratie is Cisco ASA geconfigureerd om het werkstation (10.77.241.129) toe te staan aan telnet/SSH/HTTP naar de externe server (10.1.1.1) achter de router. Er wordt ook een afzonderlijke verbindingstijd ingesteld voor Telnet/SSH/HTTP-verkeer. Al het andere TCP verkeer blijft de normale waarde van de verbinding tijd hebben verbonden aan **timeout conn 1:00:00**.

Raadpleeg PIX/ASA 7.x en hoger/FWSM: Stel de Time-out bij SSH/telnet/HTTP-verbinding in met behulp van MPF-configuratievoorbeeld voor dezelfde configuratie op Cisco ASA met versies 8.2 en eerder.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ASA security applicatie, versie 8.3(1) met Adaptieve Security Devices Manager (ASDM) 6.3.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

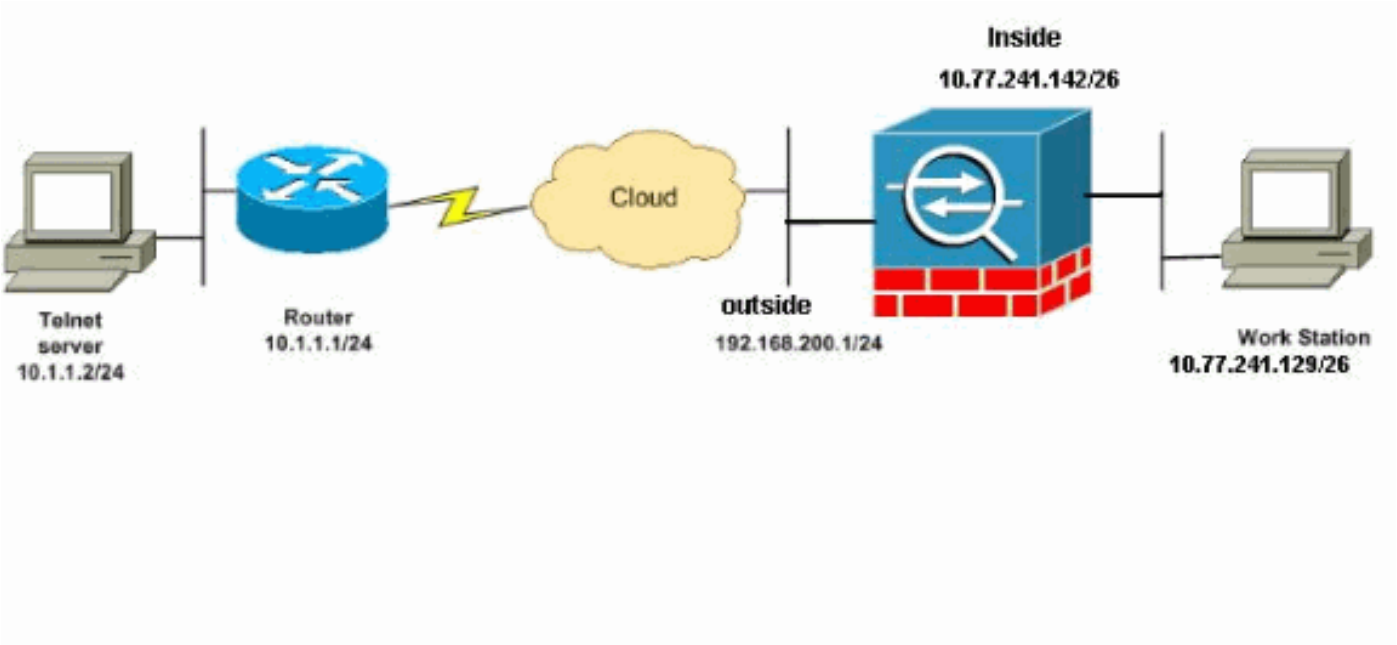
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn RFC 1918-adressen, die in een labomgeving zijn gebruikt.

Configuraties

Dit document gebruikt deze configuraties:

- CLI-configuratie
- ASDM-configuratie

Opmerking: Deze CLI- en ASDM-configuraties zijn van toepassing op de Firewallservicemodule (FWSM).

CLI-configuratie

ASA 8.3(1) configuratie

```
ASA Version 8.3(1)
!
hostname ASA
domain-name nantes-port.fr
enable password S39lgaewi/JM5WyY level 3 encrypted
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 1mZfSd48bl0UdPgP encrypted
no names

dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
ip address 10.77.241.142 255.255.255.0


boot system disk0:/asa831-k8.bin
ftp mode passive
dns domain-lookup outside

!--- Creates an object called DM_INLINE_TCP_1. This
defines the traffic !--- that has to be matched in the
class map. object-group service DM_INLINE_TCP_1 tcp
 port-object eq www
 port-object eq ssh
 port-object eq telnet

access-list outside_mpc extended permit tcp host
10.77.241.129 any object-group DM_INLINE_TCP_1


pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list inside_nat0_outbound
access-group 101 in interface outside

route outside 0.0.0.0 0.0.0.0 192.168.200.2 1
timeout xlate 3:00:00
```

```
!--- The default connection timeout value of one hour is
applicable to !--- all other TCP applications. timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!

!--- Define the class map Cisco-class in order !--- to
classify Telnet/ssh/http traffic when you use Modular
Policy Framework !--- to configure a security feature.
!--- Assign the parameters to be matched by class map.


class-map Cisco-class
 match access-list outside_mpc

class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp

!--- Use the pre-defined class map Cisco-class in the
policy map.


policy-map Cisco-policy

!--- Set the connection timeout under the class mode
where !--- the idle TCP (Telnet/ssh/http) connection is
disconnected. !--- There is a set value of ten minutes
in this example. !--- The minimum possible value is five
minutes. class Cisco-class
  set connection timeout idle 0:10:00 reset
!
!
service-policy global_policy global
```

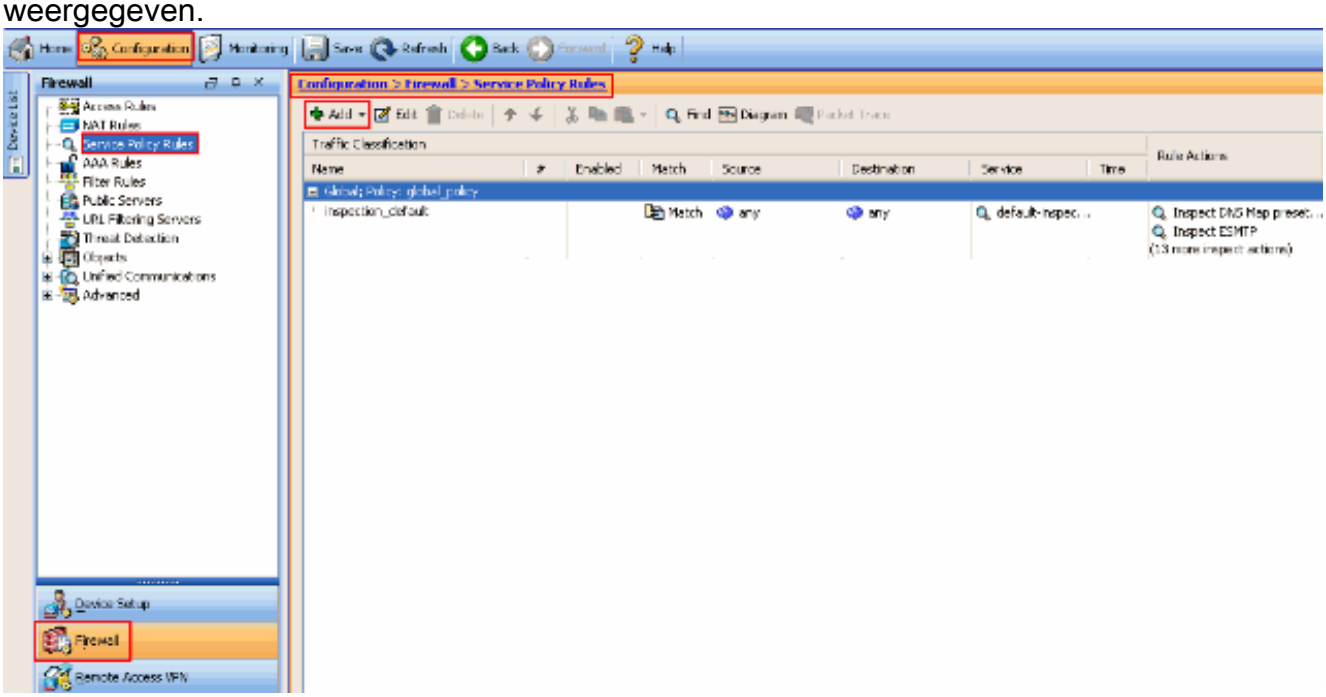
```
!--- Apply the policy-map Cisco-policy on the interface.
!--- You can apply the service-policy command to any
interface that !--- can be defined by the nameif
command.

service-policy Cisco-policy interface outside
end
```

ASDM-configuratie

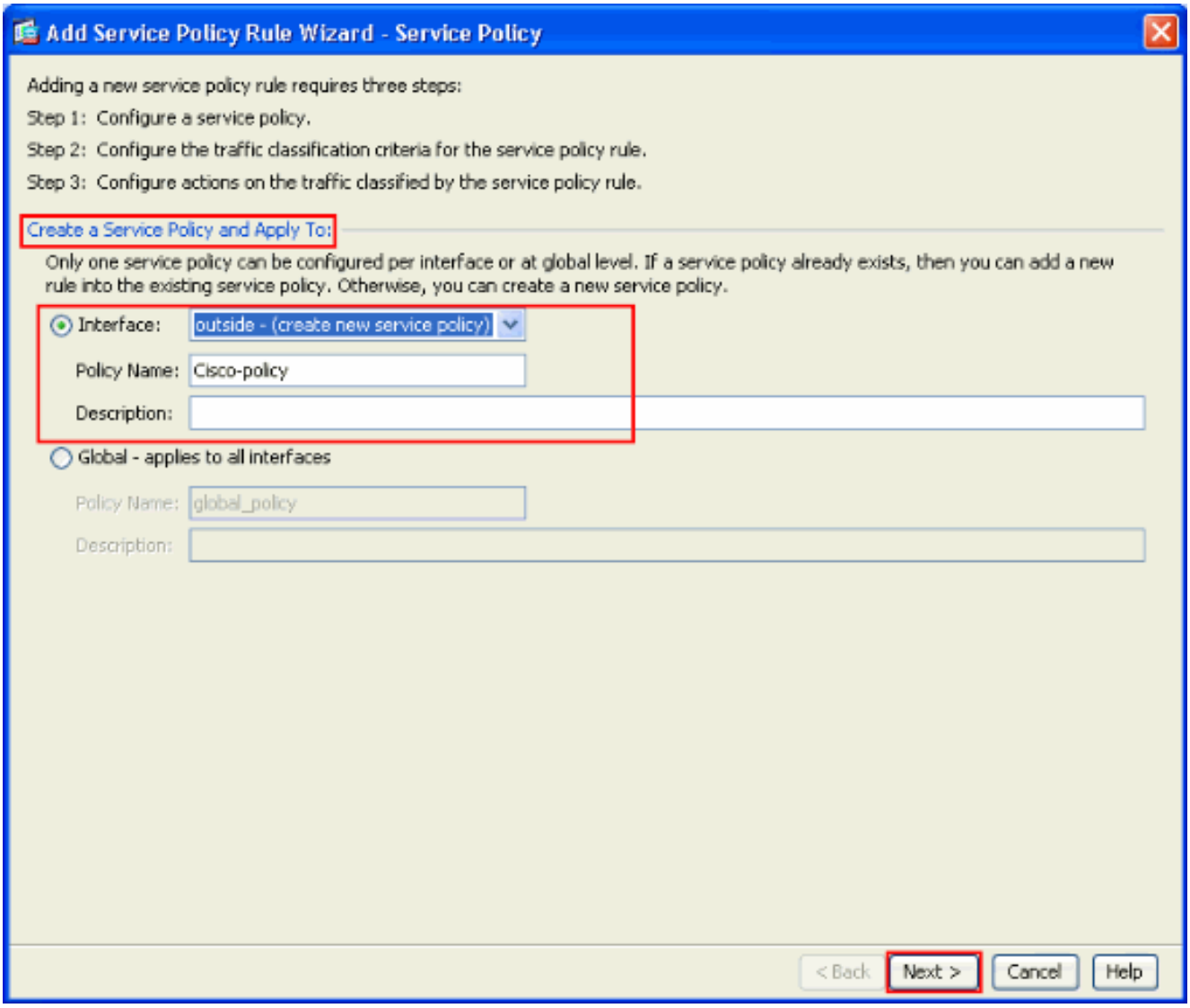
Voltooi deze stappen om de TCP-verbindingsonderbreking voor telnet, SSH en HTTP verkeer in te stellen met behulp van ASDM zoals getoond.

Opmerking: Raadpleeg HTTPS-toegang voor ASDM voor basisinstellingen om toegang te krijgen tot de PIX/ASA via ASDM.

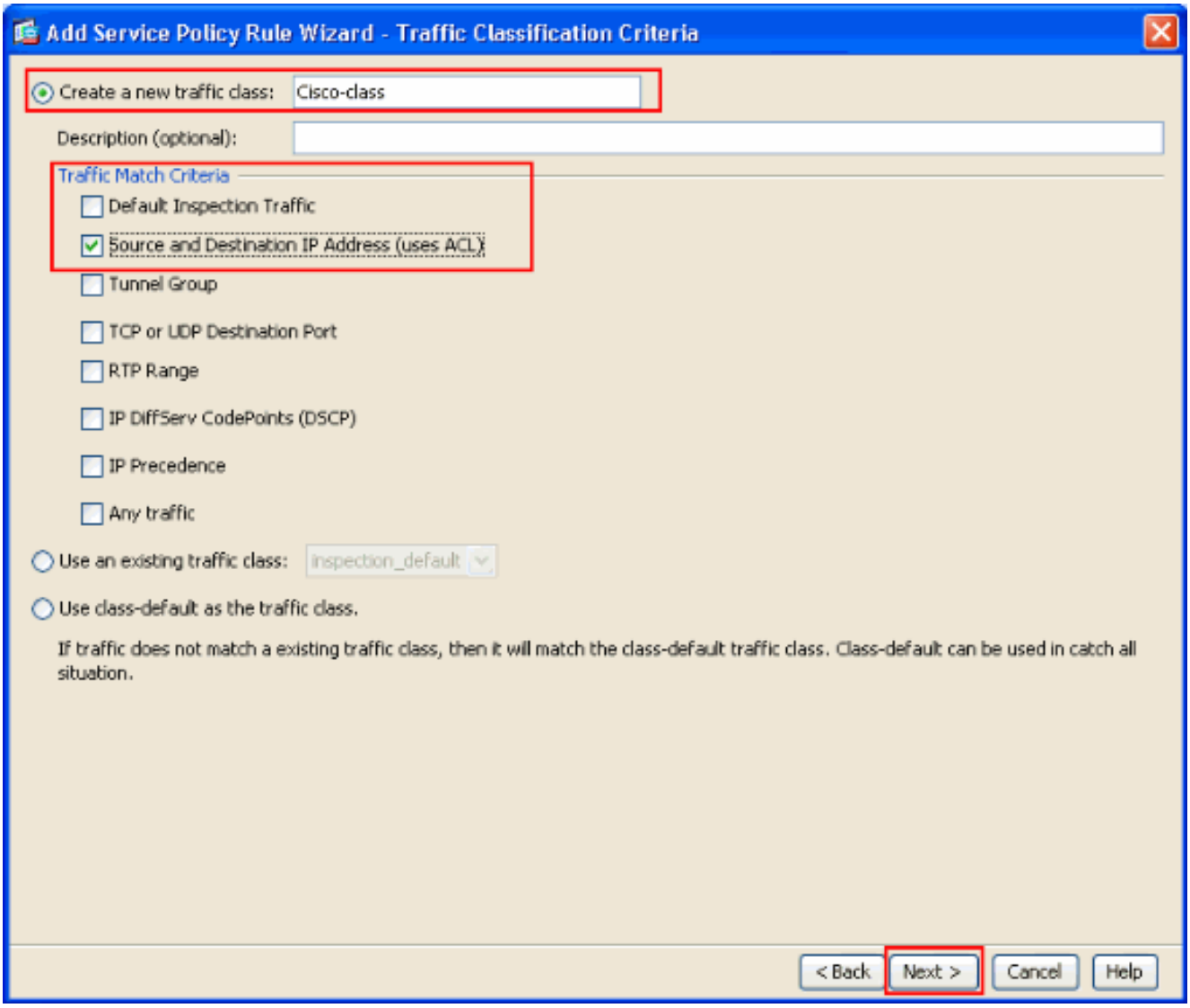
1. Kies **Configuration > Firewall > Service Policy Regels** en klik op **Add** om de regel Service Policy te configureren zoals wordt weergegeven.



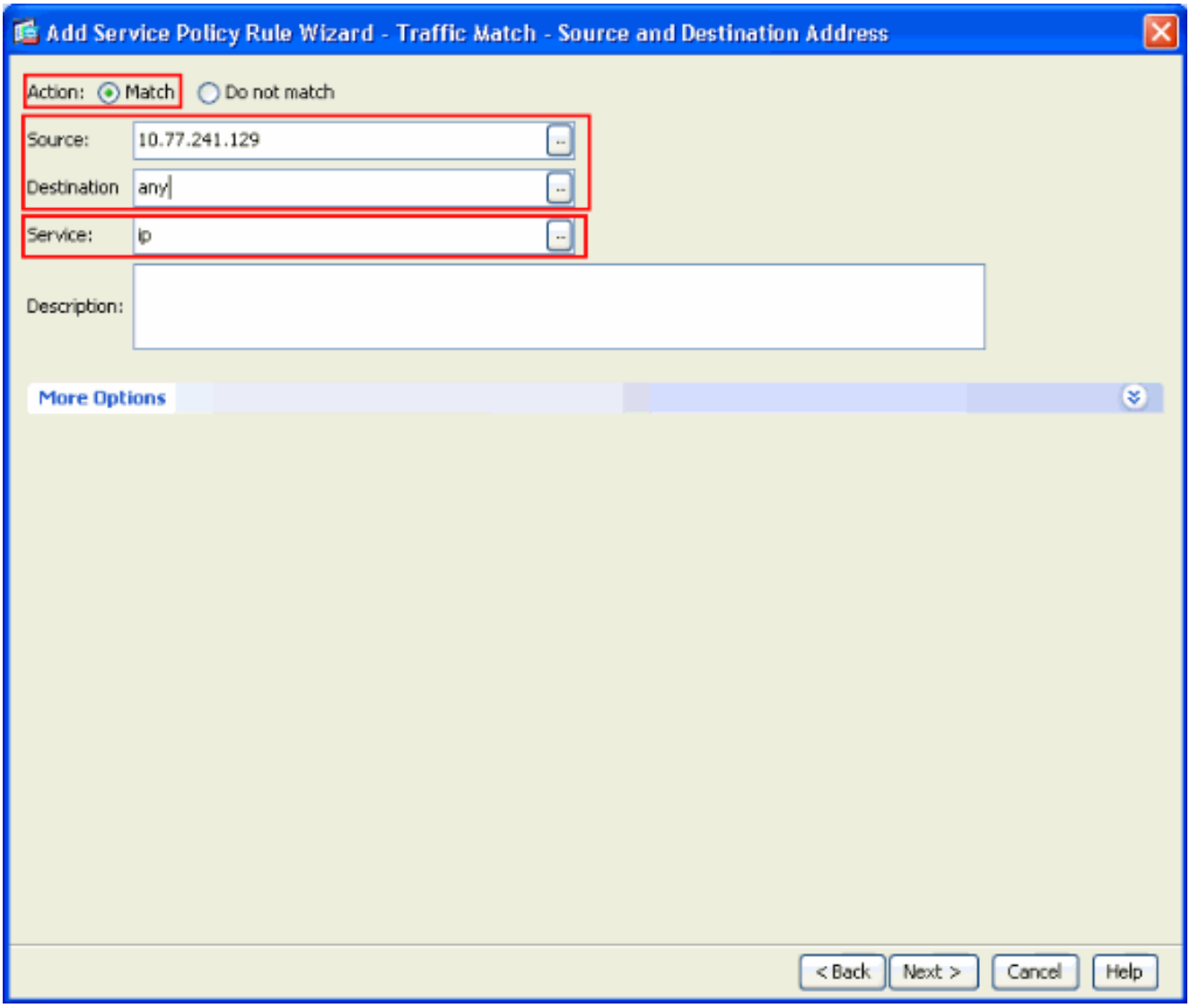
2. Kies in het venster **Add Service Policy Policy Wizard - Service Policy** venster de radioknop naast **interface** onder het **onderdeel Create a Service Policy en is van toepassing op** paragraaf. Kies nu de gewenste interface in de vervolgkeuzelijst en geef een **beleidsnaam op**. De beleidsnaam die in dit voorbeeld wordt gebruikt is **Cisco-beleid**. Klik vervolgens op **Volgende**.



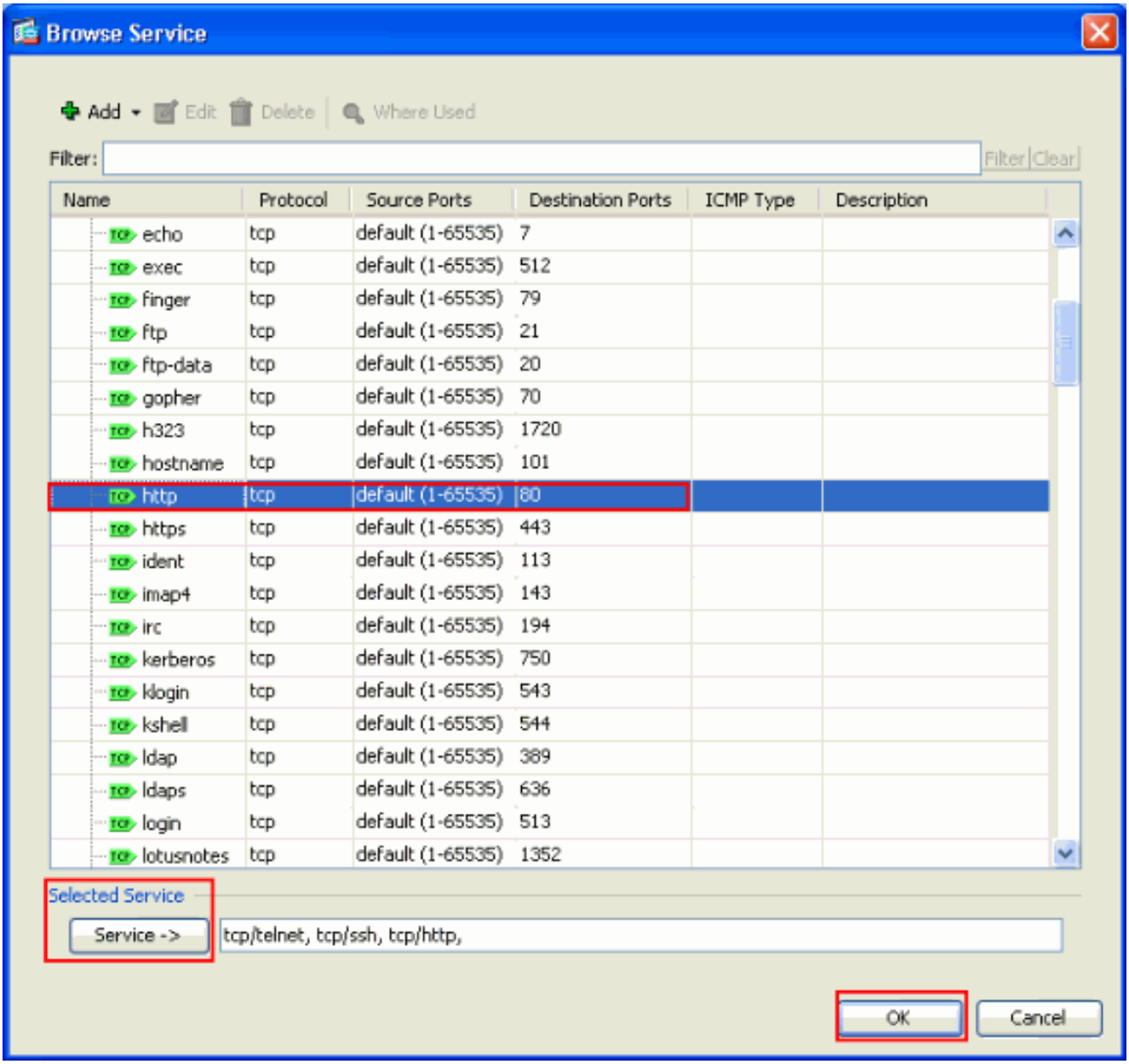
3. Maak een class-kaartnaam **van Cisco-klasse** en controleer het **IP-adres bron en bestemming (gebruikt ACL)** in de Traffic Match Criteria. Klik vervolgens op **Volgende**.



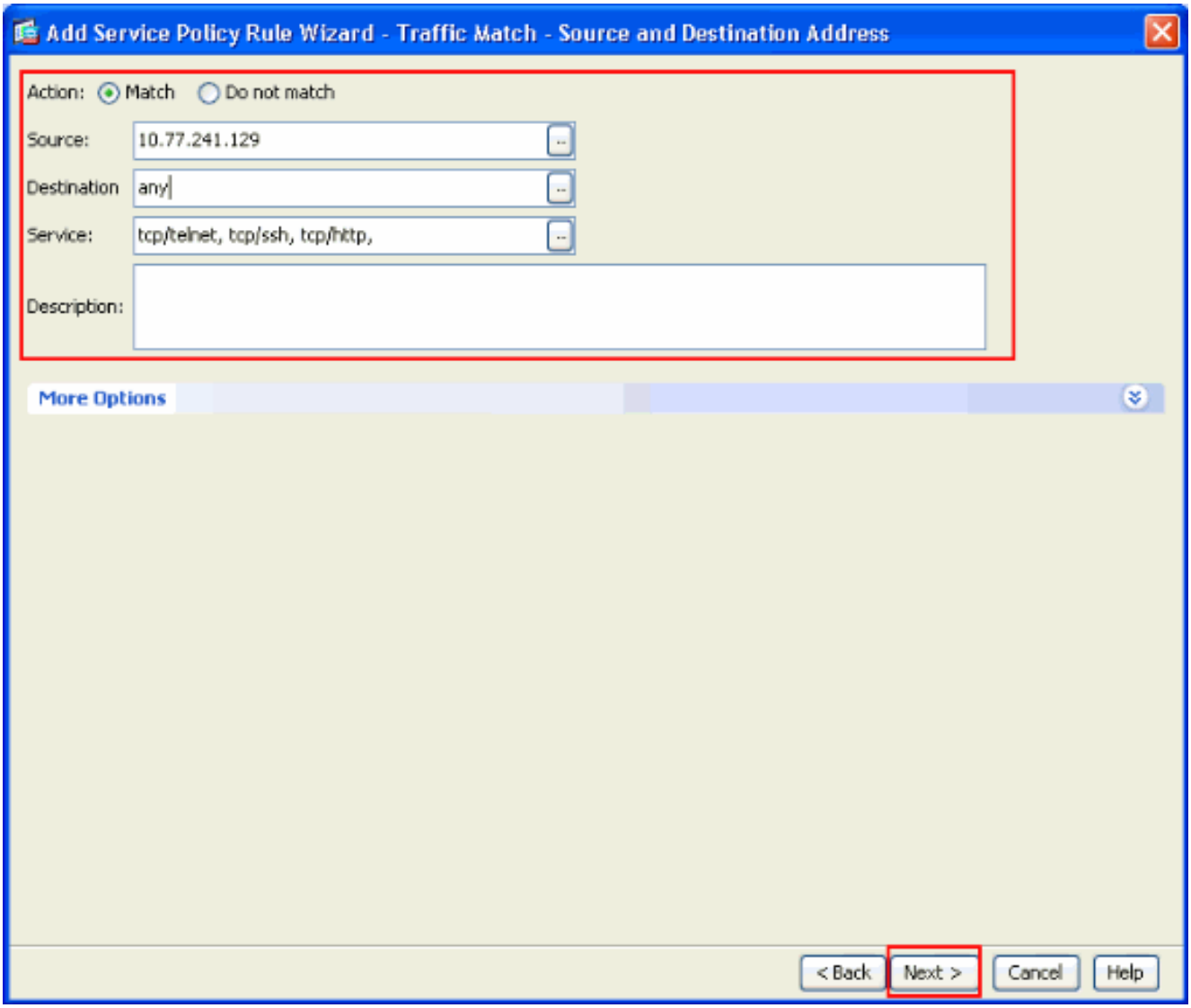
4. Kies in het **venster Add Service Policy Rule Wizard - Traffic Match - Source and Destation Address**, de radioknop naast **Match** en geef vervolgens de bron en het doeladres op zoals aangegeven. Klik op de vervolgkeuzelijst naast **Service** om de gewenste services te kiezen.



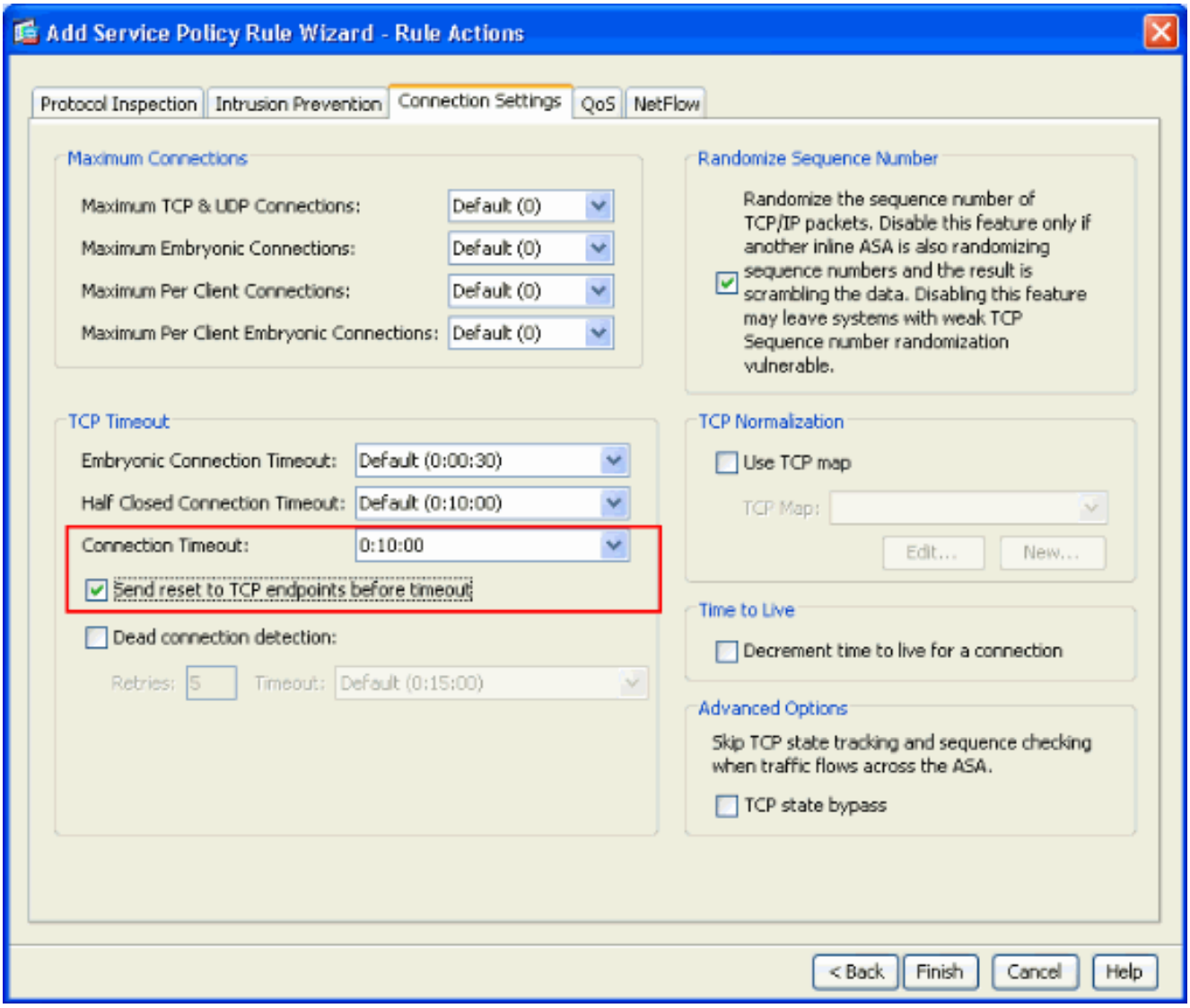
5. Selecteer de gewenste services zoals **telnet**, **ssh** en **http**. Klik vervolgens op **OK**.



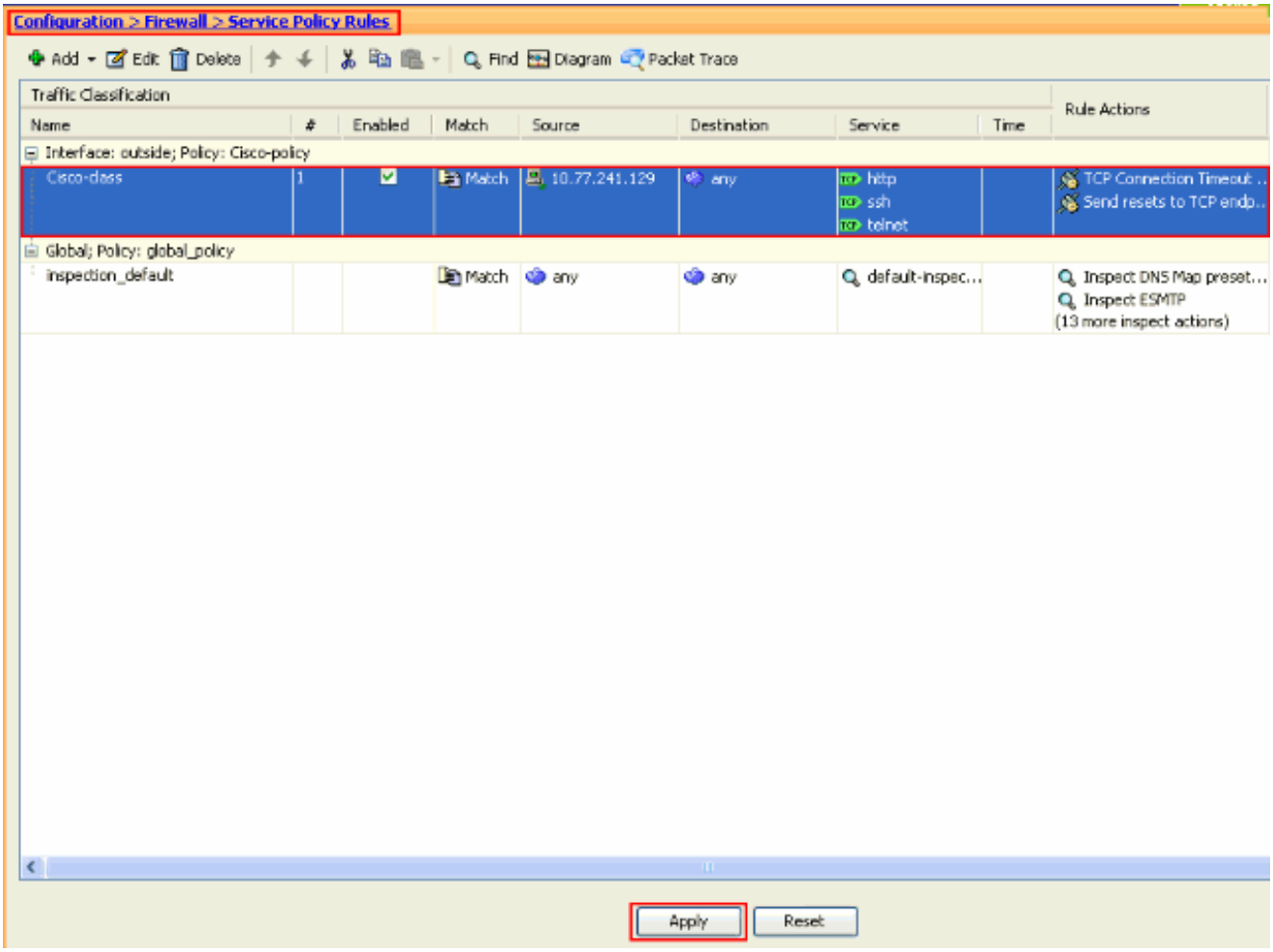
6. **Time-out instellen**. Klik op **Volgende**.



7. Kies **verbindingsinstellingen** om de time-out van de TCP-verbinding in te stellen als 10 minuten. Controleer ook de **Send reset to TCP endpoints voordat timeout** aanvinkt. Klik op **Voltooien**.



8. Klik op **Toepassen** om de configuratie op het security applicatie toe te passen.Dit voltooit de configuratie.



Ethernet-out

Een embryonale verbinding is de verbinding die half open is of, bijvoorbeeld, de drierichtingshanddruk is niet voltooid. Het wordt gedefinieerd als SYN timeout bij de ASA. Standaard is de SYN-tijd op de ASA 30 seconden. Dit is hoe u een embryonale time-out kunt configureren:

```
access-list emb_map extended permit tcp any any

class-map emb_map
match access-list emb_map

policy-map global_policy
class emb_map
set connection timeout embryonic 0:02:00

service-policy global_policy global
```

Problemen oplossen

Als u ontdekt dat de verbindingstijd niet met MPF werkt, controleer dan de TCP initiatie verbinding. De kwestie kan een omkering van het bron- en bestemming IP-adres zijn, of een verkeerd ingesteld IP-adres in de toegangslijst komt niet overeen in MPF om de nieuwe timeout waarde in te stellen of de standaardtijd voor de toepassing te wijzigen. Maak een ingang van de toegangslijst (bron en bestemming) in overeenstemming met de verbindingsinitiatie om de verbindings tijd met MPF in te stellen.

Gerelateerde informatie

- Cisco adaptieve security apparaatbeheer
- Cisco ASA 5500 Series adaptieve security applicaties
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems