

# PIX/ASA 7.x 及更高版本/FWSM：使用 MPF 设置 SSH/Telnet/HTTP 连接超时的配置示例

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[初期超时](#)

[验证](#)

[故障排除](#)

## 简介

本文档为 PIX 7.1(1) 和更高版本提供特定于特定应用程序（如 SSH/Telnet/HTTP）的超时（而非适用于所有应用程序的超时）的配置示例。此配置示例使用 PIX 7.0 中引入的新模块化策略框架。有关详细信息，[请参阅使用模块化策略框架](#)。

在本配置示例中，PIX 防火墙配置为允许工作站 (10.77.241.129) 连接到 Telnet/SSH/HTTP，再到路由器后的远程服务器 (10.1.1.1)。还配置了单独的 Telnet/SSH/HTTP 数据流连接超时。所有其他 TCP 流量继续使用与 `timeout conn 1:00:00` 关联的正常连接超时值。

请参阅[AASA 8.3及更高版本：使用MPF设置SSH/Telnet/HTTP连接超时配置示例](#)，了解有关使用 ASDM 和 8.3 及更高版本的思科自适应安全设备 (ASA) 进行相同配置的详细信息。

## 先决条件

### 要求

本文档没有任何特定的要求。

## 使用的组件

本文档中的信息基于具有自适应安全管理器 (ASDM) 5.1 的 Cisco PIX/ASA 安全设备软件版本 7.1(1)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 规则

有关文档约定的更多信息，请参考 [Cisco 技术提示约定](#)。

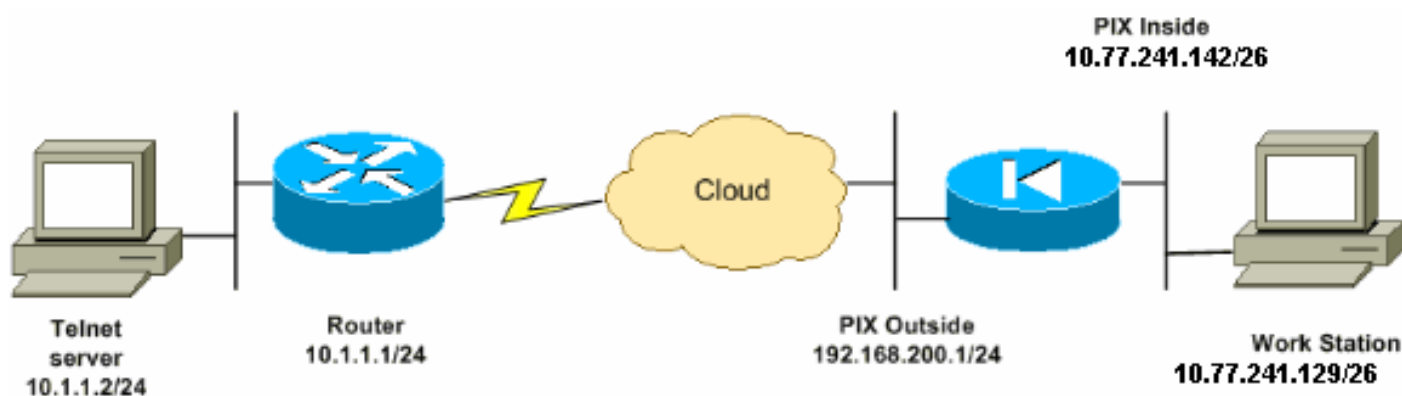
## 配置

本部分提供有关如何配置本文档所述功能的信息。

**注意：**要获取有关本部分中所使用命令的更多信息，可使用 [命令查找工具](#)（仅限 [已注册](#) 客户）。

## 网络图

本文档使用以下网络设置：



**注意：**此配置中使用的IP编址方案在Internet上不可合法路由。这些地址是在实验室环境中使用的RFC 1918 地址。

## 配置

本文档使用以下配置：

**注意：**这些CLI和ASDM配置适用于防火墙服务模块(FWSM)

### CLI 配置：

#### PIX 配置

```
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 配置：

完成以下步骤，以基于使用 ASDM 的访问控制列表设置 Telnet 数据流的 TCP 连接超时，如下所示。

**注意：**要通过ASDM访问[PIX/ASA](#)，请参阅允许ASDM的HTTPS访问以获取基本设置。

1. **配置接口**选择 **Configuration > Interfaces > Add** 以配置接口 **Ethernet0 (外部)** 和 **Ethernet1 (内部)**，如下所示。

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:

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

等效的 CLI 配置如下所示：

```
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. 配置 NAT 0 选择 Configuration > NAT > Translation Exemption Rules > Add，以允许来自网络 10.77.241.128/26 的数据流在未进行任何转换的情况下便可访问 Internet。

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.

Configuration > NAT > Translation Exemption Rules

Enable traffic through the firewall without address translation

Translation Rules  Translation Exemption Rules

Show Rules for Interface:

#	Rule Enabled	Action	Interface	Host/Network	When Connecting To Host/Network
1	<input checked="" type="checkbox"/>	exempt	inside (outbound)	10.77.241.128/26	any

等效的 CLI 配置如下所示：

```
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. 配置 ACL 选择 Configuration > Security Policy > Access Rules 以配置 ACL，如下所示。单击 Add 来配置一个允许源于网络 10.77.241.128/26 的 Telnet 数据流传输到所有目标网络的 ACL 101，并将它应用于外部接口上的出站数据流。

The screenshot shows the configuration for an Access Rule. The 'Action' is set to 'permit' and 'Apply to Traffic' is 'outgoing from destination interface'. The 'Source Host/Network' is configured with IP Address 10.77.241.128 and Mask 255.255.255.192 on the 'inside' interface. The 'Destination Host/Network' is configured with IP Address 0.0.0.0 and Mask 0.0.0.0 on the 'outside' interface. The 'Rule Flow Diagram' shows traffic flow from the 'inside' interface (10.77.241.128/26) to the 'outside' interface (any) with a green checkmark and 'Allow traffic' text. The 'Protocol and Service' section is set to TCP and telnet.

Click OK.对于 ssh 和 http 数据流，配置是类似的：  
：



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:



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

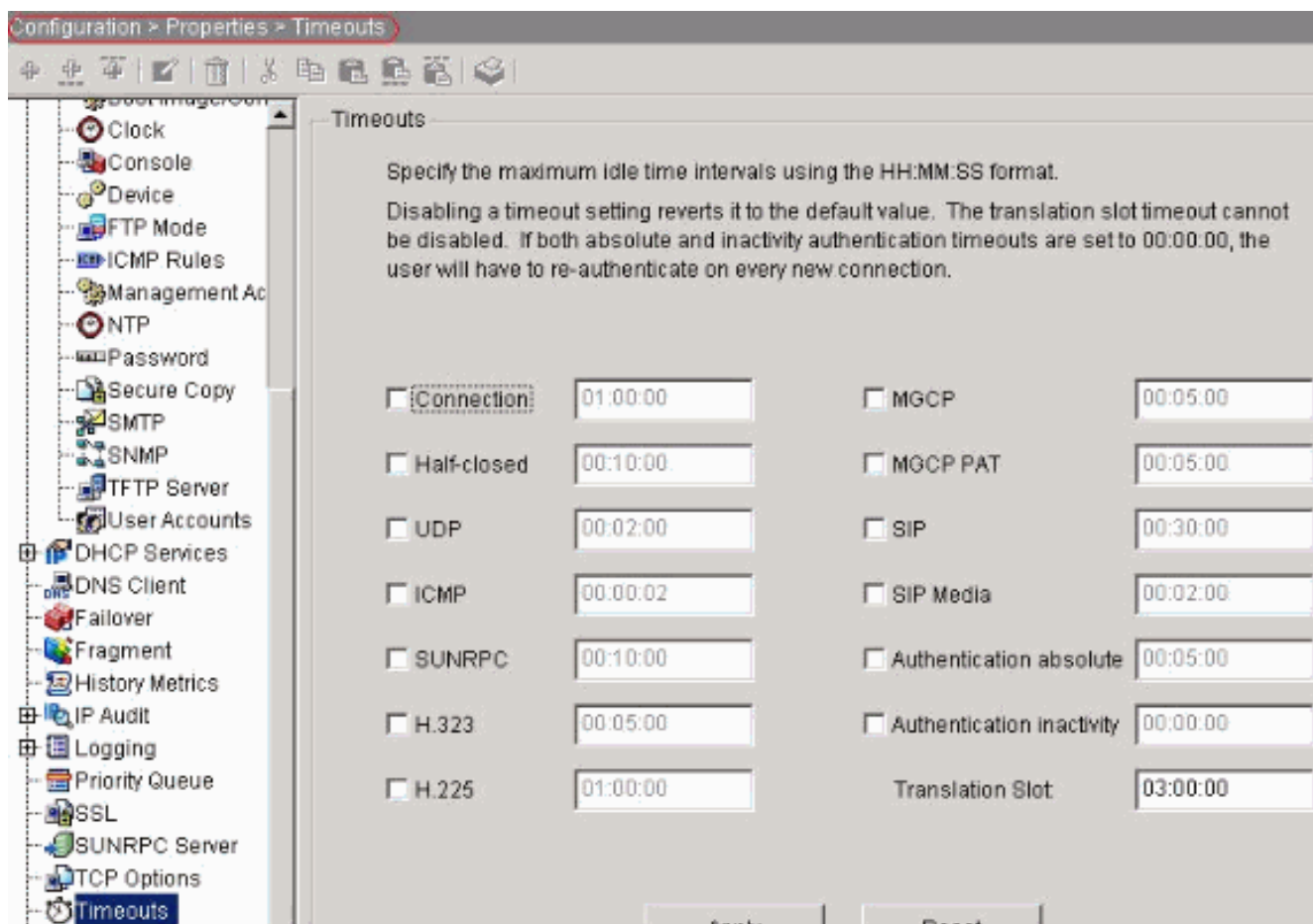
Service =

Service Group

等效的 CLI 配置如下所示：

```
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. 配置超时选择 **Configuration > Properties > Timeouts** 以配置各种超时。在此方案中，请保持所有超时的默认值。



等效的 CLI 配置如下所示：

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

5. 配置 Service Policy Rules。选择 Configuration > Security Policy > Service Policy Rules > Add 以配置类映射、策略映射以用于将 TCP 连接超时设置为 10 分钟，并将服务策略应用于外部接口，如下所示。选择 Interface 单选按钮来选择 outside - (create new service policy) (它将被创建)，然后将 telnet 指定为策略名称。

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

单击 **Next**。创建类映射名称 telnet，然后选中 Traffic 匹配条件中的 Source and Destination IP address (uses ACL) 复选框。

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.


单击 **Next**。创建 ACL 以将源于网络 10.77.241.128/26 的 Telnet 数据流与所有目标网络匹配，并将它应用于 telnet 类。

**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


单击 **Next**。对于 ssh 和 http 数据流，配置是类似的：  
 :

**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:

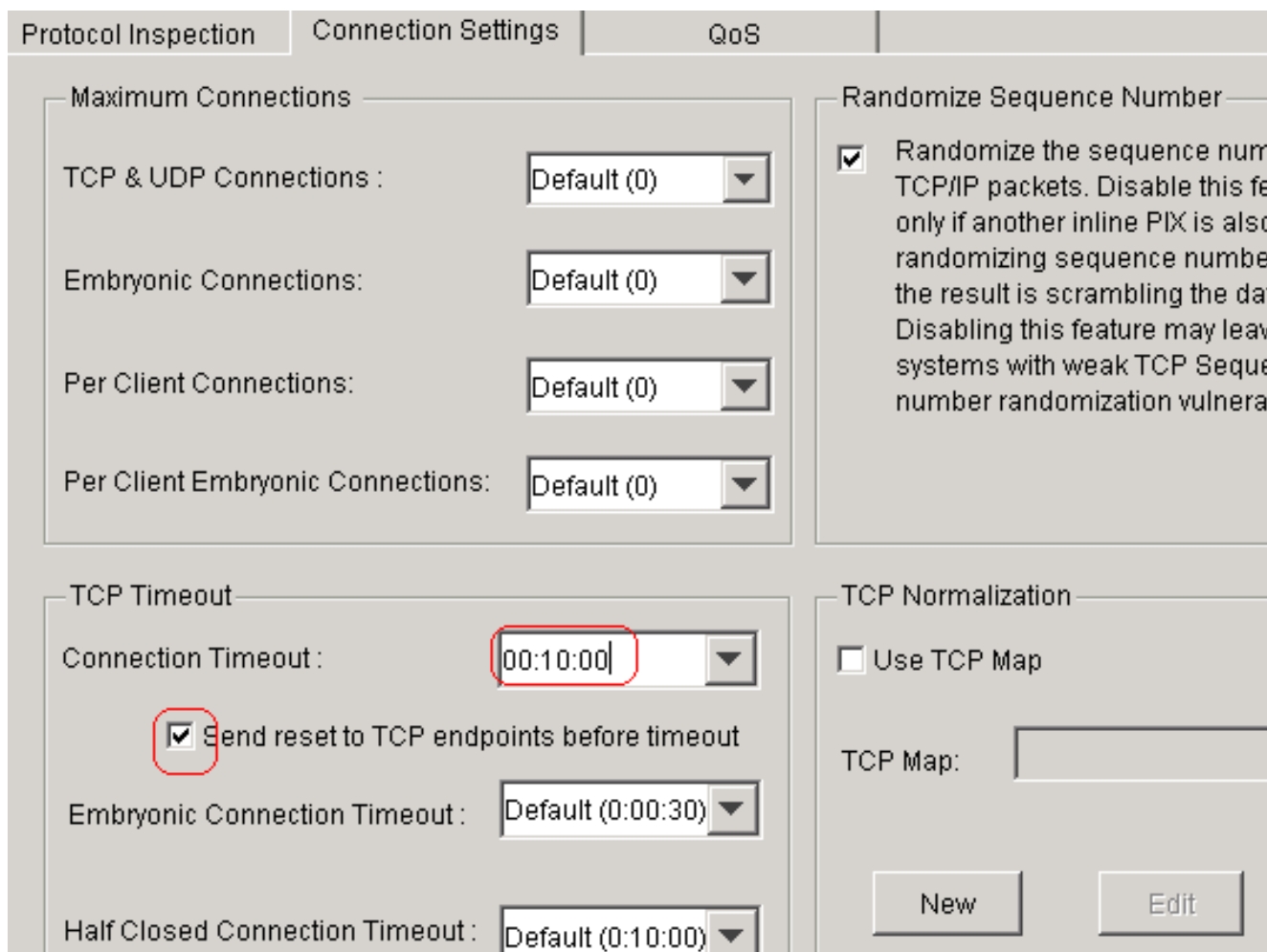
Destination Host/Network  
 IP Address  Name  Group  
Interface:   
IP address:    
Mask:

Rule Flow Diagram  
Rule applied to traffic incoming to source interface  

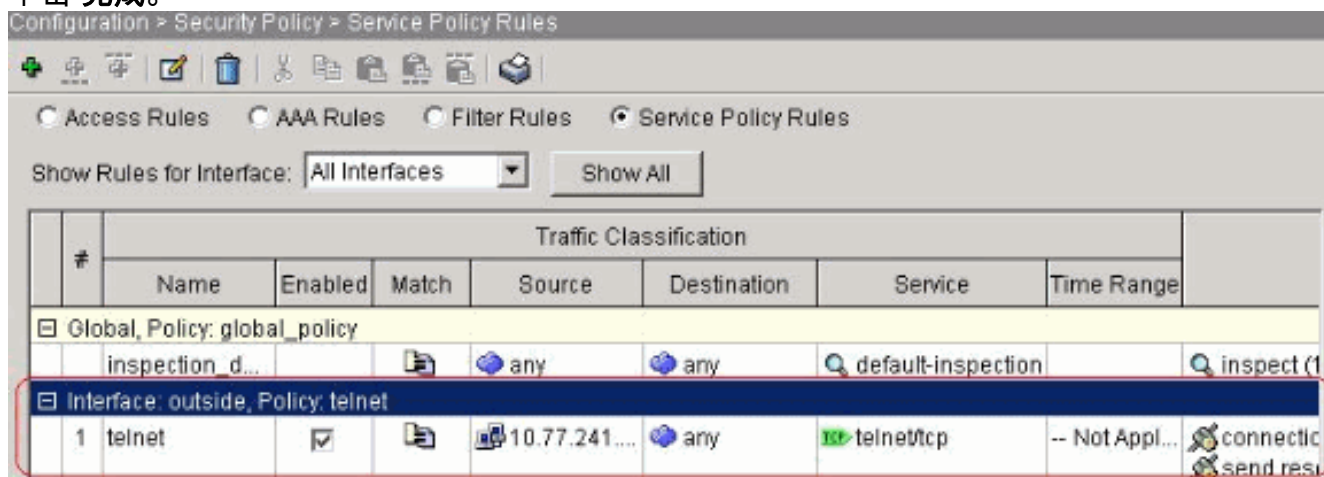
Protocol and Service  
 TCP  UDP  ICMP  IP   
Source Port  
 Service =    
 Service Group

Destination Port  
 Service =    
 Service Group

选择 Connection Settings 以将 TCP Connection Timeout 设置为 10 分钟，并选中 Send reset to TCP endpoints before timeout 复选框。



单击 完成。



等效的 CLI 配置如下所示：

```
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
```

## 初期超时



初期连接是半打开的连接，例如，尚未为其完成三方握手的连接。它被定义为 ASA 上的 SYN 超时：默认情况下，ASA 上的 SYN 超时为 30 秒。这是配置初期超时的方式：

```
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
```

## 验证

使用本部分可确认配置能否正常运行。

[命令输出解释程序 \( 仅限注册用户 \) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输出的分析。

发出 **show service-policy interface outside** 命令以验证您的配置。

```
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
```

发出 **show service-policy flow** 命令以验证特定数据流是否与服务策略配置匹配。

此命令输出显示了一个示例：

```
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
```

## 故障排除

如果发现连接超时不适用于模块化策略框架(MPF)，则检查TCP启动连接。问题可能是颠倒了源和目标 IP 地址，或访问控制列表中的 IP 地址与用于为应用程序设置新超时值或更改默认超时的 MPF

中的 IP 地址不匹配。按照连接启动创建访问控制列表条目（源和目标），以使用 MPF 设置连接超时。

## 相关信息

- [Cisco PIX 500 系列安全设备](#)
- [Cisco ASA 5500 系列自适应安全设备](#)
- [Cisco PIX 防火墙软件](#)
- [Cisco Secure PIX 防火墙命令参考](#)
- [安全产品 Field Notices \(包括 PIX\)](#)
- [请求注解 \(RFC\)](#)