

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

ID del Documento: 68332

Actualizado: De oct el 16 de 2008



[Descarga PDF](#)



[Imprimir](#)

[Comentarios](#)

Productos Relacionados

- [Cisco Adaptive Security Device Manager](#)
- [Firewall de la última generación de las 5500-X Series de Cisco ASA](#)
- [Dispositivos de seguridad Cisco PIX de la serie 500](#)

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración](#)

[Descanso de Ebrionic](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Discusiones relacionadas de la comunidad del soporte de Cisco](#)

Introducción

Este documento proporciona una configuración de muestra para PIX 7.1(1) y posterior 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 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 la **conexión de tiempo de espera 1:00:00**.

Refiera a [AASA 8.3 y posterior: 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 el 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.

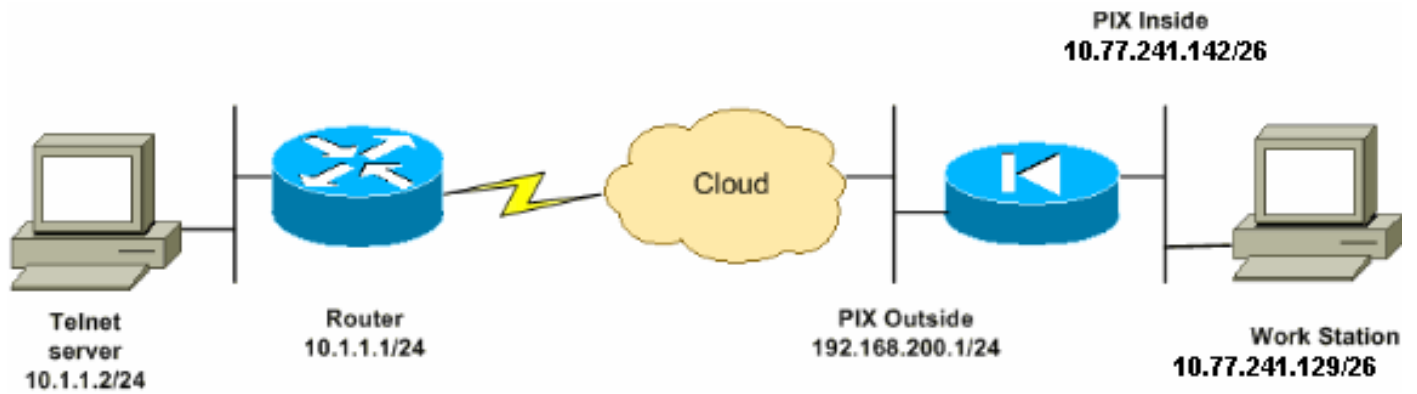
Configurar

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 ambiente de laboratorio.

Configuración

Este documento usa esta configuración:

Nota: Este el CLI y las Configuraciones de 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
esmtip 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 descanso de conexión TCP para el tráfico de Telnet basado en la lista de acceso que utiliza el ASDM como se muestra.

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

1. **Configure las interfaces** Elija el **Configuration (Configuración) > Interfaces (Interfaces) > Add** para configurar el ethernet0 de las interfaces (afuera) y el Ethernet1 (dentro) como se muestra.

Hardware Port:

Ethernet0

Configure Hardware Properti

Enable Interface

Dedicate this interface to management only

Interface Name:

outside

Security Level:

0

IP Address

Use Static IP

Obtain Address via DHCP

IP Address:

192.168.200.1

Subnet Mask:

255.255.255.0

MTU:

1500

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:

Haga clic en
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 NAT 0Elija la configuración > el NAT > las reglas de exención de la traducción > Add para permitir que el tráfico de la red 10.77.241.128/26 acceda 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:

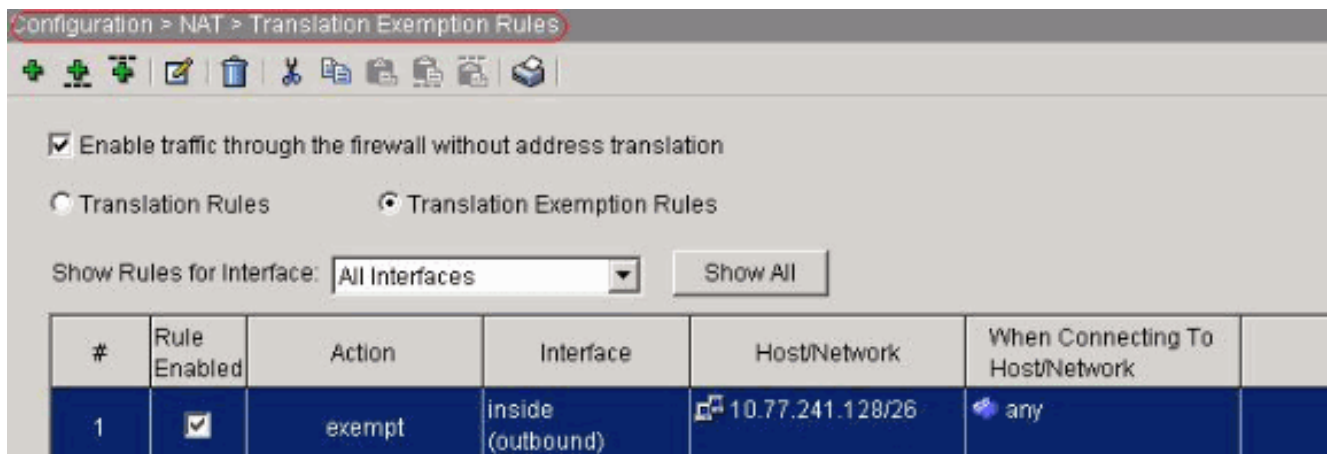
Rule Flow Diagram

Rule applied to traffic incoming to source interface

Please enter the description below (optional):

OK Cancel Help

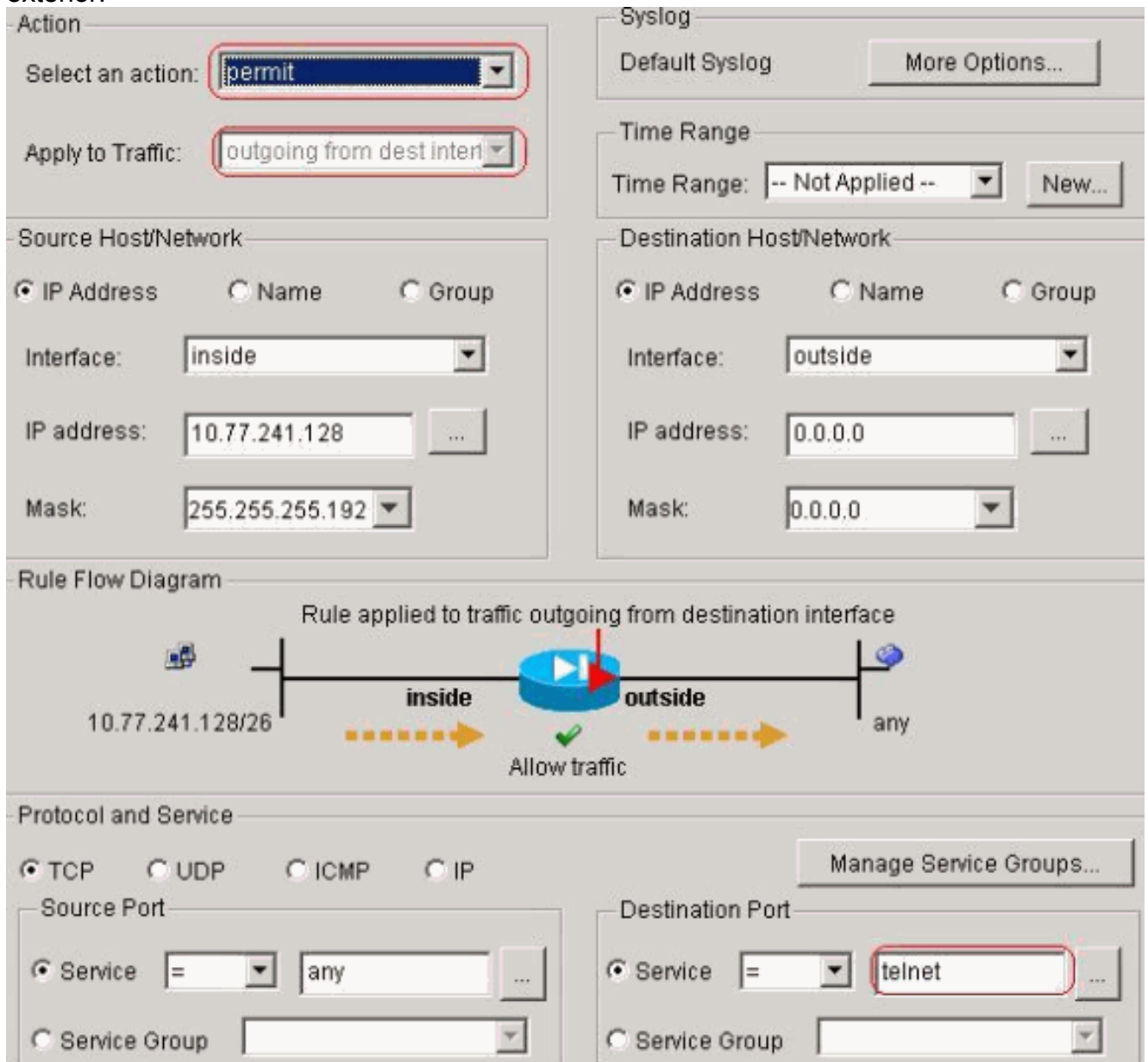
Haga clic en
OK.



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 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 permite 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.



Haga clic en 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

```
graph LR; S[10.77.241.128/26] -- "inside" --> R((Router)); R -- "outside" --> 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

 10.77.241.128/26 — inside —> [Router] — outside —> any
 Allow traffic

Protocol and Service
 TCP UDP ICMP IP

Source Port
 Service =
 Service Group

Destination Port
 Service =
 Service Group

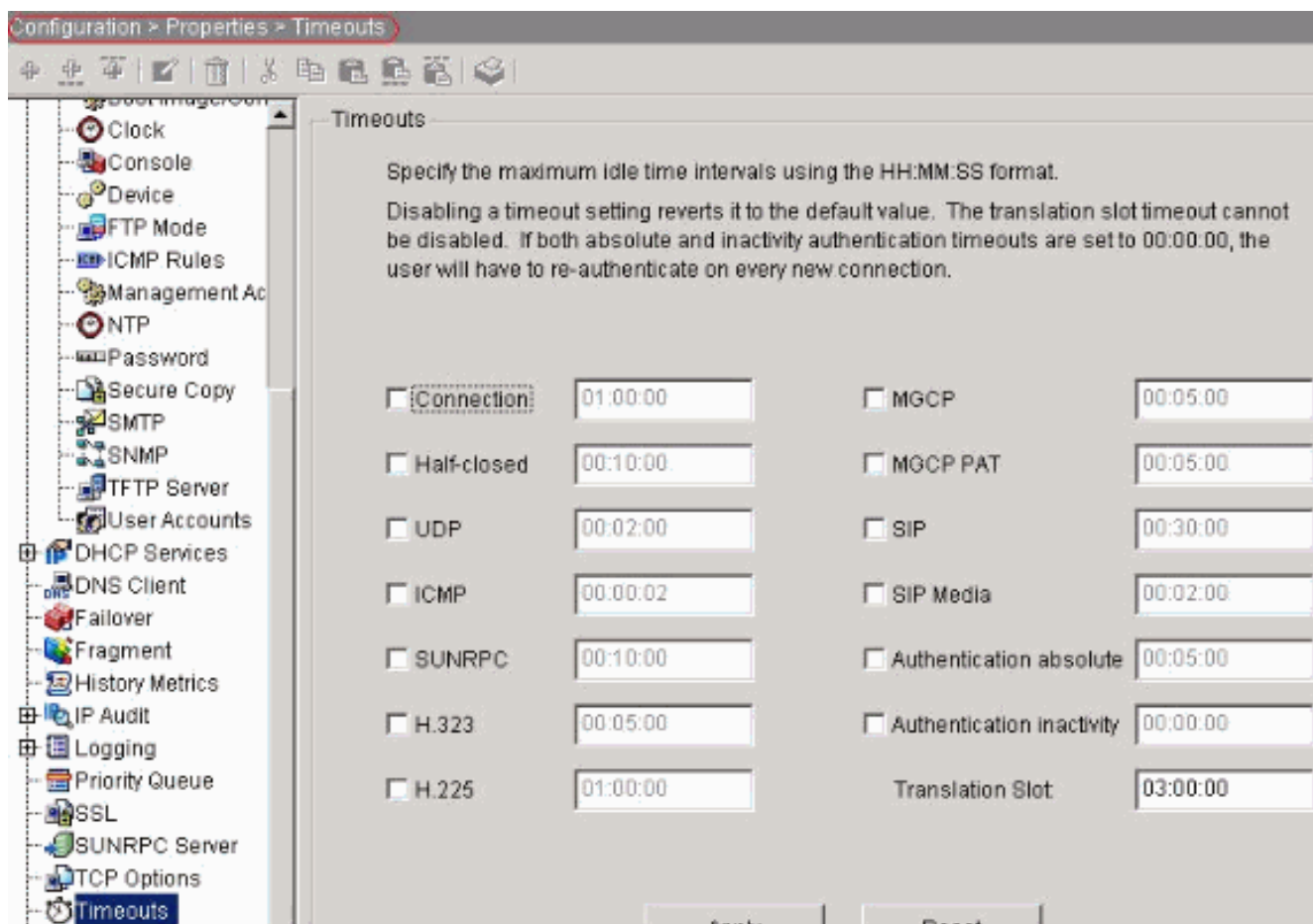
Configuración CLI equivalente como se muestra:

```

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. **Descansos de la configuración** Elija la configuración > las propiedades > los descansos para configurar los diversos descansos. En este escenario, 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`

5. Reglas de la política de servicio de la configuración. Elija las reglas de la directiva > de la política de servicio del > Security (Seguridad) de la configuración > Add para configurar la correspondencia de la clase, correspondencia de políticas para configurar el descanso de conexión TCP como 10 minutos, y aplique la política de servicio en la interfaz exterior como se muestra. Elija el botón de radio de la 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 del **IP Address de origen y de 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

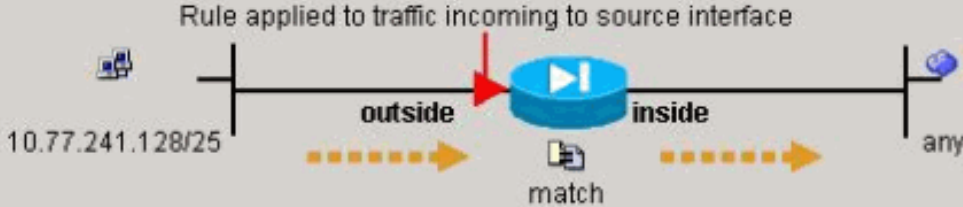
la red 10.77.241.128/26 a cualquier red de destino y aplicarlo para clasificar el telnet.

Action
Select an action: **match**

Time Range
Time Range: -- Not Applied --

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];
```

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:

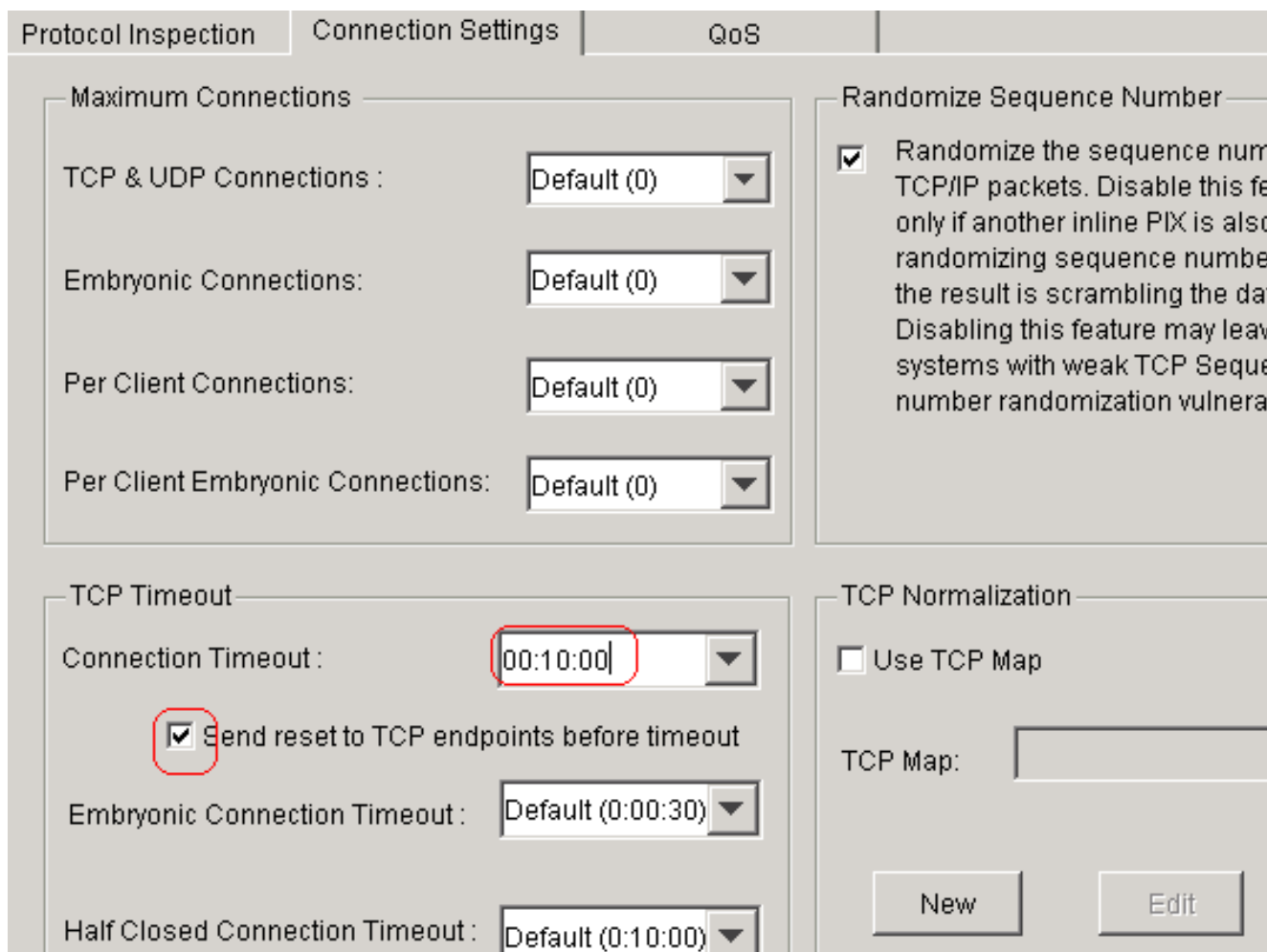
Rule Flow Diagram
 Rule applied to traffic incoming to source interface

 The diagram shows a central router with a play button icon. On the left, a vertical line represents the source interface 'outside' with a red arrow pointing to the router. Below this line is the IP address '10.77.241.128/25'. On the right, a vertical line represents the destination interface 'inside' with a red arrow pointing away from the router. Below this line is the text 'any'. A red arrow points from the source interface to the router, and another red arrow points from the router to the destination interface. Below the router, the word 'match' is written with a red arrow pointing to the router. Dashed orange arrows indicate the flow of traffic from the source to the router and then to the destination.

Protocol and Service
 TCP UDP ICMP IP

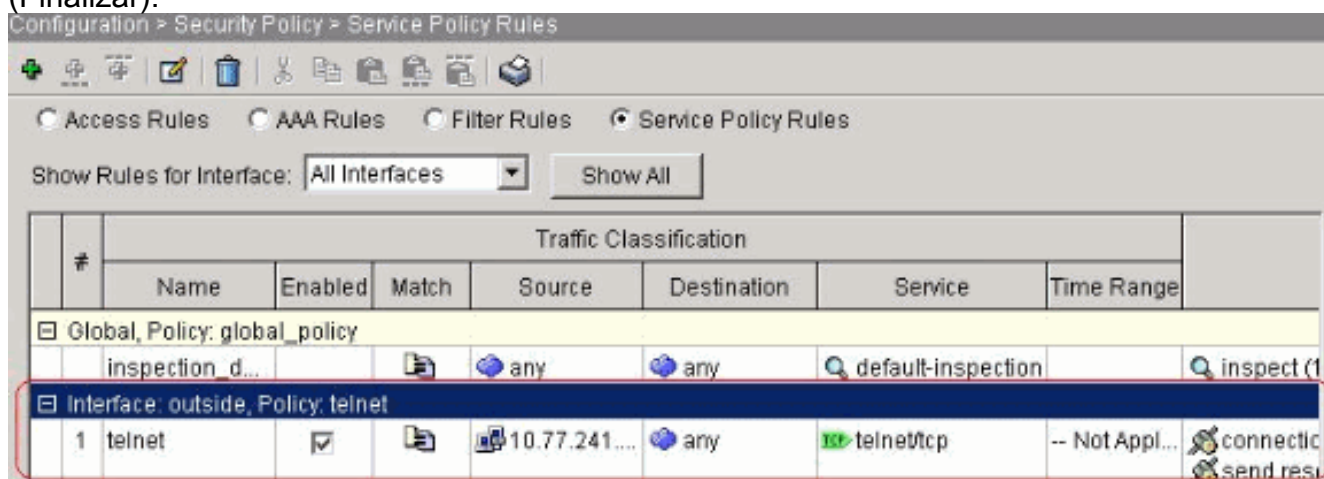
Source Port
 Service =
 Service Group

Destination Port
 Service =
 Service Group

Elija las **configuraciones de la conexión** para configurar 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**.



Haga clic en Finish
(Finalizar).



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 Embryonic](#)

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 de 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 marque la conexión del lanzamiento TCP. El problema puede ser una revocación del IP Address de origen y de destino o una dirección IP mal configurado 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 el MPF.

[Información Relacionada](#)

- [Dispositivos de seguridad Cisco PIX de la serie 500](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)

- [Release Note del dispositivo de seguridad del Cisco PIX](#)
- [Cisco PIX Firewall Software](#)
- [Referencias de Comandos de Cisco Secure PIX Firewall](#)
- [Avisos de campos de productos de seguridad \(incluido PIX\)](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

¿Era este documento útil? [Sí](#) [ningún](#)

Gracias por su feedback.

[Abra un caso de soporte](#) (requiere un [contrato de servicios con Cisco](#).)

Discusiones relacionadas de la comunidad del soporte de Cisco

[La comunidad del soporte de Cisco](#) es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Refiera a los [convenios de los consejos técnicos de Cisco](#) para la información sobre los convenios usados en este documento.

Actualizado: De oct el 16 de 2008

ID del Documento: 68332