

# PIX/ASA 7.x und höher/FWSM: Festlegen des Timeout für SSH/Telnet/HTTP-Verbindungen mithilfe des MPF-Konfigurationsbeispiels

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfiguration](#)

[Ebryonic-Timeout](#)

[Überprüfen](#)

[Fehlerbehebung](#)

## Einführung

Dieses Dokument enthält eine Beispielkonfiguration für PIX 7.1(1) und höher eines Timeouts, das für eine bestimmte Anwendung wie SSH/Telnet/HTTP spezifisch ist, im Gegensatz zu einer Konfiguration, die für alle Anwendungen gilt. In diesem Konfigurationsbeispiel wird das in PIX 7.0 eingeführte modulare Richtlinien-Framework verwendet. Weitere Informationen finden Sie unter [Verwenden des modularen Richtlinien-Frameworks](#).

In dieser Beispielkonfiguration ist die PIX-Firewall so konfiguriert, dass die Workstation (10.77.241.129) Telnet/SSH/HTTP an den Remote-Server (10.1.1.1) hinter dem Router anschließen kann. Ein separates Zeitlimit für Verbindungen zum Telnet-/SSH-/HTTP-Datenverkehr wird ebenfalls konfiguriert. Alle anderen TCP-Datenverkehr haben weiterhin den normalen Zeitüberschreitungswert für die Verbindung, der **Timeout conn 1:00:00** zugeordnet ist.

Weitere Informationen finden Sie unter [AASA 8.3 und höher: Legen Sie das Timeout für SSH/Telnet/HTTP-Verbindungen mithilfe des MPF-Konfigurationsbeispiels](#) für weitere Informationen zur identischen Konfiguration mithilfe von ASDM mit Cisco Adaptive Security Appliance (ASA) mit Version 8.3 und höher fest.

## Voraussetzungen

### Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

# Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco PIX/ASA Security Appliance Software Version 7.1(1) mit Adaptive Security Device Manager (ASDM) 5.1.

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).

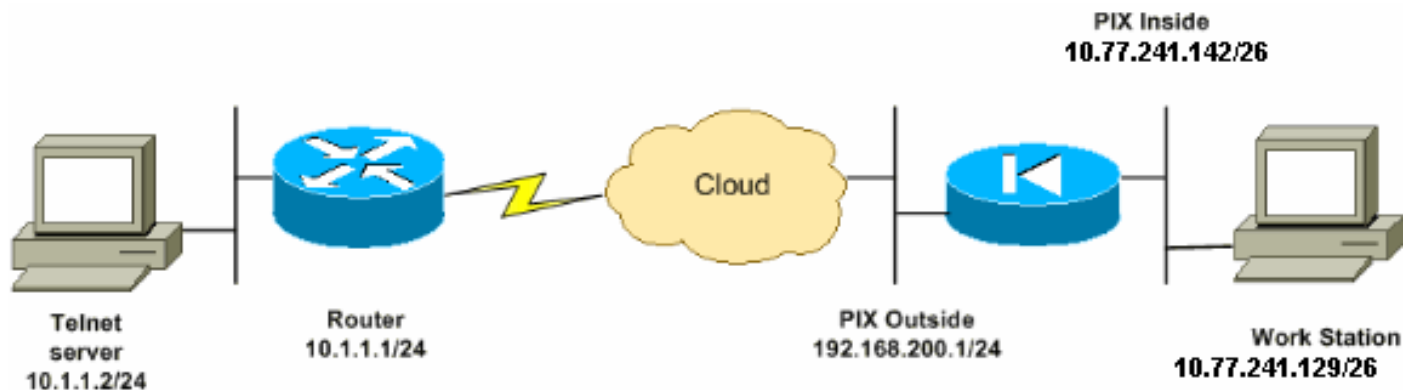
## Konfigurieren

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:



**Hinweis:** Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

## Konfiguration

In diesem Dokument wird diese Konfiguration verwendet:

**Hinweis:** Diese CLI- und ASDM-Konfigurationen gelten für das Firewall Service Module (FWSM).

CLI-Konfiguration:

## PIX-Konfiguration

```
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-Konfiguration:

Führen Sie diese Schritte aus, um ein TCP-Verbindungs-Timeout für Telnet-Datenverkehr

basierend auf einer Zugriffsliste einzurichten, die ASDM wie gezeigt verwendet.

**Hinweis:** Unter [Zulassen von HTTPS-Zugriff für ASDM](#) finden Sie grundlegende Einstellungen, um über ASDM auf PIX/ASA zuzugreifen.

1. **Schnittstellen konfigurieren** Wählen Sie **Configuration > Interfaces > Add**, um die Schnittstellen Ethernet0 (extern) und Ethernet1 (inside) wie dargestellt zu konfigurieren.

Hardware Port: **Ethernet0** Configure Hardware Property

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:

Klicken Sie auf  
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

Entsprechende CLI-Konfiguration wie gezeigt:

```
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. Konfigurieren von NAT 0Wählen Sie **Configuration > NAT > Translation Exemption Rules > Add** (Konfiguration > NAT > Übersetzungsfreistellungsregeln > Hinzufügen, damit der Datenverkehr aus dem Netzwerk 10.77.241.128/26 ohne Übersetzung auf das Internet zugreifen kann.

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

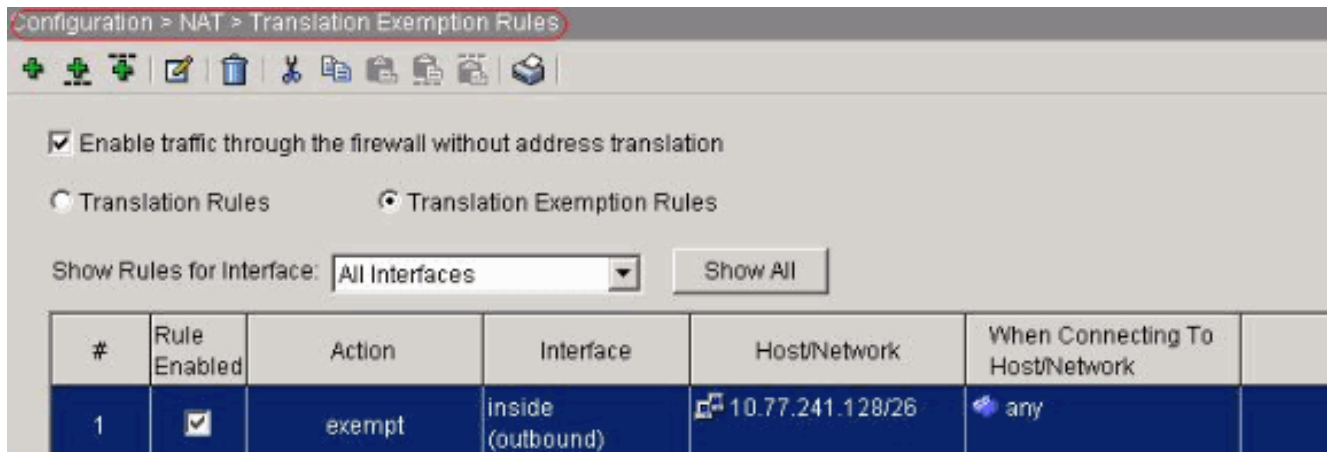
any inside outside any

exempt

Please enter the description below (optional):

OK Cancel Help

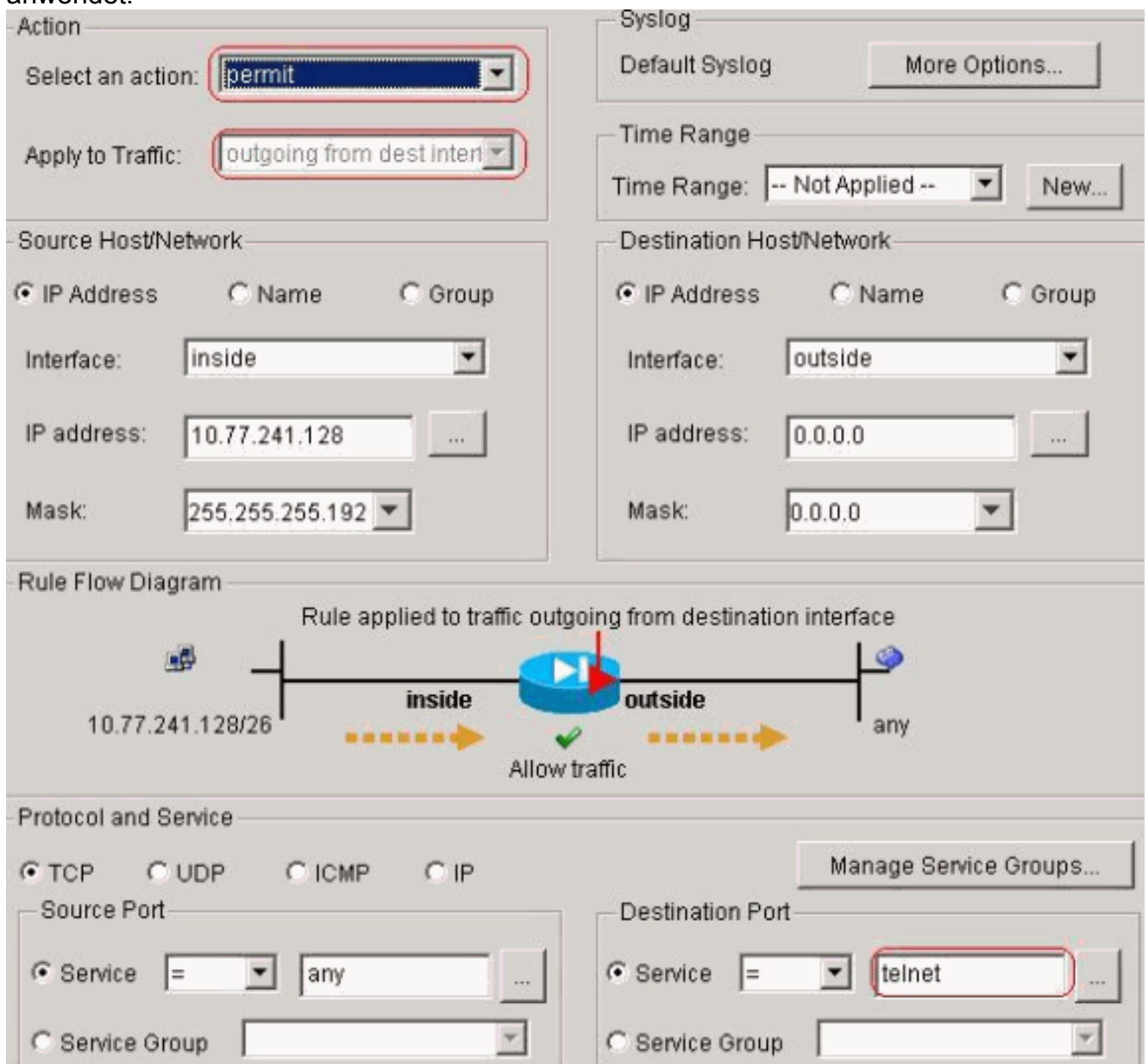
Klicken Sie auf  
OK.



Entsprechende CLI-Konfiguration wie gezeigt:

```
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. Konfigurieren von ACLs Wählen Sie **Configuration > Sicherheitsrichtlinie > Zugriffsregeln**, um die Zugriffskontrolllisten wie gezeigt zu konfigurieren. Klicken Sie auf **Hinzufügen**, um eine ACL 101 zu konfigurieren, die den Telnet-Datenverkehr vom Netzwerk 10.77.241.128/26 an ein beliebiges Zielnetzwerk anbindet und ihn für ausgehenden Datenverkehr an der externen Schnittstelle anwendet.





Klicken Sie auf **OK**. Ähnlich für SSH- und HTTP-Datenverkehr:

**Action**

Select an action: **permit**

Apply to Traffic: **outgoing from dest inter**

**Source Host/Network**

IP Address     Name     Group

Interface: **inside**

IP address: **10.77.241.128** ...

Mask: **255.255.255.192**

**Destination Host/Network**

IP Address     Name     Group

Interface: **outside**

IP address: **0.0.0.0** ...

Mask: **0.0.0.0**

**Syslog**

Default Syslog **More Options...**

**Time Range**

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

**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    **Manage Service Groups...**

**Source Port**

Service = **any** ...

Service Group

**Destination Port**

Service = **ssh** ...

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

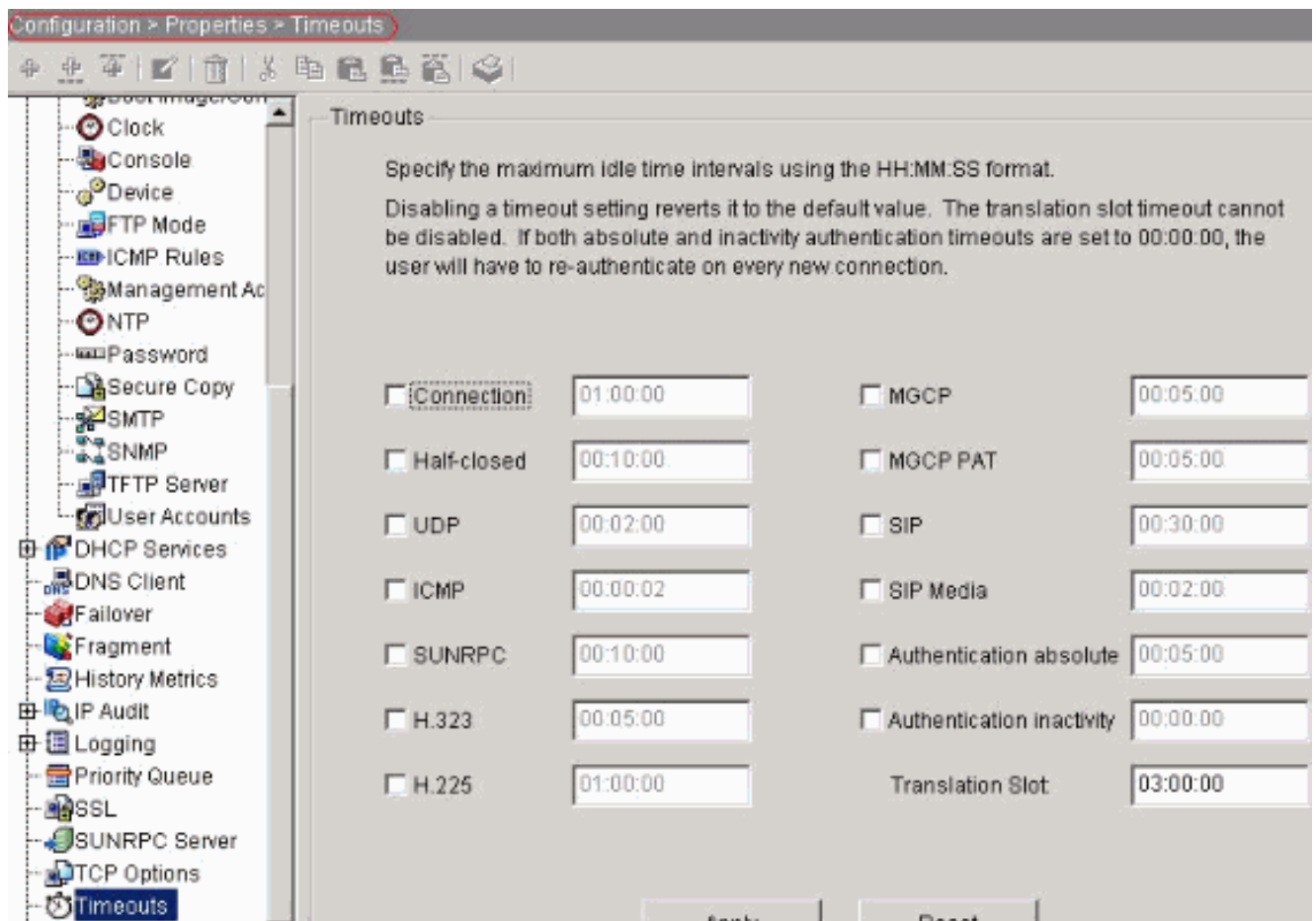
Service =

Service Group

Entsprechende CLI-Konfiguration wie gezeigt:

```
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. Konfigurieren von Timeouts Wählen Sie **Konfiguration > Eigenschaften > Timeouts**, um die verschiedenen Timeouts zu konfigurieren. Behalten Sie in diesem Szenario den Standardwert für alle Timeouts bei.



Entsprechende CLI-Konfiguration wie gezeigt:

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

5. Konfigurieren Sie die **Servicebestimmungen**. Wählen Sie **Configuration > Security Policy > Service Policy Rules > Add (Konfiguration > Sicherheitsrichtlinie > Dienstrichtlinien > Hinzufügen)**, um die Klassenzuordnung und die Richtlinienzuordnung für die Einrichtung des TCP-Verbindungs-Timeouts als 10 Minuten zu konfigurieren, und wenden Sie die Dienstrichtlinie auf die externe Schnittstelle wie gezeigt an. Wählen Sie das Optionsfeld **Interface (Schnittstelle)** aus, um **externe (Erstellen einer neuen Servicerichtlinie)** auszuwählen, die erstellt werden soll, und weisen Sie **telnet** als Richtliniennamen zu.

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

Klicken Sie auf **Weiter**. Erstellen Sie einen Klassenzuordnungsname **telnet**, und aktivieren Sie das **Kontrollkästchen Quell- und Ziel-IP-Adresse (verwendet ACL)** in den Kriterien für die Zuordnung des Datenverkehrs.

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.

Klicken Sie auf **Weiter**. Erstellen Sie eine ACL, um den Telnet-Datenverkehr vom Netzwerk

10.77.241.128/26 an ein beliebiges Zielnetzwerk anzupassen und auf das Telnet der Klasse anzuwenden.

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

Klicken Sie auf **Weiter**. Ähnlich für SSH- und HTTP-Datenverkehr:



**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

**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

Wählen Sie **Verbindungseinstellungen**, um das TCP-Verbindungs-Timeout auf 10 Minuten festzulegen, und aktivieren Sie außerdem das Kontrollkästchen **Rücksetzen an TCP-Endpunkte senden vor dem Timeout**.

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

Klicken Sie auf **Fertig stellen**.

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

Entsprechende CLI-Konfiguration wie gezeigt:

```

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

```



## Ebryonic-Timeout

Eine embryonale Verbindung ist die Verbindung, die halb offen ist oder z.B. der Drei-Wege-Handshake für sie noch nicht abgeschlossen ist. Es wird als SYN-Timeout auf der ASA definiert. Standardmäßig beträgt der SYN-Timeout auf der ASA 30 Sekunden. So konfigurieren Sie die embryonale Zeitüberschreitung:

```
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
```

## 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.

Geben Sie den Befehl **show service-policy interface external** ein, um Ihre Konfigurationen zu überprüfen.

```
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
```

Führen Sie den Befehl [show service-policy flow](#) aus, um zu überprüfen, ob der bestimmte Datenverkehr mit den Servicerichtlinienkonfigurationen übereinstimmt.

Diese Befehlsausgabe zeigt ein Beispiel:

```
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
```

## Fehlerbehebung

Wenn Sie feststellen, dass das Verbindungs-Timeout nicht mit dem Modular Policy Framework (MPF) funktioniert, überprüfen Sie die TCP-Initialisierungsverbindung. Das Problem kann eine Umkehr der Quell- und Ziel-IP-Adresse sein, oder eine falsch konfigurierte IP-Adresse in der Zugriffsliste stimmt nicht mit dem MPF überein, um den neuen Timeout-Wert festzulegen oder das Standard-Timeout für die Anwendung zu ändern. Erstellen Sie einen Zugriffslisteneintrag (Quelle und Ziel) entsprechend der Initiierung der Verbindung, um das Verbindungszeitlimit mit MPF festzulegen.

## Zugehörige Informationen

- [Cisco Security Appliances der Serie PIX 500](#)
- [Cisco Adaptive Security Appliances der Serie ASA 5500](#)
- [Cisco PIX Firewall-Software](#)
- [Cisco Secure PIX Firewall - Befehlsreferenzen](#)
- [Problemhinweise zu Sicherheitsprodukten \(einschließlich PIX\)](#)
- [Anforderungen für Kommentare \(RFCs\)](#)