

PIX/ASA 7.x en hoger/FWSM: Stel SSH/telnet/HTTP-verbinding in met behulp van MPF-configuratievoorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuratie](#)

[Ethernet-out](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document biedt een voorbeeldconfiguratie voor PIX 7.1(1) en later van een tijdelijke versie die specifiek is voor een bepaalde toepassing zoals SSH/telnet/HTTP, in tegenstelling tot een toepassing die van toepassing is op alle toepassingen. Dit configuratievoorbeeld gebruikt het nieuwe modulaire beleidskader dat in PIX 7.0 is geïntroduceerd. Raadpleeg [Het modulaire beleidskader gebruiken](#) voor meer informatie.

In deze voorbeeldconfiguratie is de PIX Firewall 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 [AASA 8.3 en hoger: Stel de Time-out bij SSH/telnet/HTTP-verbinding in met behulp van MPF-configuratievoorbeeld](#) voor meer informatie over identieke configuratie met behulp van ASDM adaptieve security applicatie (ASA) met versie 8.3 en hoger.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco PIX/ASA security applicatie softwareversie 7.1(1) met Adaptieve Security Devices Manager (ASDM) 5.1.

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.

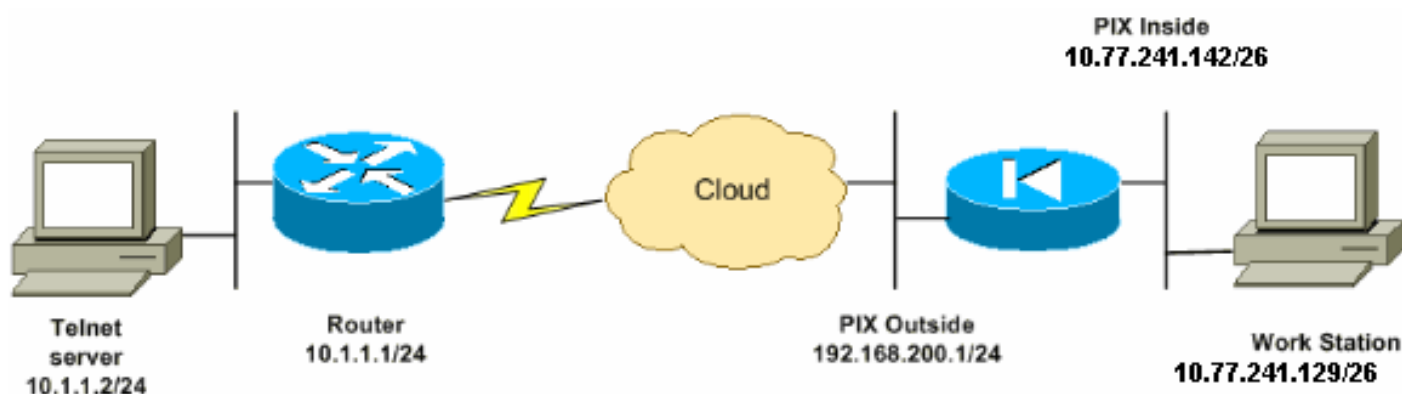
Configureren

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

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

Netwerkdigram

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.

Configuratie

Dit document gebruikt deze configuratie:

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

CLI-configuratie:

PIX-configuratie

```
PIX Version - 7.1(1)
!
hostname PIX
domain-name Cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!

access-list inside_nat0_outbound extended permit ip
10.77.241.128 255.255.255.192 any

!--- Define the traffic that has to be matched in the
class map. !--- Telnet is defined in this example.
access-list outside_mpc_in extended permit tcp host
10.77.241.129 any eq telnet
access-list outside_mpc_in extended permit tcp host
10.77.241.129 any eq ssh
access-list outside_mpc_in extended permit tcp host
10.77.241.129 any eq www
access-list 101 extended permit tcp 10.77.241.128
255.255.255.192 any eq telnet
access-list 101 extended permit tcp 10.77.241.128
255.255.255.192 any eq ssh
access-list 101 extended permit tcp 10.77.241.128
255.255.255.192 any eq www

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
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 telnet 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 telnet
  description telnet
  match access-list outside_mpc_in

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 telnet in the policy
map.

policy-map telnet

!--- Set the connection timeout under the class mode in
which !--- 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 telnet
  set connection timeout tcp 00:10:00 reset
!
!
service-policy global_policy global

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

service-policy telnet interface outside
end

```

ASDM-configuratie:

Voltooi deze stappen om de TCP verbinding-tijd voor Telnet verkeer in te stellen dat op toegang-lijst gebaseerd is die ASDM zoals getoond gebruikt.

Opmerking: Raadpleeg [HTTPS-toegang voor ASDM](#) voor basisinstellingen om toegang te krijgen tot de PIX/ASA via ASDM.

1. **Interfaces configureren**Kies **Configuratie > Interfaces > Add** om de interfaces Ethernet0 (buiten) en Ethernet1 (binnen) te configureren zoals wordt weergegeven.

The screenshot shows the 'Configure Hardware Properties' dialog for the 'Ethernet0' interface. The 'Hardware Port' is set to 'Ethernet0'. The 'Enable Interface' checkbox is checked, and the 'Dedicate this interface to management only' checkbox is unchecked. The 'Interface Name' is 'outside', the 'Security Level' is '0', and the 'IP Address' is '192.168.200.1' with a 'Subnet Mask' of '255.255.255.0'. The 'Use Static IP' radio button is selected. The 'MTU' is set to '1500' and the 'Description' field is empty. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Hardware Port: **Ethernet0** Configure Hardware Properties

Enable Interface Dedicate this interface to management only

Interface Name:

Security Level:

IP Address

Use Static IP Obtain Address via DHCP

IP Address:

Subnet Mask:

MTU:

Description:

OK Cancel Help

Hardware Port: **Ethernet1** Configure Hardware Properties

Enable Interface Dedicate this interface to management only

Interface Name:

Security Level:

IP Address

Use Static IP Obtain Address via DHCP

IP Address:

Subnet Mask:

MTU:

Description:

Klik op
OK.

Configuration > Interfaces

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU
Ethernet0	outside	Yes	0	192.168.200.1	255.255.255.0	No	1500
Ethernet1	inside	Yes	100	10.77.241.142	255.255.255.192	No	1500

Equivalent CLI-configuratie zoals weergegeven:

```
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
```

```
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
```

2. NAT 0 configureren Kies Configuratie > NAT > Regels voor vrijstelling van vertaling > Toevoegen om het verkeer van het netwerk 10.77.241.128/26 toegang te geven tot het internet zonder enige vertaling.

Configuration > NAT > Translation Exemption Rules

Add Address Exemption Rule

Action

Select an action:

Host/Network Exempted From NAT

IP Address Name Group

Interface:

IP address: ...

Mask:

When Connecting To

IP Address Name Group

Interface:

IP address: ...

Mask:

Rule Flow Diagram

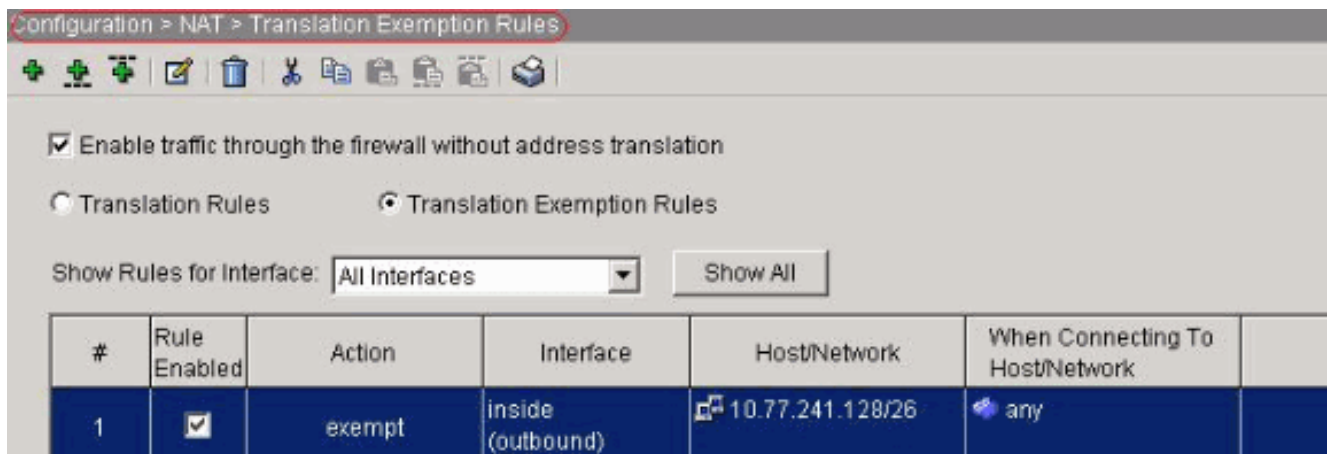
Rule applied to traffic incoming to source interface

The diagram shows a central router icon with two interfaces: 'inside' on the left and 'outside' on the right. A red arrow points to the 'inside' interface. Below the router, a green checkmark is labeled 'exempt'. Dotted orange arrows show traffic flow from 'any' on the left, through the 'inside' interface, through the router, and out through the 'outside' interface to 'any' on the right.

Please enter the description below (optional):

OK Cancel Help

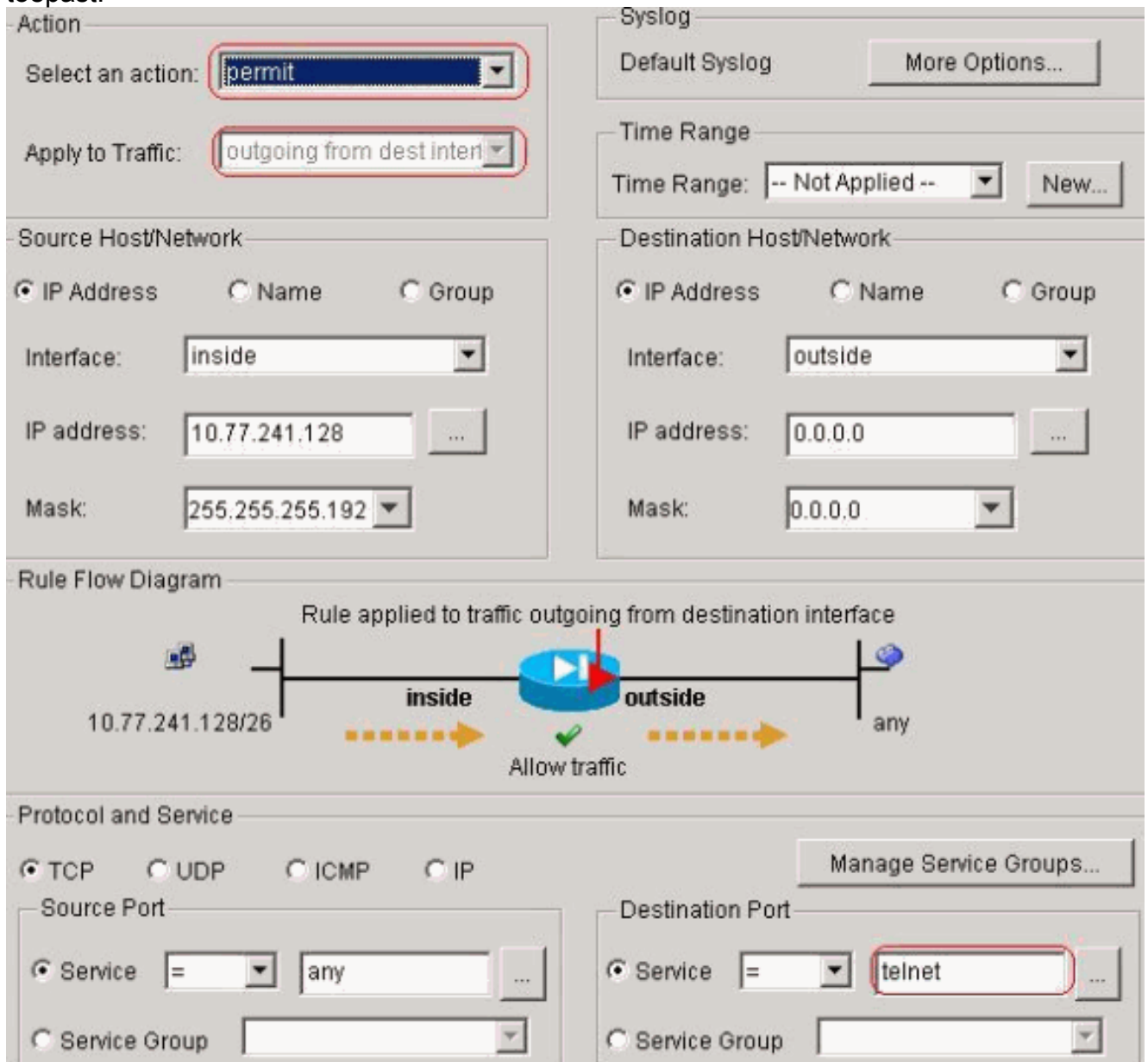
Klik op
OK.



Equivalent CLI-configuration zoals weergegeven:

```
access-list inside_nat0_outbound extended permit ip 10.77.241.128 255.255.255.192 any
nat (inside) 0 access-list inside_nat0_outbound
```

3. **ACL's configureren** Kies **Configuration > Security Policy > Access**, zodat u de ACL's kunt configureren zoals aangegeven in de afbeelding. Klik op **Add** om ACL 101 te vormen die het Telnet verkeer van het netwerk 10.77.241.128/26 aan om het even welk bestemmingsnetwerk toelaat en het voor uitgaande verkeer op de buiteninterface toepast.



Klik op **OK**. Evenzo voor de ssh en http

traffic:

Action

Select an action:

Apply to Traffic:

Source Host/Network

IP Address Name Group

Interface:

IP address: ...

Mask:

Destination Host/Network

IP Address Name Group

Interface:

IP address: ...

Mask:

Syslog

Default Syslog

Time Range

Time Range:

Rule Flow Diagram

Rule applied to traffic outgoing from destination interface

10.77.241.128/26

inside

outside

any

Allow traffic

Protocol and Service

TCP UDP ICMP IP

Source Port

Service = ...

Service Group

Destination Port

Service = ...

Service Group

Action

Select an action:

Apply to Traffic:

Syslog

Default Syslog

Time Range

Time Range:

Source Host/Network

IP Address Name Group

Interface:

IP address:

Mask:

Destination Host/Network

IP Address Name Group

Interface:

IP address:

Mask:

Rule Flow Diagram

Rule applied to traffic outgoing from destination interface

Protocol and Service

TCP UDP ICMP IP

Source Port

Service =

Service Group

Destination Port

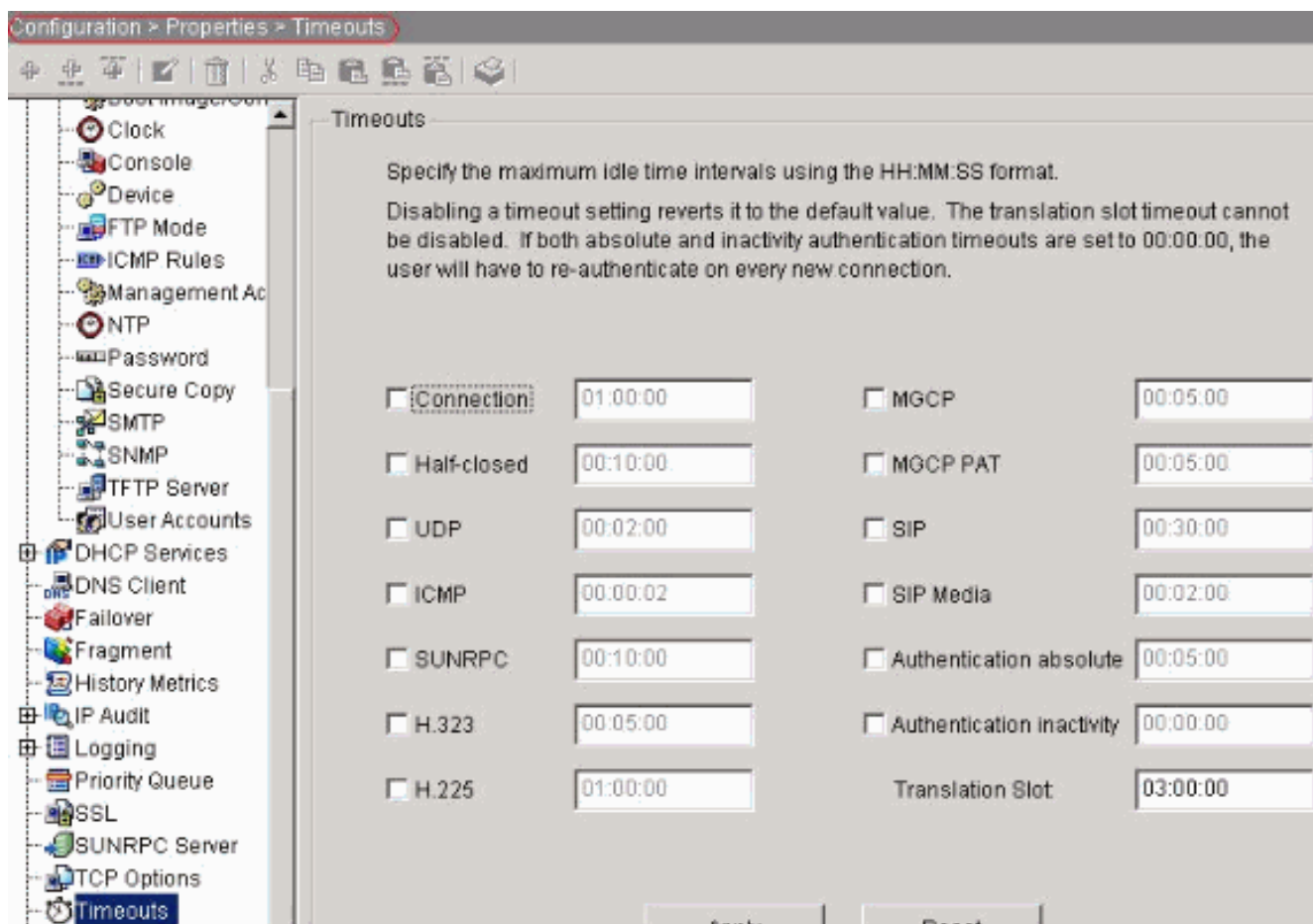
Service =

Service Group

Equivalent CLI-configuratie zoals weergegeven:

```
access-list 101 extended permit tcp 10.77.241.128 255.255.255.192 any eq telnet
access-list 101 extended permit tcp 10.77.241.128 255.255.255.192 any eq ssh
access-list 101 extended permit tcp 10.77.241.128 255.255.255.192 any eq www
access-group 101 out interface outside
```

4. **Time-out configureren**Kies **Configuration > Properties > Time-outs** om de verschillende timeouts te configureren. In dit scenario, houd de standaardwaarde voor alle timeouts.



Equivalent CLI-configuration zoals weergegeven:

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
```

5. **Servicebeleid regels** configureren. Kies **Configuration > Security Policy > Service Policy Rules > Add** om class-kaart te configureren, beleidskaart voor het instellen van de TCP-verbindingstijd in 10 minuten, en pas het servicebeleid toe op de externe interface zoals getoond. Kies de knop **Interface** om **buiten** te kiezen - (**maak een nieuw servicebeleid**), dat moet worden gemaakt, en verdeel **telnet** als de beleidsnaam.

Adding a new service policy rule requires three steps:

Step 1: Configure a service policy.

Step 2: Configure the traffic classification criteria for the service policy rule.

Step 3: Configure actions on the traffic classified by the service policy rule.

Create a service policy and apply to:

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

Interface:

outside - (create new service policy)

Policy Name:

telnet

Description:

Global - applies to all interfaces

Policy Name:

global_policy

Klik op **Volgende**. Maak een class map name **telnet** en kies het **IP-adres bron en bestemming (gebruikt ACL)** in de Verkeerscriteria.

Create a new traffic class:

telnet

Description (optional):

Traffic match criteria

Default Inspection Traffic

Source and Destination IP Address (uses ACL)

Tunnel Group

TCP or UDP Destination Port

RTP Range

IP DiffServ CodePoints (DSCP)

IP Precedence

Any traffic

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.

Use class-default as the traffic class.

Klik op **Volgende**. Maak een ACL om het Telnet verkeer aan te passen dat van het netwerk 10.77.241.128/26 aan om het even welk bestemmingsnetwerk is voortgekomen en pas het

op class telnet toe.
toe.

Action
Select an action: **match**

Time Range
Time Range: -- Not Applied -- New...

Source Host/Network
 IP Address Name Group
Interface: outside
IP address: 10.77.241.128
Mask: 255.255.255.128

Destination Host/Network
 IP Address Name Group
Interface: inside
IP address: 0.0.0.0
Mask: 0.0.0.0

Rule Flow Diagram
Rule applied to traffic incoming to source interface

Protocol and Service
 TCP UDP ICMP IP Manage Service Groups...

Source Port
 Service = any
 Service Group

Destination Port
 Service = **telnet**
 Service Group

Klik op **Volgende**. Evenzo voor de ssh en http traffic:

Action
Select an action:

Time Range
Time Range:

Source Host/Network
 IP Address Name Group
Interface:
IP address:
Mask:

Destination Host/Network
 IP Address Name Group
Interface:
IP address:
Mask:

Rule Flow Diagram
Rule applied to traffic incoming to source interface

```
graph LR; S[10.77.241.128/25] --> O[outside]; O --> R((Router)); R --> I[inside]; I --> D[any];
```

Protocol and Service
 TCP UDP ICMP IP

Source Port
 Service =
 Service Group


Destination Port
 Service =
 Service Group

Action
 Select an action:

Time Range
 Time Range:

Source Host/Network
 IP Address Name Group
 Interface:
 IP address:
 Mask:

Destination Host/Network
 IP Address Name Group
 Interface:
 IP address:
 Mask:

Rule Flow Diagram
 Rule applied to traffic incoming to source interface

 10.77.241.128/25 → outside → match → inside → any

Protocol and Service
 TCP UDP ICMP IP

Source Port
 Service =
 Service Group

Destination Port
 Service =
 Service Group

Kies **verbindinginstellingen** om de Time-out bij TCP-verbinding in te stellen als 10 minuten, en kies ook de optie **Reset naar TCP-eindpunten sturen voor tijdelijke uitvoer**.

Protocol Inspection | Connection Settings | QoS

Maximum Connections

TCP & UDP Connections : Default (0) ▼

Embryonic Connections: Default (0) ▼

Per Client Connections: Default (0) ▼

Per Client Embryonic Connections: Default (0) ▼

Randomize Sequence Number

Randomize the sequence number of TCP/IP packets. Disable this feature only if another inline PIX is also randomizing sequence numbers. The result is scrambling the data. Disabling this feature may leave systems with weak TCP Sequence number randomization vulnerable.

TCP Timeout

Connection Timeout : 00:10:00 ▼

Send reset to TCP endpoints before timeout

Embryonic Connection Timeout : Default (0:00:30) ▼

Half Closed Connection Timeout : Default (0:10:00) ▼

TCP Normalization

Use TCP Map

TCP Map: []

New Edit

Klik op
Voltoeien.

Configuration > Security Policy > Service Policy Rules

Access Rules | AAA Rules | Filter Rules | **Service Policy Rules**

Show Rules for Interface: All Interfaces ▼ Show All

#	Traffic Classification							
	Name	Enabled	Match	Source	Destination	Service	Time Range	
Global, Policy: global_policy								
	inspection_d...			any	any	default-inspection		inspect (1
Interface: outside, Policy: telnet								
1	telnet	<input checked="" type="checkbox"/>		10.77.241...	any	telnet/tcp	-- Not Appl...	connectio send resu

Equivalent CLI-configuratie zoals weergegeven:

```
access-list outside_mpc_in extended permit tcp host 10.77.241.129 any eq telnet
access-list outside_mpc_in extended permit tcp host 10.77.241.129 any eq ssh
access-list outside_mpc_in extended permit tcp host 10.77.241.129 any eq www
```

```
class-map telnet
description telnet
match access-list outside_mpc_in
```

```
policy-map telnet
class telnet
set connection timeout tcp 00:10:00 reset
service-policy telnet interface outside
```


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; de SYN-onderbreking op de ASA is standaard 30 seconden. Dit is de manier om embryonale time-out te 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
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het [Uitvoer Tolk](#) ([uitsluitend geregistreeerde](#) klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van de opdrachtoutput van de **show** te bekijken.

Geef de **showservice-beleidsinterface buiten** commando uit om uw configuraties te controleren.

```
PIX#show service-policy interface outside

Interface outside:
Service-policy: http
Class-map: http
Set connection policy:
Set connection timeout policy:
tcp 0:05:00 reset
Inspect: http, packet 80, drop 0, reset-drop 0
```

Geef de [show service-policy flow](#) opdracht uit om te controleren of het specifieke verkeer overeenkomt met de verschillende beleidsconfiguraties van de dienst.

Deze opdrachtoutput toont een voorbeeld:

```
PIX#show service-policy flow tcp host 10.77.241.129 host 10.1.1.2 eq 23

Global policy:
Service-policy: global_policy

Interface outside:
Service-policy: telnet
Class-map: telnet
Match: access-list 101
Access rule: permit tcp 10.77.241.128 255.255.255.192 any eq telnet
Action:
Input flow: set connection timeout tcp 0:10:00 reset
```

Problemen oplossen

Als u ontdekt dat de verbindingstijd niet met het Modular Policy Framework (MPF) werkt, controleer dan de TCP initiatieverbinding. Het probleem kan een omkering van het IP-adres van bron en bestemming zijn of een verkeerd ingesteld IP-adres in de toegangslijst komt niet overeen in MPF om de nieuwe tijdelijke 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 verbindingsovername om de verbindingstijd met MPF in te stellen.

Gerelateerde informatie

- [Cisco PIX 500 Series security applicaties](#)
- [Adaptieve security applicaties van Cisco ASA 5500 Series](#)
- [Cisco PIX-firewallsoftware](#)
- [Opdrachtreferenties van Cisco Secure PIX-firewall](#)
- [Security meldingen uit het veld \(inclusief PIX\)](#)
- [Verzoeken om opmerkingen \(RFC's\)](#)