

PIX/ASA 7.x y later/FWSM: Fije el tiempo de espera de la conexión SSH/Telnet/HTTP usando el ejemplo de la configuración MPF

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración](#)

[Descanso de Ebrionic](#)

[Verificación](#)

[Troubleshooting](#)

Introducción

Este documento proporciona a una configuración de muestra para PIX 7.1(1) y más adelante de un descanso que sea específico a una aplicación determinada tal como SSH/Telnet/HTTP, en comparación con uno que se aplique a todas las aplicaciones. Este ejemplo de la configuración utiliza el nuevo Marco de políticas modular introducido en PIX 7.0. Refiérase [usando el Marco de políticas modular](#) para más información.

En esta configuración de muestra, el Firewall PIX se configura para permitir el puesto de trabajo (10.77.241.129) a Telnet/SSH/HTTP al servidor remoto (10.1.1.1) detrás del router. Un descanso de otra conexión al tráfico Telnet/SSH/HTTP también se configura. Todo el otro tráfico TCP continúa teniendo el valor de agotamiento del tiempo de la conexión normal asociado a **conec 1:00:00 del descanso**.

Refiera a [AASA 8.3 y más adelante: Fije el tiempo de espera de la conexión SSH/Telnet/HTTP usando el ejemplo de la configuración MPF](#) para más información sobre la configuración idéntica usando ASDM con el dispositivo de seguridad adaptante de Cisco (ASA) con la versión 8.3 y posterior.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en la versión de software del dispositivo de seguridad del PIX/ASA de Cisco 7.1(1) con el Administrador de dispositivos de seguridad adaptante (ASDM) 5.1.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

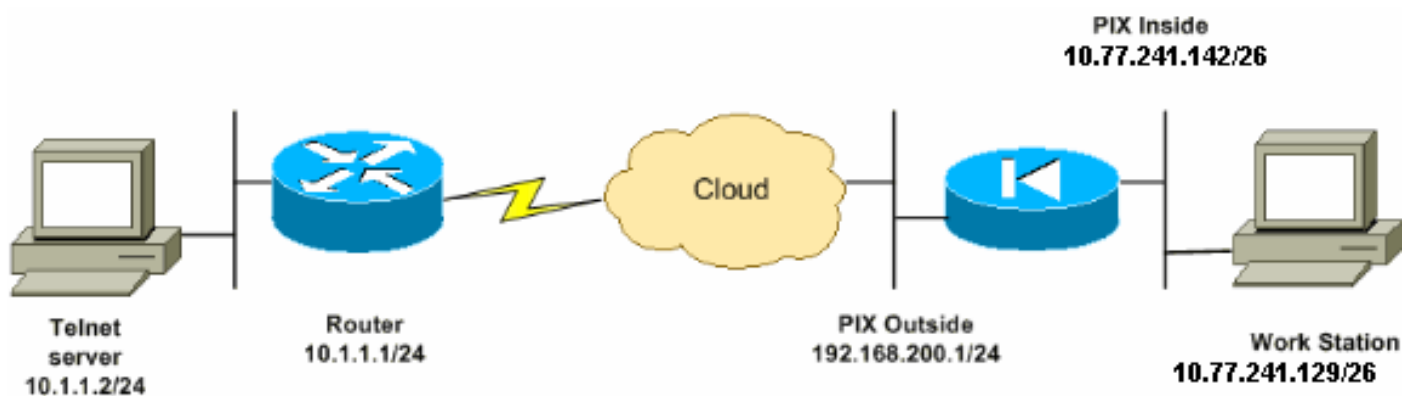
Configurar

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

Nota: Use la [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



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

Configuración

Este documento usa esta configuración:

Nota: Estas configuraciones CLI y ASDM son aplicables al módulo firewall service (el FWSM)

Configuración 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 ASDM:

Complete estos pasos para poner el descanso de conexión TCP para el tráfico de Telnet basado

en la acceso-lista que utiliza ASDM como se muestra.

Nota: Refiera a [permitir que el acceso HTTPS para ASDM](#) para las configuraciones básicas para tener acceso al PIX/ASA con ASDM.

1. **Configure los interfaces** Elija el **Configuration (Configuración) > Interfaces (Interfaces) > agregan** para configurar los interfaces Ethernet0 (afuera) y Ethernet1 (dentro) como se muestra.

The screenshot shows the 'Configure Hardware Property' dialog box 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 '1500' and the 'Description' field is empty. The dialog has 'OK', 'Cancel', and 'Help' buttons at the bottom.

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:

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. **Configure NAT** 0Elija la configuración > el NAT > las reglas de exención de la traducción > agregan para permitir que el tráfico de la red 10.77.241.128/26 tenga acceso a Internet sin ninguna traducción.

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:

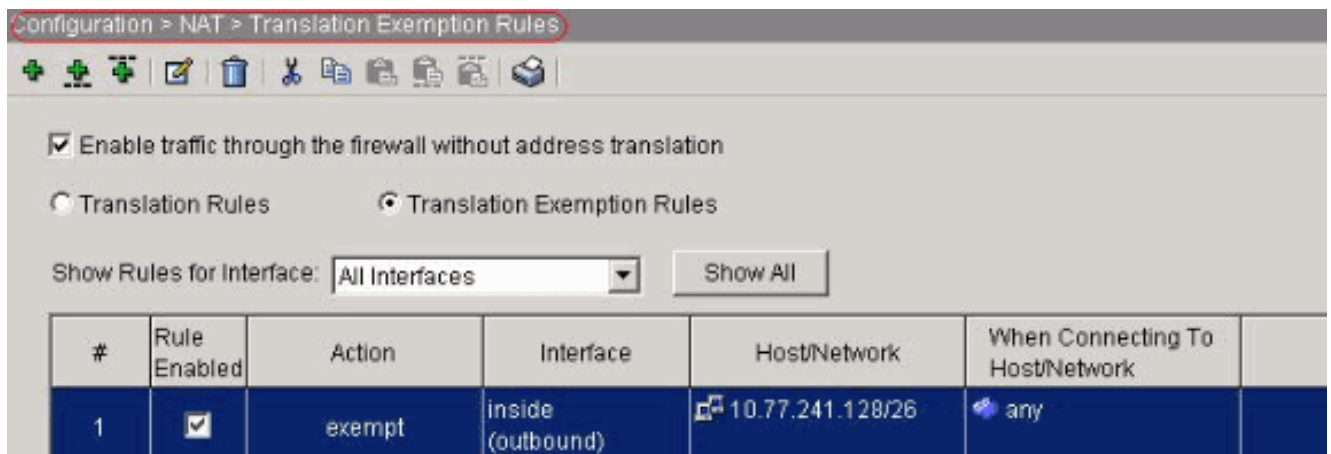
Rule Flow Diagram

Rule applied to traffic incoming to source interface

Please enter the description below (optional):

OK Cancel Help

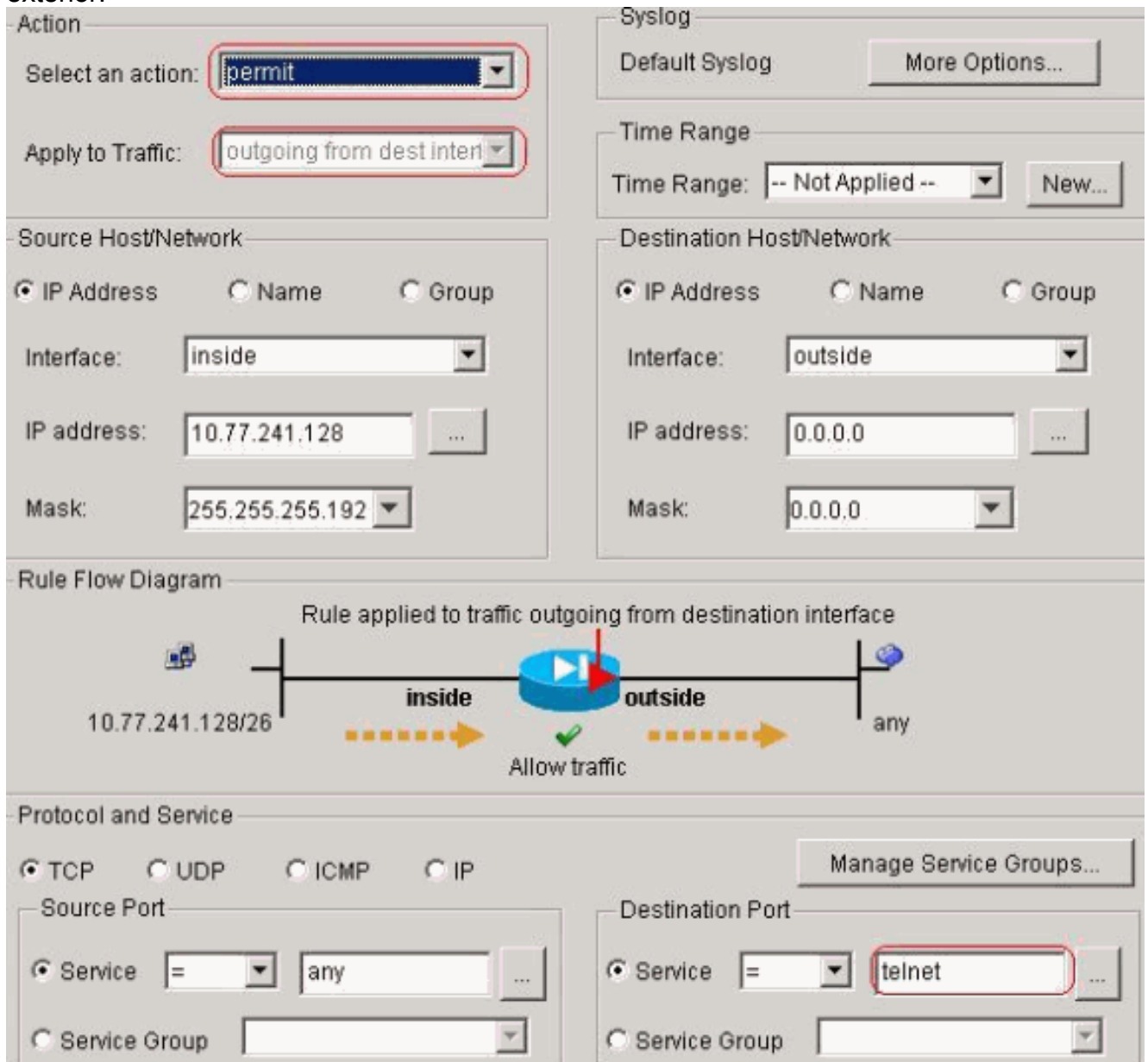
Click
OK.



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. Configure los ACL Elija las reglas de los >Access de la directiva del > Security (Seguridad) de la configuración para configurar los ACL como se muestra. El tecleo agrega para configurar un ACL 101 que permita el tráfico de Telnet originado de la red 10.77.241.128/26 a cualquier red de destino y la solicita el tráfico saliente en la interfaz exterior.



Click OK. Semejantemente para el ssh y el tráfico

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

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

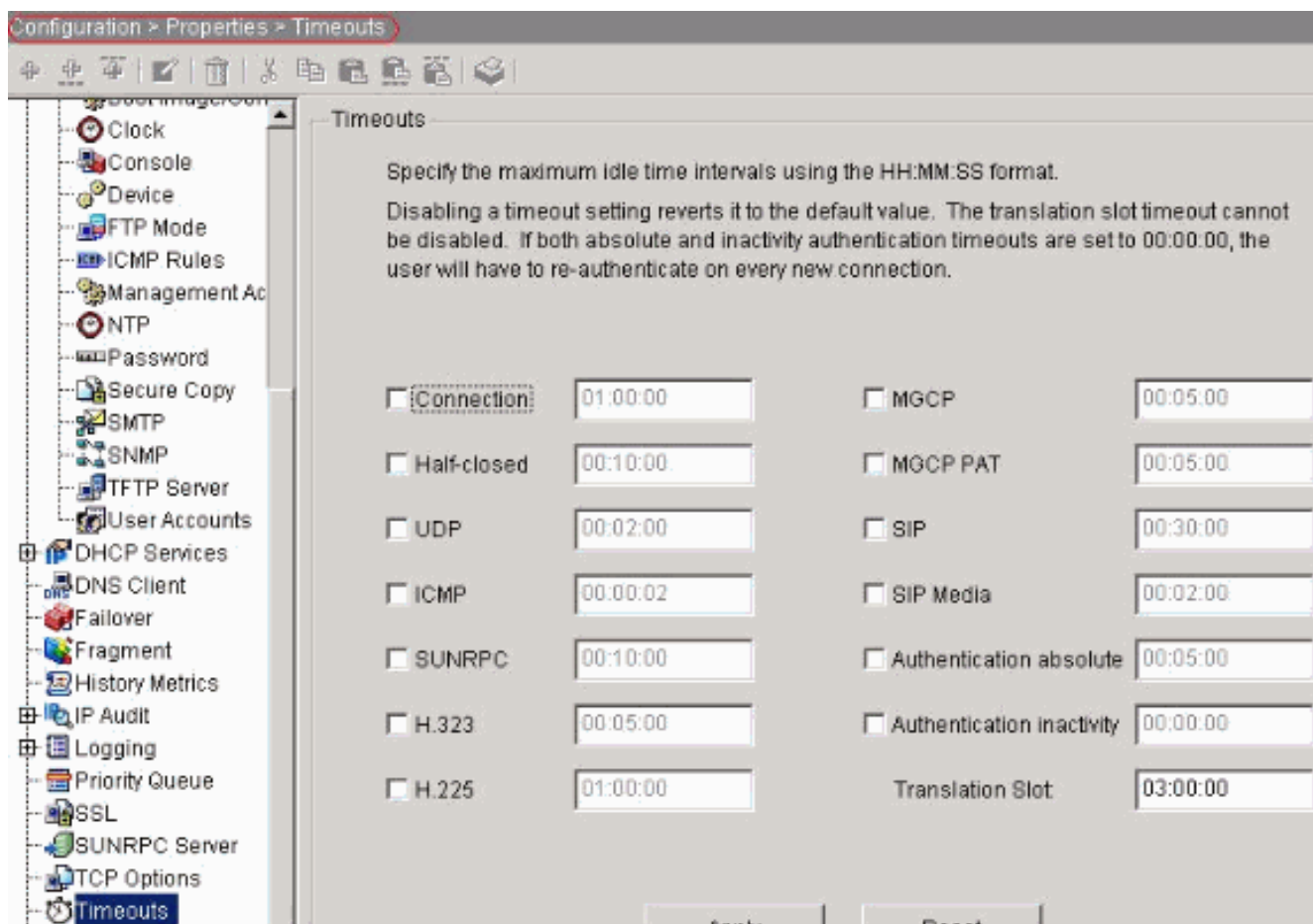
Source Port
 Service =
 Service Group

Destination Port
 Service =
 Service Group

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. **Configure los descansos** Elija la configuración > las propiedades > los descansos para configurar los diversos descansos. En este decorado, guarde el valor predeterminado para todos los descansos.



Configuración CLI equivalente como se muestra:

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

- Configure las reglas de la política de servicio. Elija las reglas de la directiva > de la política de servicio del > Security (Seguridad) de la configuración > agregan para configurar la correspondencia de la clase, correspondencia de la directiva para la creación el descanso de conexión TCP como 10 minutos, y aplican la política de servicio en la interfaz exterior como se muestra. Elija el botón de radio del **interfaz** para elegir el **exterior - (cree la nueva política de servicio)**, que debe ser creada, y asignar el **telnet** como el nombre de la directiva.

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** del nombre de asignación de la clase y elija la casilla de verificación de la **fuentes y de la dirección IP del destino (aplicaciones ACL)** en los criterios de concordancia del 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 un ACL para hacer juego el tráfico de Telnet originado de

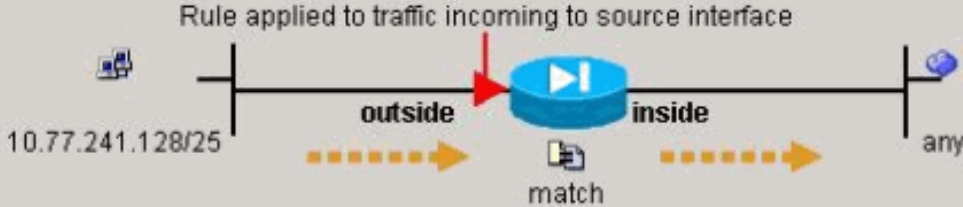
la red 10.77.241.128/26 a cualquier red de destino y aplicarlo para clasificar el telnet.

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). Semejantemente para el ssh y el tráfico 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]; R --- M[match];
```

Protocol and Service
 TCP UDP ICMP IP

Source Port
 Service =
 Service Group

Destination Port
 Service =
 Service Group

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

 10.77.241.128/25 → outside → match → inside → any

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

Source Port
 Service = any
 Service Group

Destination Port
 Service = www
 Service Group

Elija las **configuraciones de la conexión** para poner el descanso de conexión TCP como 10 minutos, y también elija el **envío reajustado a los Puntos finales de TCP** antes de la casilla de verificación del **descanso**.

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

```


Descanso de Ebrionic

Una conexión embrionaria es la conexión que es media se abre o, por ejemplo, la entrada en contacto de tres vías no se ha completado para ella. Se define como tiempo de espera SYN en el ASA; por abandono el tiempo de espera SYN en el ASA es 30 segundos. Ésta es la manera de configurar el descanso 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.

Publique 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
```

Publique el comando del [flujo de la servicio-directiva de la demostración](#) para verificar que el tráfico determinado hace juego las configuraciones de la política de servicio.

Esta salida 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
```

Troubleshooting

Si usted encuentra que el tiempo de espera de la conexión no trabaja con el Marco de políticas modular (MPF), después controle la conexión del lanzamiento TCP. El problema puede ser una revocación de la fuente y la dirección IP del destino o una dirección IP misconfigured en la lista de acceso no hace juego en el MPF para fijar el nuevo valor de agotamiento del tiempo o para cambiar el tiempo de espera predeterminado para la aplicación. Cree una entrada de lista de acceso (fuente y destino) de acuerdo con el lanzamiento de conexión para fijar 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 Secure PIX firewall](#)
- [Avisos de campos de productos de seguridad \(incluido PIX\)](#)
- [Pedidos los comentarios \(RFC\)](#)