

PIX/ASA 7.x y posterior/FWSM: Ejemplo de Configuración de Set SSH/Telnet/HTTP Connection Timeout con MPF

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración](#)

[Tiempo de espera electrónico](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento proporciona una configuración de ejemplo para PIX 7.1(1) y posteriores de un tiempo de espera que es específico para una aplicación particular como SSH/Telnet/HTTP, en lugar de uno que se aplica a todas las aplicaciones. Este ejemplo de configuración utiliza el nuevo Marco de política modular introducido en PIX 7.0. Refiérase a [Uso de la Estructura de Políticas Modular](#) para obtener más información.

En esta configuración de ejemplo, el firewall PIX se configura para permitir que la estación de trabajo (10.77.241.129) a Telnet/SSH/HTTP al servidor remoto (10.1.1.1) detrás del router. También se configura un tiempo de espera de conexión separado para el tráfico de Telnet/SSH/HTTP. El resto del tráfico TCP continúa teniendo el valor de tiempo de espera de conexión normal asociado con la **conexión de tiempo de espera 1:00:00**.

Consulte [AASA 8.3 y posteriores: Configure el Tiempo de Espera de Conexión SSH/Telnet/HTTP usando el Ejemplo de Configuración de MPF](#) para obtener más información sobre la configuración idéntica mediante ASDM con Cisco Adaptive Security Appliance (ASA) con la versión 8.3 y posteriores.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco PIX/ASA Security Appliance Software Version 7.1(1) con Adaptive Security Device Manager (ASDM) 5.1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

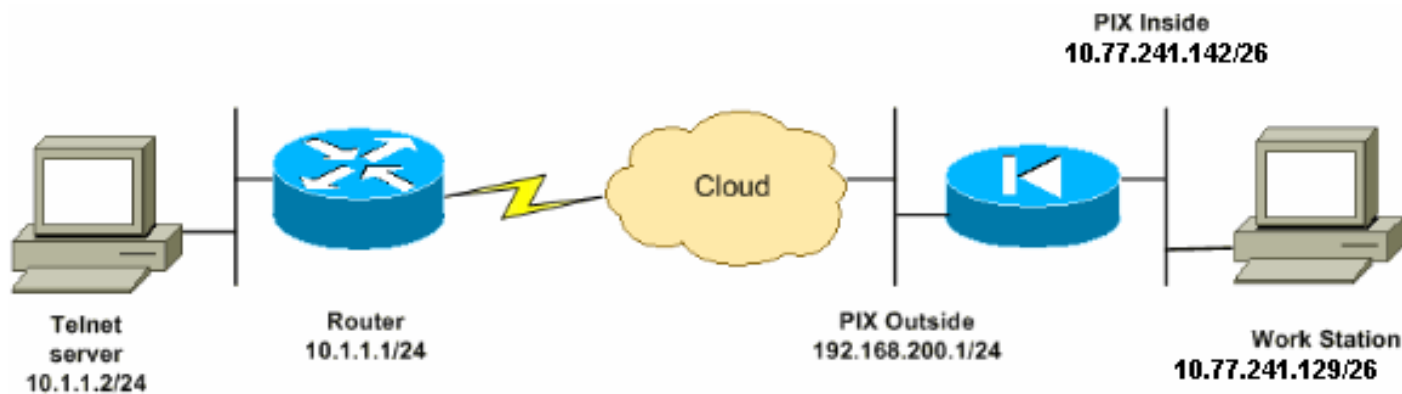
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use el [Command Lookup Tool](#) (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP utilizados en esta configuración no son legalmente enrutables en Internet. Son direcciones RFC 1918, que se han utilizado en un entorno de laboratorio.

Configuración

Este documento usa esta configuración:

Nota: Estas configuraciones CLI y ASDM se aplican al módulo de servicio de firewall (FWSM)

Configuración de CLI:

Configuración de PIX

```
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

```

Configuración de ASDM:

Complete estos pasos para configurar el tiempo de espera de conexión TCP para el tráfico Telnet

basado en la lista de acceso que utiliza ASDM como se muestra.

Nota: Refiérase a [Permiso de Acceso HTTPS para ASDM](#) para la configuración básica para acceder al PIX/ASA a través de ASDM.

1. **Configurar interfaces** Elija **Configuration > Interfaces > Add** para configurar las interfaces Ethernet0 (outside) y Ethernet1 (inside) como se muestra.

The screenshot shows the 'Configure Hardware Properties' dialog box in ASDM. The 'Hardware Port' is set to 'Ethernet0'. The 'Enable Interface' checkbox is checked. The 'Interface Name' is 'outside'. The 'Security Level' is '0'. The 'IP Address' is '192.168.200.1' and the 'Subnet Mask' is '255.255.255.0'. The 'MTU' is '1500'. The 'Description' field is empty. The 'Use Static IP' radio button is selected. The 'OK', 'Cancel', and 'Help' buttons are at the bottom.

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:

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:

Click
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

Configuración CLI equivalente como se muestra:

```
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. Configuración de NAT 0Elija Configuration > NAT > Translation Exemption Rules > Add para permitir que el tráfico de la red 10.77.241.128/26 acceda a Internet sin ninguna traducción.

Configuration > NAT > Translation Exemption Rules

Add Address Exemption Rule

Action

Select an action: **exempt**

Host/Network Exempted From NAT

IP Address Name Group

Interface: **inside**

IP address: **10.77.241.128**

Mask: **255.255.255.192**

When Connecting To

IP Address Name Group

Interface: **outside**

IP address: **0.0.0.0**

Mask: **0.0.0.0**

Rule Flow Diagram

Rule applied to traffic incoming to source interface

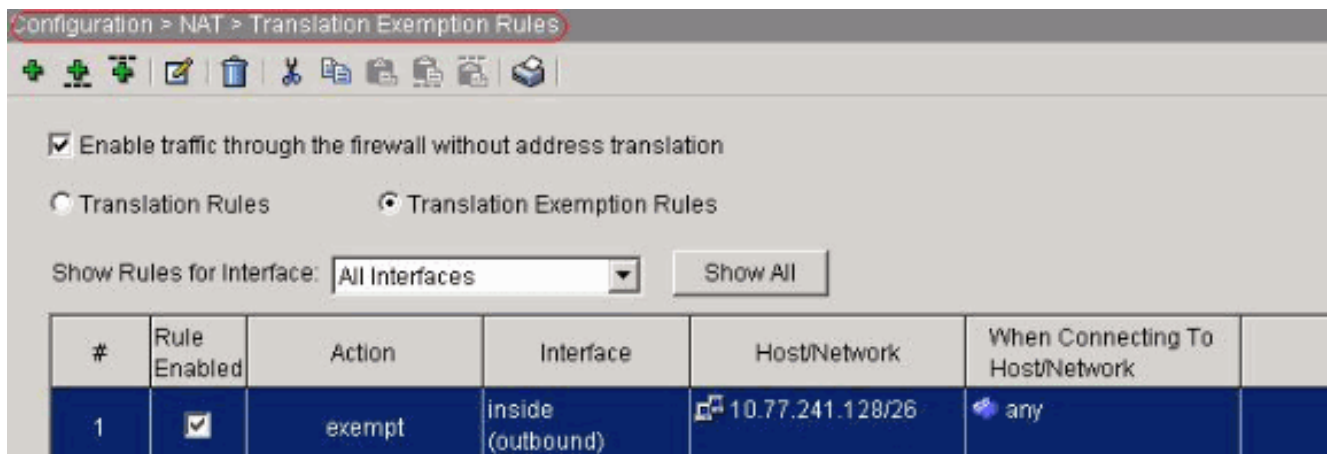
any inside outside any

exempt

Please enter the description below (optional):

OK Cancel Help

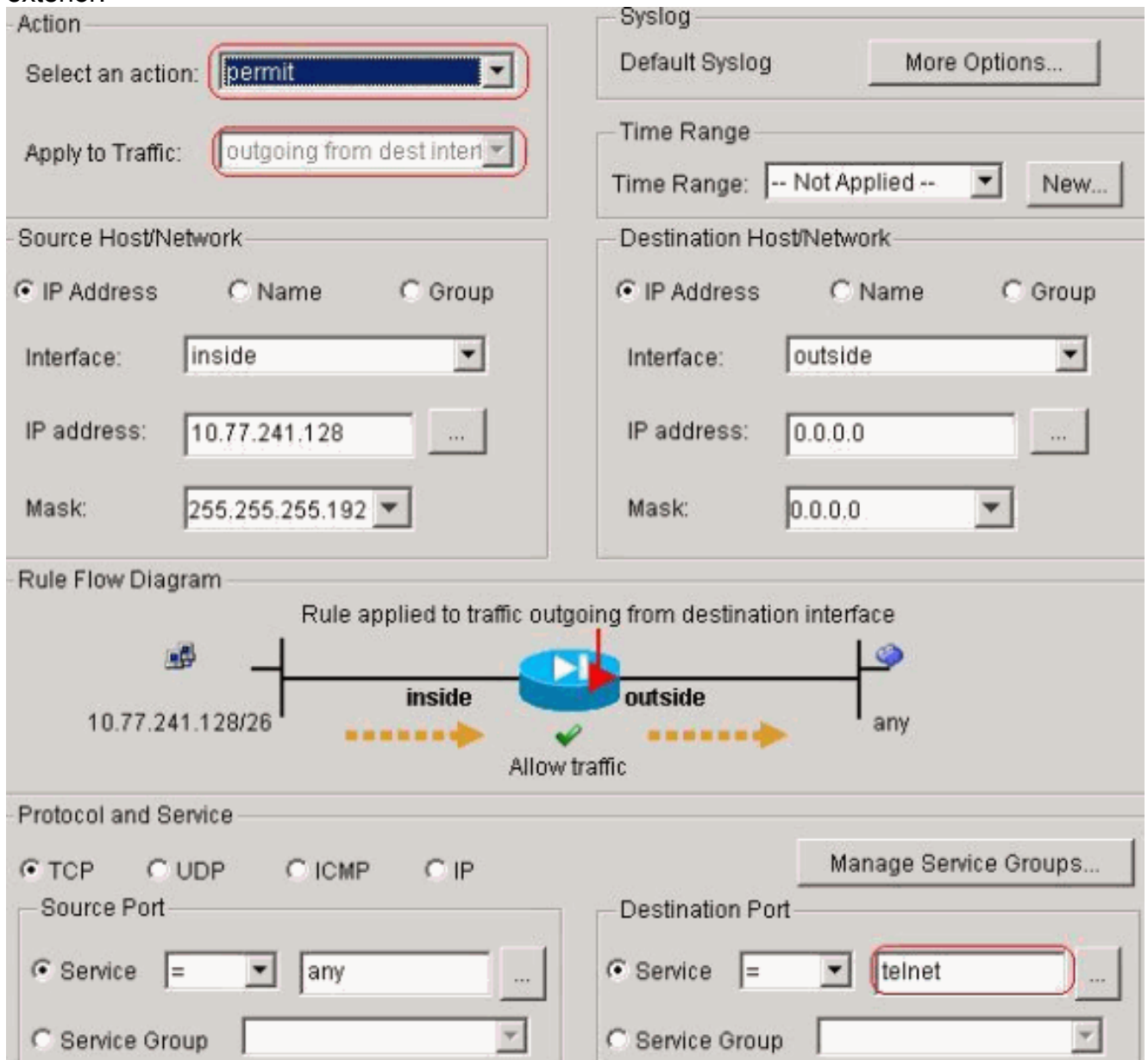
Click
OK.



Configuración CLI equivalente como se muestra:

```
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. Configuración de ACL Elija **Configuration > Security Policy > Access Rules** para configurar las ACL como se muestra. Haga clic en **Agregar** para configurar una ACL 101 que permita el tráfico Telnet originado desde la red 10.77.241.128/26 a cualquier red de destino y aplicarla para el tráfico saliente en la interfaz exterior.



Click OK. De manera similar para el tráfico ssh y

http:

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

```
graph LR; S[10.77.241.128/26] --> I[inside]; I --> R((Router)); R --> O[outside]; O --> D[any];
```

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


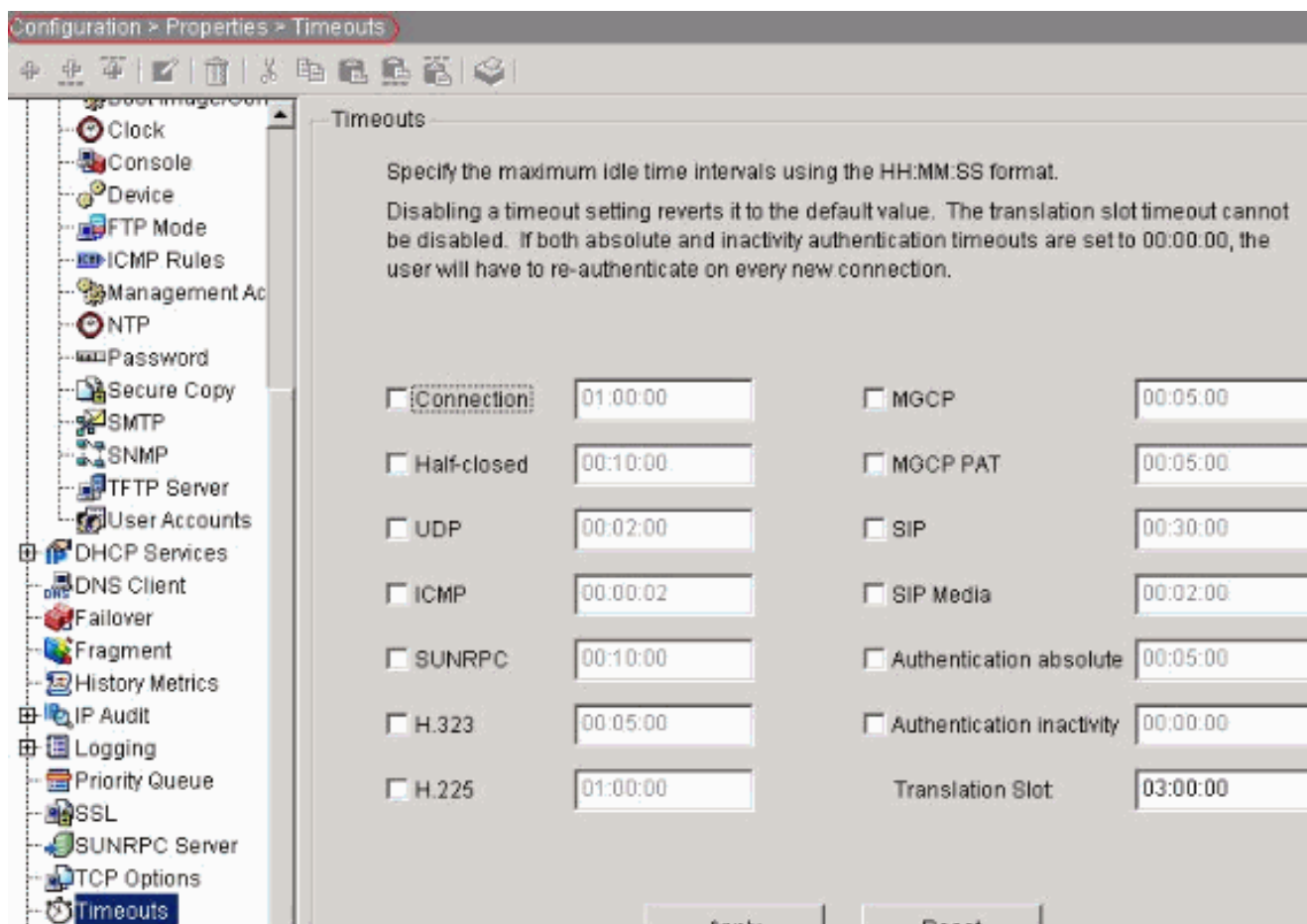
Protocol and Service
 TCP UDP ICMP IP
Source Port
 Service =
 Service Group

Destination Port
 Service =
 Service Group

Configuración CLI equivalente como se muestra:

```
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. **Configurar tiempos de espera** Elija **Configuration > Properties > Timeout** para configurar los diversos tiempos de espera. En este escenario, mantenga el valor predeterminado para todos los tiempos de espera.



Configuración CLI equivalente como se muestra:

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

5. Configurar Reglas de política de servicio. Elija **Configuration > Security Policy > Service Policy Rules > Add** para configurar el mapa de clase, el mapa de políticas para la configuración del tiempo de espera de la conexión TCP como 10 minutos y aplicar la política de servicio en la interfaz externa como se muestra. Elija el botón de radio **Interface** para elegir **outside - (create new service policy)**, que se creará, y asigne **telnet** como nombre de política.

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

Haga clic en Next (Siguiente). Cree un **telnet** con nombre de mapa de clase y elija la **casilla de verificación Dirección IP de origen y destino (utiliza ACL)** en los criterios de coincidencia de tráfico.

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.

Haga clic en Next (Siguiente). Cree una ACL para hacer coincidir el tráfico Telnet originado

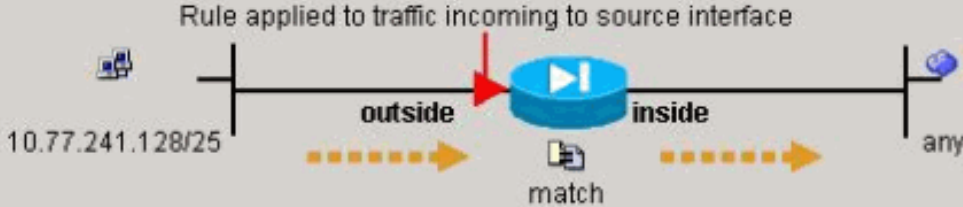
desde la red 10.77.241.128/26 con cualquier red de destino y aplicarla a la clase telnet.

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

Haga clic en Next (Siguiente). De manera similar para el tráfico ssh y http:

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];
```

The diagram shows a central router with two interfaces: 'outside' on the left and 'inside' on the right. A red arrow points to the router from the left, indicating traffic coming from the source network '10.77.241.128/25'. A red arrow also points to the router from the top, with the text 'Rule applied to traffic incoming to source interface'. Below the router, a red arrow points to the 'match' action. Dashed orange arrows show traffic flow from the 'outside' interface through the router to the 'inside' interface, and then to the destination '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

Elija **Connection Settings** para configurar el tiempo de espera de conexión TCP como 10 minutos, y también elija la casilla de verificación **Send reset to TCP endpoints before 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: [Empty field]

New Edit

Haga clic en Finish
(Finalizar).

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

Configuración CLI equivalente como se muestra:

```

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

```


Tiempo de espera electrónico

Una conexión embrionaria es la conexión que está a mitad de camino o, por ejemplo, el intercambio de señales de tres vías no se ha completado para ella. Se define como tiempo de espera SYN en el ASA; de forma predeterminada, el tiempo de espera SYN en el ASA es de 30 segundos. Esta es la forma de configurar el tiempo de espera embrionario:

```
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
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice el OIT para ver una análisis de la salida del comando show.

Ejecute el comando **show service-policy interface outside** para verificar sus configuraciones.

```
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
```

Ejecute el comando [show service-policy flow para verificar que el tráfico particular coincida con las configuraciones de política de servicio.](#)

Este resultado del comando muestra un ejemplo:

```
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
```

Troubleshoot

Si descubre que el tiempo de espera de la conexión no funciona con el marco de políticas modular (MPF), compruebe la conexión de inicio de TCP. El problema puede ser una inversión de la dirección IP de origen y destino o una dirección IP mal configurada en la lista de acceso no coincide en el MPF para establecer el nuevo valor de tiempo de espera o para cambiar el tiempo de espera predeterminado para la aplicación. Cree una entrada de lista de acceso (origen y destino) de acuerdo con el inicio de la conexión para establecer el tiempo de espera de la conexión con MPF.

Información Relacionada

- [Dispositivos de seguridad Cisco PIX de la serie 500](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Cisco PIX Firewall Software](#)
- [Referencias de Comandos de Cisco Secure PIX Firewall](#)
- [Avisos de campos de productos de seguridad \(incluido PIX\)](#)
- [Solicitudes de Comentarios \(RFC\)](#)