

PIX/ASA 7.x et versions ultérieures/FWSM : Exemple de configuration de définition de l'expiration de la connexion SSH/Telnet/HTTP à l'aide de MPF

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration](#)

[Délai d'expiration embryonique](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document fournit un exemple de configuration pour PIX 7.1(1) et les versions ultérieures d'un délai d'attente spécifique à une application particulière telle que SSH/Telnet/HTTP, par opposition à une configuration qui s'applique à toutes les applications. Cet exemple de configuration utilise le nouveau cadre de stratégie modulaire introduit dans PIX 7.0. Référez-vous à [Utilisation d'un cadre de politique modulaire](#) pour plus d'informations.

Dans cet exemple de configuration, le pare-feu PIX est configuré pour autoriser la station de travail (10.77.241.129) à établir une connexion Telnet/SSH/HTTP au serveur distant (10.1.1.1) derrière le routeur. Un délai de connexion distinct au trafic Telnet/SSH/HTTP est également configuré. Tous les autres trafics TCP continuent d'avoir la valeur de délai d'expiration de connexion normale associée au **délai d'expiration conn 1:00:00**.

Reportez-vous à [AASA 8.3 et versions ultérieures : Définissez le délai d'attente de connexion SSH/Telnet/HTTP à l'aide de l'exemple de configuration MPF](#) pour plus d'informations sur la configuration identique à l'aide d'ASDM avec Cisco Adaptive Security Appliance (ASA) avec la version 8.3 et ultérieure.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur le logiciel Cisco PIX/ASA Security Appliance Version 7.1(1) avec 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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

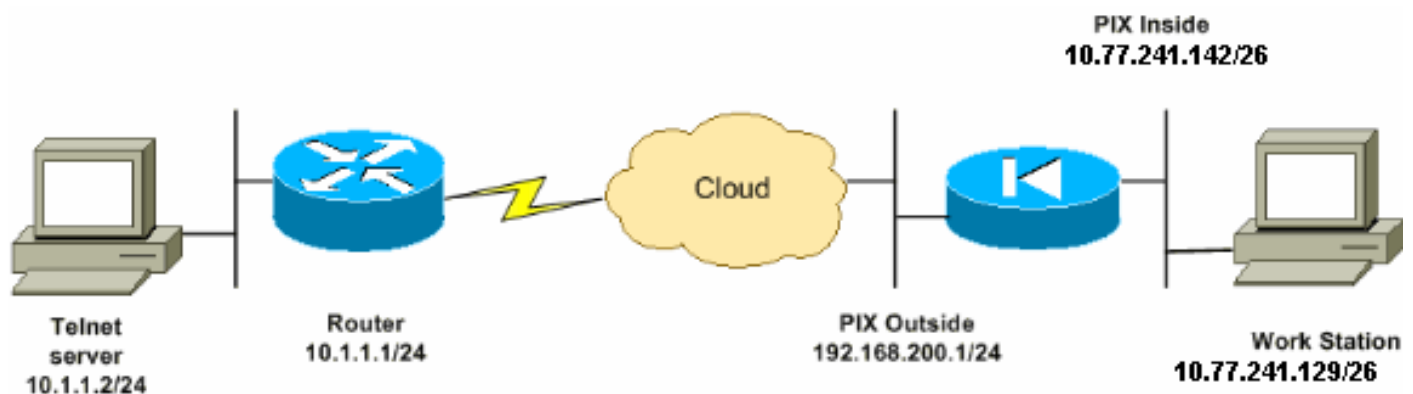
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) afin d'obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Remarque : les schémas d'adressage IP utilisés dans cette configuration ne sont pas routables légalement sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Configuration

Ce document utilise la configuration suivante :

Remarque : ces configurations CLI et ASDM sont applicables au module de service de pare-feu (FWSM)

Configuration CLI :

Configuration 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

```

Configuration ASDM :

Complétez ces étapes afin de configurer le délai de connexion TCP pour le trafic Telnet en

fonction de la liste d'accès qui utilise ASDM comme indiqué.

Remarque : Reportez-vous à [Autoriser l'accès HTTPS pour ASDM](#) pour les paramètres de base afin d'accéder au PIX/ASA par l'intermédiaire d'ASDM.

1. **Configurer les interfaces** Choisissez **Configuration > Interfaces > Add** afin de configurer les interfaces Ethernet0 (externe) et Ethernet1 (interne) comme indiqué.

The screenshot shows the 'Configure Hardware Properties' 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 set to '1500' and the 'Description' field is empty. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

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

Configuration CLI équivalente comme indiqué :

```
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. Configuration de NAT 0 Choisissez **Configuration > NAT > Translation Exemption Rules > Add** afin de permettre au trafic du réseau 10.77.241.128/26 d'accéder à Internet sans traduction.

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**

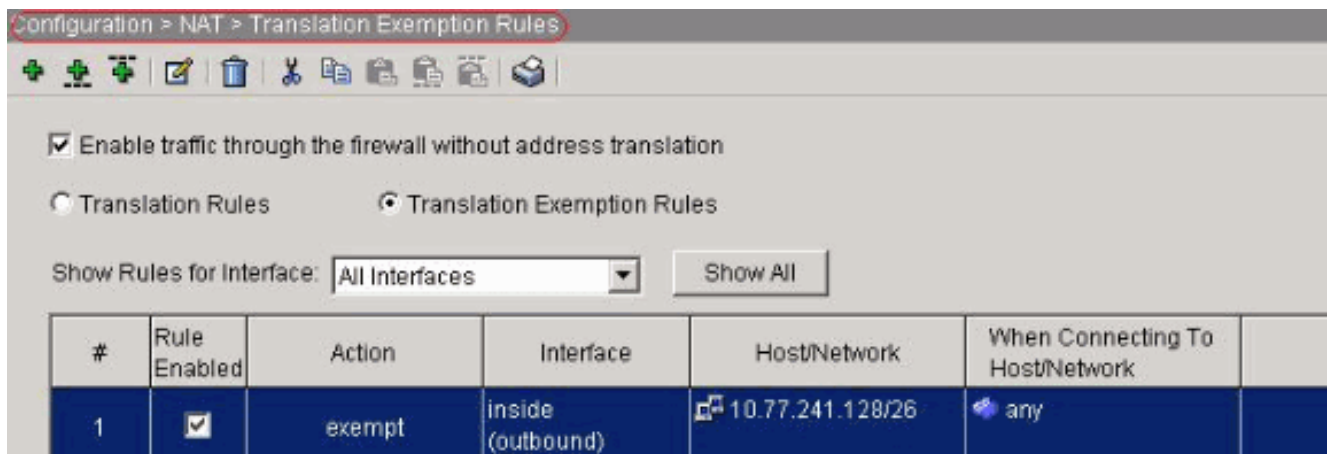
Rule Flow Diagram

Rule applied to traffic incoming to source interface

Please enter the description below (optional):

OK Cancel Help

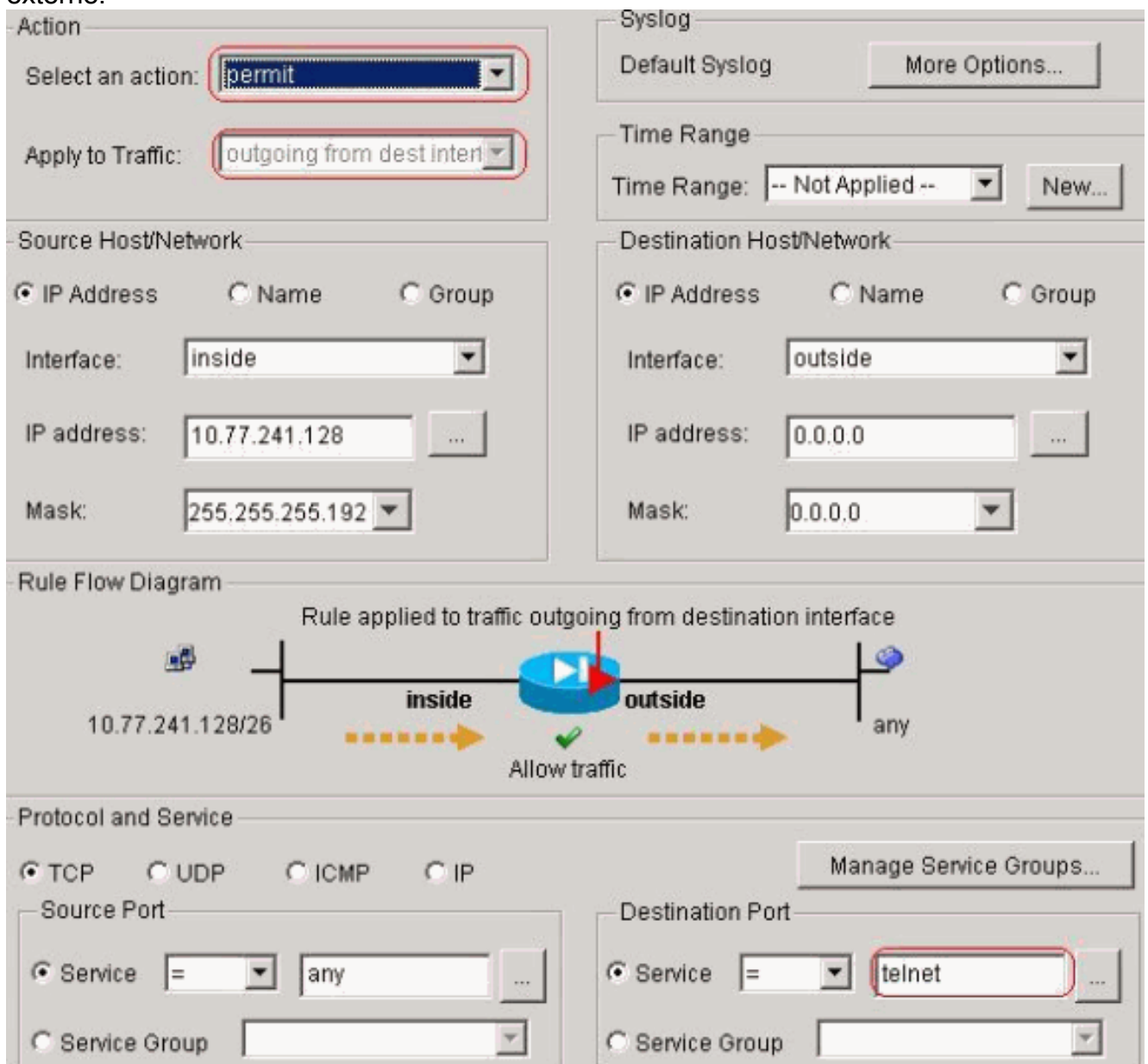
Click
OK.



Configuration CLI équivalente comme indiqué :

```
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. **Configuration des listes de contrôle d'accès** Choisissez **Configuration > Security Policy > Access Rules** afin de configurer les listes de contrôle d'accès comme indiqué. Cliquez sur **Add** afin de configurer une liste de contrôle d'accès 101 qui autorise le trafic Telnet provenant du réseau 10.77.241.128/26 vers n'importe quel réseau de destination et l'applique au trafic sortant sur l'interface externe.



Click OK. De même pour le trafic ssh et http

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

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

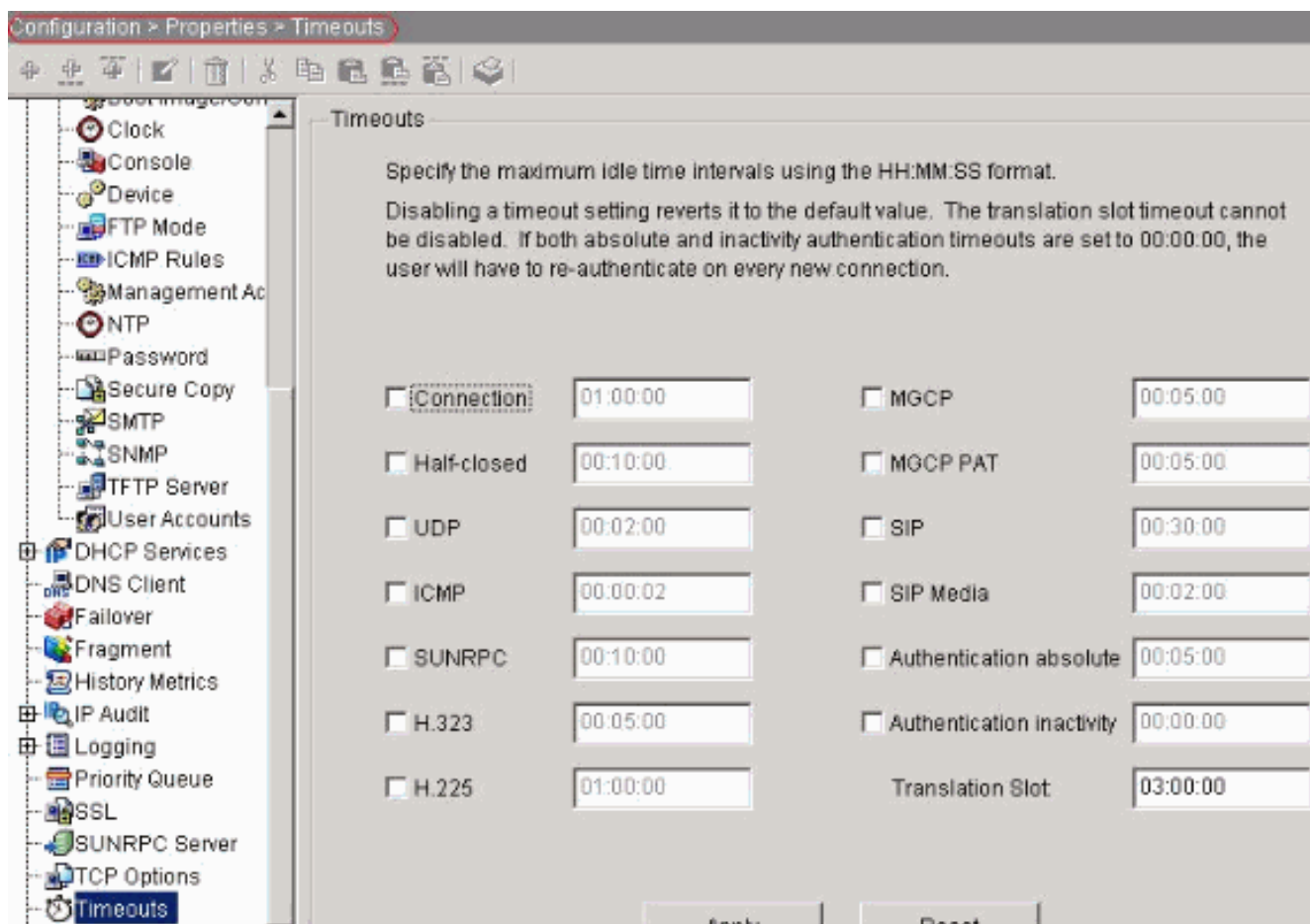
Service =

Service Group

Configuration CLI équivalente comme indiqué :

```
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. **Configurer les délais d'attente** Choisissez **Configuration > Propriétés > Timeouts** afin de configurer les différents timeouts. Dans ce scénario, conservez la valeur par défaut pour tous les dépassements de délai.



Configuration CLI équivalente comme indiqué :

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

5. Configurer les règles de stratégie de service. Choisissez **Configuration > Security Policy > Service Policy Rules > Add** afin de configurer le mappage de classe, le mappage de stratégie pour la configuration du délai de connexion TCP comme 10 minutes, et appliquez la stratégie de service sur l'interface externe comme indiqué. Sélectionnez la case d'option **Interface** afin de choisir **externe - (créer une nouvelle stratégie de service)**, qui doit être créée, et attribuez **telnet** comme nom de stratégie.

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

Cliquez sur **Next** (Suivant). Créez un nom de mappage de classe **telnet** et activez la case à cocher **Adresse IP source et de destination (utilise la liste de contrôle d'accès)** dans les critères de correspondance de trafic.

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.

Cliquez sur **Next** (Suivant). Créez une liste de contrôle d'accès afin de faire correspondre le


trafic Telnet provenant du réseau 10.77.241.128/26 à n'importe quel réseau de destination et appliquez-le à la classe 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

Cliquez sur **Next** (Suivant). De même pour le trafic ssh et 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' and 'inside'. A red arrow points to the 'outside' interface, indicating the source of traffic. A red arrow also points to the router, with a red box around the word 'match' below it, indicating the action applied to the traffic. Dashed orange arrows show the flow of traffic from the 'outside' interface through the router to the 'inside' interface, and finally 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

Choisissez **Paramètres de connexion** afin de configurer le délai d'attente de connexion TCP comme 10 minutes, et activez également la case à cocher **Envoyer la réinitialisation aux points de terminaison TCP avant expiration**.

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

Cliquez sur
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

Configuration CLI équivalente comme indiqué :

```
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
```


Délai d'expiration embryonique

Une connexion embryonnaire est la connexion qui est à moitié ouverte ou, par exemple, la connexion en trois étapes n'a pas été effectuée pour elle. Il est défini comme délai SYN sur l'ASA ; par défaut, le délai d'attente SYN sur l'ASA est de 30 secondes. Voici comment configurer Embryonic Timeout :

```
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
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\) prend en charge certaines commandes show](#). Employez l'OIT afin d'afficher une analyse de la sortie de la commande show.

Émettez la commande **show service-policy interface outside** afin de vérifier vos configurations.

```
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
```

Émettez la commande [show service-policy flow](#) afin de vérifier que le trafic particulier correspond aux configurations de la stratégie de service.

Cette sortie de commande montre un exemple :

```
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
```

Dépannage

Si vous constatez que le délai d'expiration de la connexion ne fonctionne pas avec le cadre de stratégie modulaire (MPF), vérifiez la connexion d'initialisation TCP. Le problème peut être un renversement de l'adresse IP source et de destination ou une adresse IP mal configurée dans la liste d'accès ne correspond pas dans le MPF pour définir la nouvelle valeur de délai d'attente ou pour modifier le délai d'attente par défaut de l'application. Créez une entrée de liste d'accès (source et destination) conformément à l'initialisation de la connexion afin de définir le délai d'attente de connexion avec MPF.

Informations connexes

- [Dispositifs de sécurité de la gamme Cisco PIX 500](#)
- [Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500](#)
- [Logiciels pare-feu Cisco PIX](#)
- [Références des commandes du pare-feu Cisco Secure PIX](#)
- [Notices de champs relatives aux produits de sécurité \(y compris PIX\)](#)
- [Demandes de commentaires \(RFC\)](#)