

PIX/ASA 7.x e posterior/FWSM: Defina o tempo limite da conexão SSH/Telnet/HTTP usando o exemplo de configuração de MPF

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração](#)

[Timeout Ebrônico](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento fornece uma configuração de exemplo para o PIX 7.1(1) e posterior de um tempo limite que é específico para um aplicativo específico, como SSH/Telnet/HTTP, ao contrário de um que se aplica a todos os aplicativos. Este exemplo de configuração usa a nova Estrutura de Política Modular introduzida no PIX 7.0. Consulte [Utilização da Estrutura de Política Modular](#) para obter mais informações.

Nesta configuração de exemplo, o PIX Firewall é configurado para permitir que a estação de trabalho (10.77.241.129) faça Telnet/SSH/HTTP para o servidor remoto (10.1.1.1) atrás do roteador. Um tempo limite de conexão separado para o tráfego Telnet/SSH/HTTP também é configurado. Todos os outros tráfegos TCP continuam a ter o valor de tempo limite de conexão normal associado ao **tempo limite conn 1:00:00**.

Consulte o [ASA 8.3 e posterior: Defina o tempo limite da conexão SSH/Telnet/HTTP usando o exemplo de configuração do MPF](#) para obter mais informações sobre a configuração idêntica usando o ASDM com o Cisco Adaptive Security Appliance (ASA) com a versão 8.3 e posterior.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no software Cisco PIX/ASA Security Appliance versão 7.1(1) com 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.

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.](#)

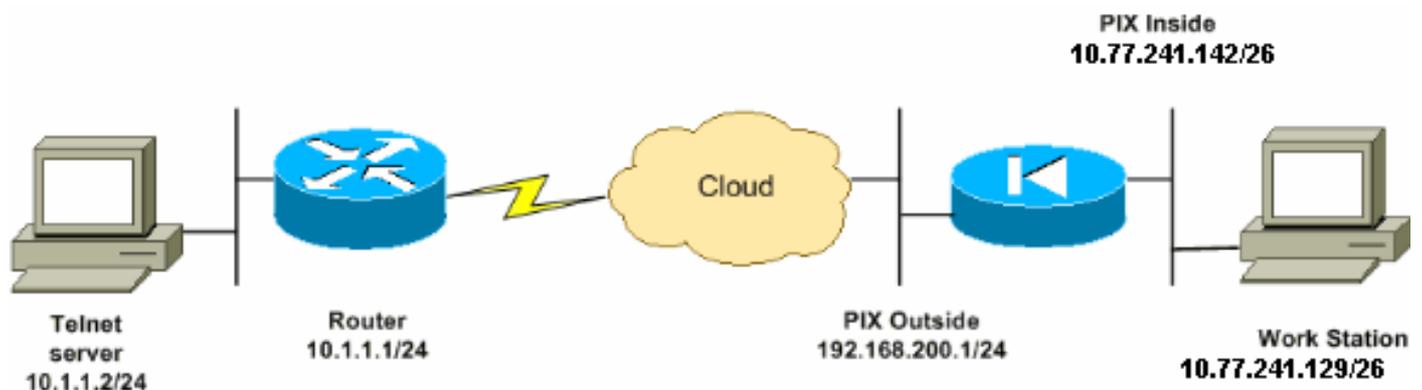
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Observação: os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. Eles são endereços RFC 1918, que foram usados em um ambiente de laboratório.

Configuração

Este documento utiliza esta configuração:

Observação: essas configurações de CLI e ASDM são aplicáveis ao Firewall Service Module (FWSM)

Configuração de CLI:

Configuração 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

```

Configuração do ASDM:

Conclua estes passos para configurar o tempo limite da conexão TCP para o tráfego Telnet com base na lista de acesso que usa ASDM como mostrado.

Observação: consulte [Permitindo Acesso HTTPS para ASDM](#) para obter as configurações básicas para acessar o PIX/ASA por meio do ASDM.

1. **Configurar interfaces** Escolha **Configuration > Interfaces > Add** para configurar as interfaces Ethernet0 (externa) e Ethernet1 (interna) como mostrado.

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:

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

Configuração de CLI equivalente conforme mostrado:

```
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. **Configurar NAT** 0Escolha **Configuration > NAT > Translation Exception Rules > Add** para permitir que o tráfego da rede 10.77.241.128/26 acesse a Internet sem nenhuma tradução.

Configuration > NAT > Translation Exception 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

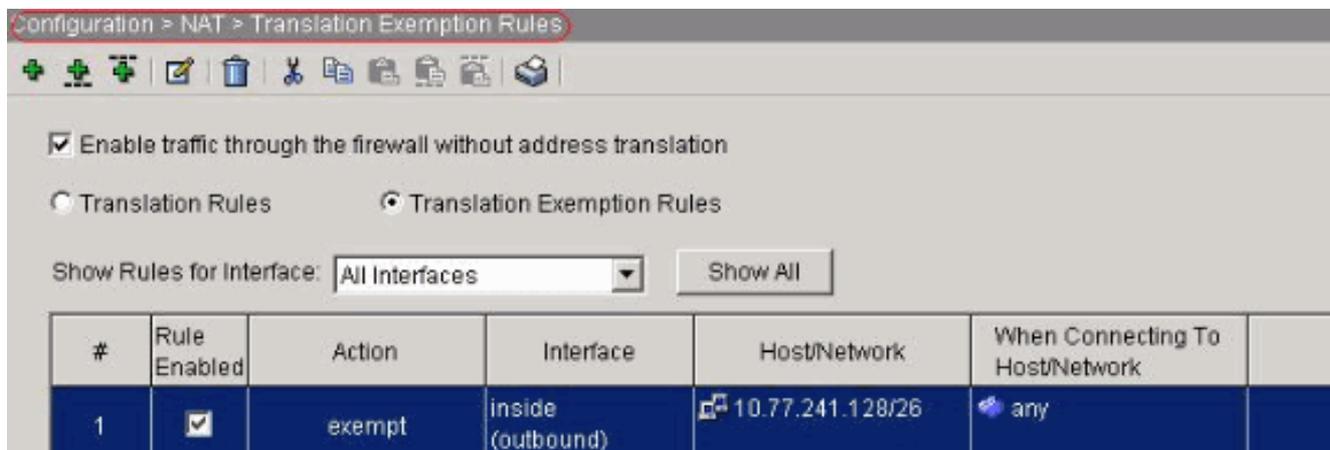
Rule applied to traffic incoming to source interface

The diagram shows a central router with two interfaces: 'inside' and 'outside'. On the left, a vertical line represents the 'any' source interface. A red arrow points from this line to the 'inside' interface of the router. Below this path, a dashed orange arrow points right, labeled 'exempt' with a green checkmark. On the right, a vertical line represents the 'any' destination interface. A dashed orange arrow points from the 'outside' interface of the router to this line.

Please enter the description below (optional):

OK Cancel Help

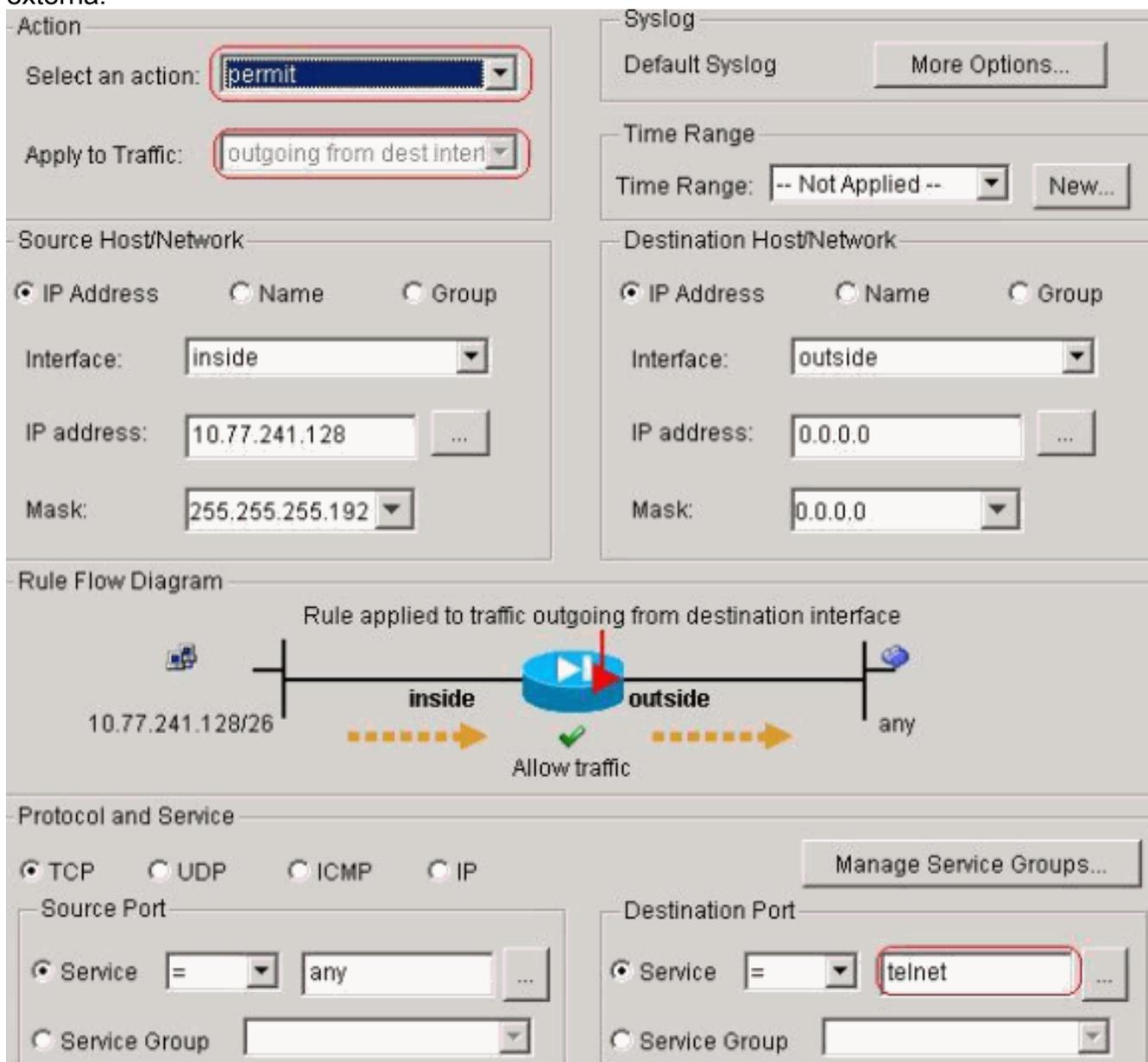
Click
OK.



Configuração de CLI equivalente conforme mostrado:

```
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. **Configurar ACLs** Escolha **Configuration > Security Policy > Access Rules** para configurar as ACLs conforme mostrado. Clique em **Add** para configurar uma ACL 101 que permita que o tráfego Telnet originado da rede 10.77.241.128/26 para qualquer rede de destino e aplique-o para o tráfego de saída na interface externa.



Click **OK**. Da mesma forma para o tráfego ssh e

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

The diagram shows a central router icon with a play button. To the left, a vertical line represents the 'inside' interface with a host icon and the IP address '10.77.241.128/26'. To the right, a vertical line represents the 'outside' interface with a host icon and the label 'any'. A red arrow points from the router to the 'outside' interface. Below the router, a green checkmark and the text 'Allow traffic' are displayed. Dashed orange arrows indicate traffic flow from the 'inside' interface through the router to the 'outside' interface.

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

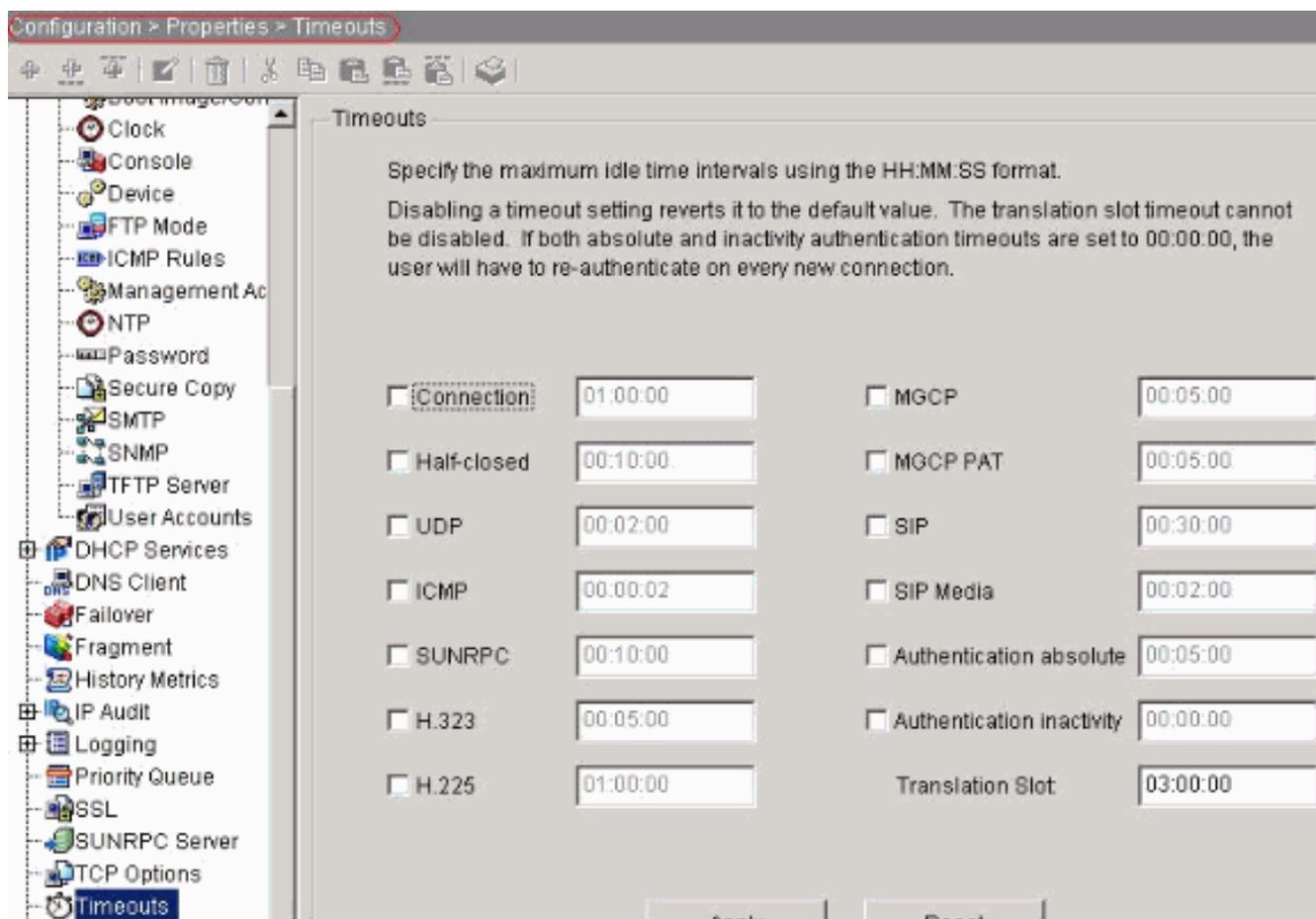
Source Port
 Service =
 Service Group

Destination Port
 Service =
 Service Group

Configuração de CLI equivalente conforme mostrado:

```
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 tempos limite** Escolha **Configuration > Properties > Timeouts** para configurar os vários timeouts. Nesse cenário, mantenha o valor padrão para todos os tempos limite.



Configuração de CLI equivalente conforme mostrado:

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

5. Configurar **regras de política de serviço**. Escolha **Configuration > Security Policy > Service Policy Rules > Add** para configurar o mapa de classes, o mapa de políticas para a configuração do tempo limite da conexão TCP como 10 minutos e aplique a política de serviço na interface externa como mostrado. Escolha o botão de opção **Interface** para escolher **fora - (criar nova política de serviço)**, que será criada, e atribua **telnet** como o nome da 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

Clique em Next. Crie um nome de mapa de classe **telnet** e escolha a caixa de seleção **Endereço IP de origem e destino (usa ACL)** nos critérios de correspondência de tráfego.

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 an 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.

Clique em Next. Crie uma ACL para corresponder o tráfego Telnet originado da rede 10.77.241.128/26 a qualquer rede de destino e aplique-o à classe

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

```
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 Manage Service Groups...

Source Port
 Service = **any** ...
 Service Group

Destination Port
 Service = **telnet** ...
 Service Group

Clique em Next. Da mesma forma para o tráfego ssh e 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:

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. To the left, a vertical line represents the 'outside' interface, with a red arrow pointing towards the router. Below this line is the IP address '10.77.241.128/25'. To the right, a vertical line represents the 'inside' interface, with a red arrow pointing away from the router. Below this line is the text 'any'. A red arrow points to the router from the top. Below the router, the word 'match' is written. Two orange dashed arrows point from the 'outside' interface towards the 'inside' interface, indicating the direction of traffic flow.

Protocol and Service
 TCP UDP ICMP IP

Source Port
 Service =
 Service Group

Destination Port
 Service =
 Service Group

Escolha **Connection Settings** para configurar o TCP Connection Timeout como 10 minutos e também escolha a caixa de seleção **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: []

New Edit

Clique em
Finish.

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

Configuração de CLI equivalente conforme mostrado:

```
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
```

Timeout Embrionário

Uma conexão embrionária é a conexão que está meio aberta ou, por exemplo, o handshake triplo não foi concluído para ela. É definido como o tempo limite de SYN no ASA; por padrão, o tempo limite de SYN no ASA é de 30 segundos. Esta é a maneira de configurar o tempo limite de Embrionária:

```
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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A [Output Interpreter Tool \(somente clientes registrados\) \(OIT\) oferece suporte a determinados comandos show](#). Use a OIT para visualizar uma análise da saída do comando **show**.

Execute o comando **show service-policy interface outside** para verificar suas configurações.

```
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
```

Emita o comando [show service-policy flow](#) para verificar se o tráfego específico corresponde às configurações da política de serviço.

Esta saída de comando mostra um exemplo:

```
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

Se você descobrir que o tempo limite da conexão não funciona com o Modular Policy Framework (MPF), verifique a conexão de início do TCP. O problema pode ser uma reversão do endereço IP origem e destino ou um endereço IP mal configurado na lista de acesso não corresponde no MPF para definir o novo valor de tempo limite ou para alterar o tempo limite padrão para o aplicativo. Crie uma entrada da lista de acesso (origem e destino) de acordo com o início da conexão para definir o tempo limite da conexão com o MPF.

Informações Relacionadas

- [Cisco PIX 500 Series Security Appliances](#)
- [Dispositivos de segurança adaptáveis Cisco ASA 5500 Series](#)
- [Cisco PIX Firewall Software](#)
- [Referências do comando Cisco Secure PIX Firewall](#)
- [Avisos de campo de produto de segurança \(incluindo PIX\)](#)
- [Solicitações de Comentários \(RFCs\)](#)