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

ID de document : 68332

Mis à jour : Oct. 16, 2008

Produits connexes

- Cisco Adaptive Security Device Manager
- Pare-feu de la deuxième génération de gamme 5500-X de Cisco ASA
- Dispositifs de sécurité de la gamme Cisco PIX 500

Contenu

Introduction

Ces document fournit une configuration d'échantillon pour PIX 7.1(1) et plus tard d'un délai d'attente qui est spécifique à une application particulière telle que SSH/Telnet/HTTP, par opposition à un 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 utilisant le pour en

savoir plus modulaire de cadre de stratégie.

Dans cette configuration d'échantillon, le Pare-feu PIX est configuré pour permettre le poste de travail (10.77.241.129) à Telnet/SSH/HTTP au serveur distant (10.1.1.1) derrière le routeur. Un délai d'attente de connexion distinct au trafic Telnet/SSH/HTTP est également configuré. Tout autre trafic TCP continue à avoir la valeur du dépassement de durée normale de connexion associée avec **conn. 1:00:00 de délai d'attente**.

Référez-vous à AASA 8.3 et plus tard : Placez le délai d'attente de connexion SSH/Telnet/HTTP utilisant l'exemple de configuration MPF pour plus d'informations sur la configuration identique utilisant l'ASDM avec l'appliance de sécurité adaptable Cisco (ASA) avec la version 8.3 et ultérieures.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur la version de logiciel d'appareils de Sécurité de Cisco PIX/ASA 7.1(1) avec Adaptive Security Device Manager (ASDM) 5.1.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

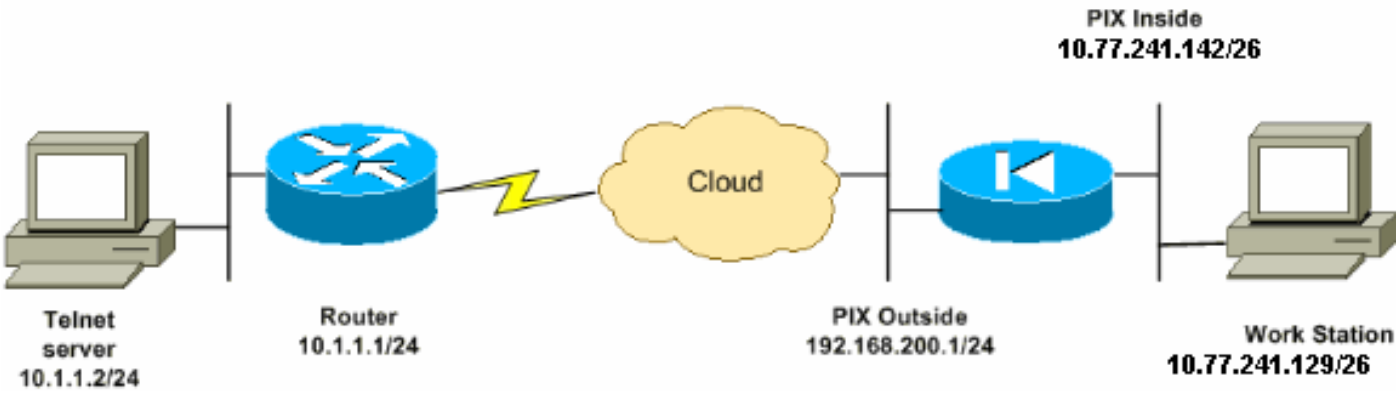
Configurez

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

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour 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 d'IP utilisés dans cette configuration ne sont pas légalement routables 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 les configurations CLI et ASDM s'appliquent 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
```

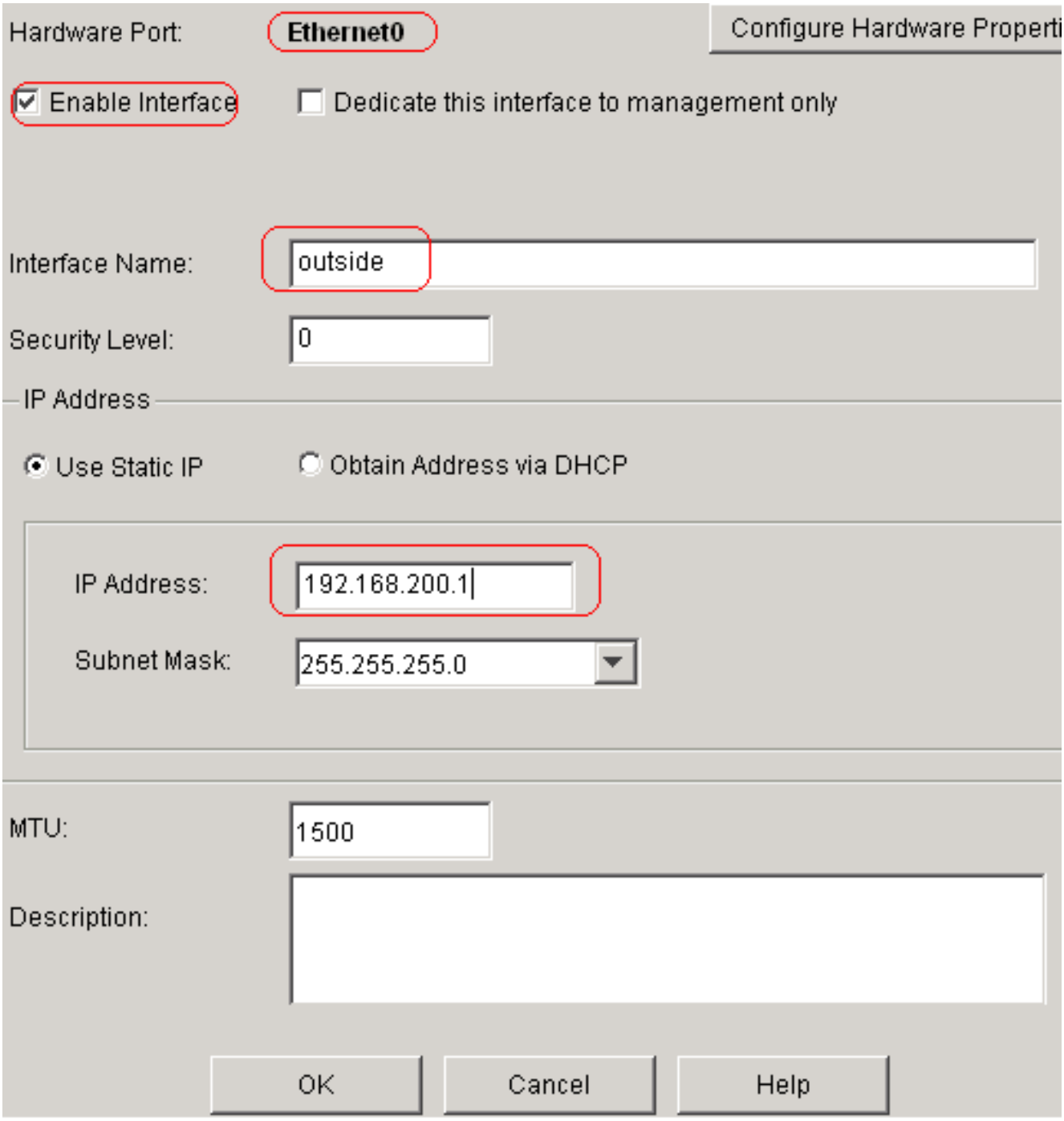
```
pager lines 24 mtu inside 1500 mtu outside 1500 no
failover no asdm history enable arp timeout 14400 nat
(inside) 0 access-list inside_nat0_outbound access-group
101 in interface outside route outside 0.0.0.0 0.0.0.0
192.168.200.2 1 timeout xlate 3:00:00 !--- The default
connection timeout value 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
```

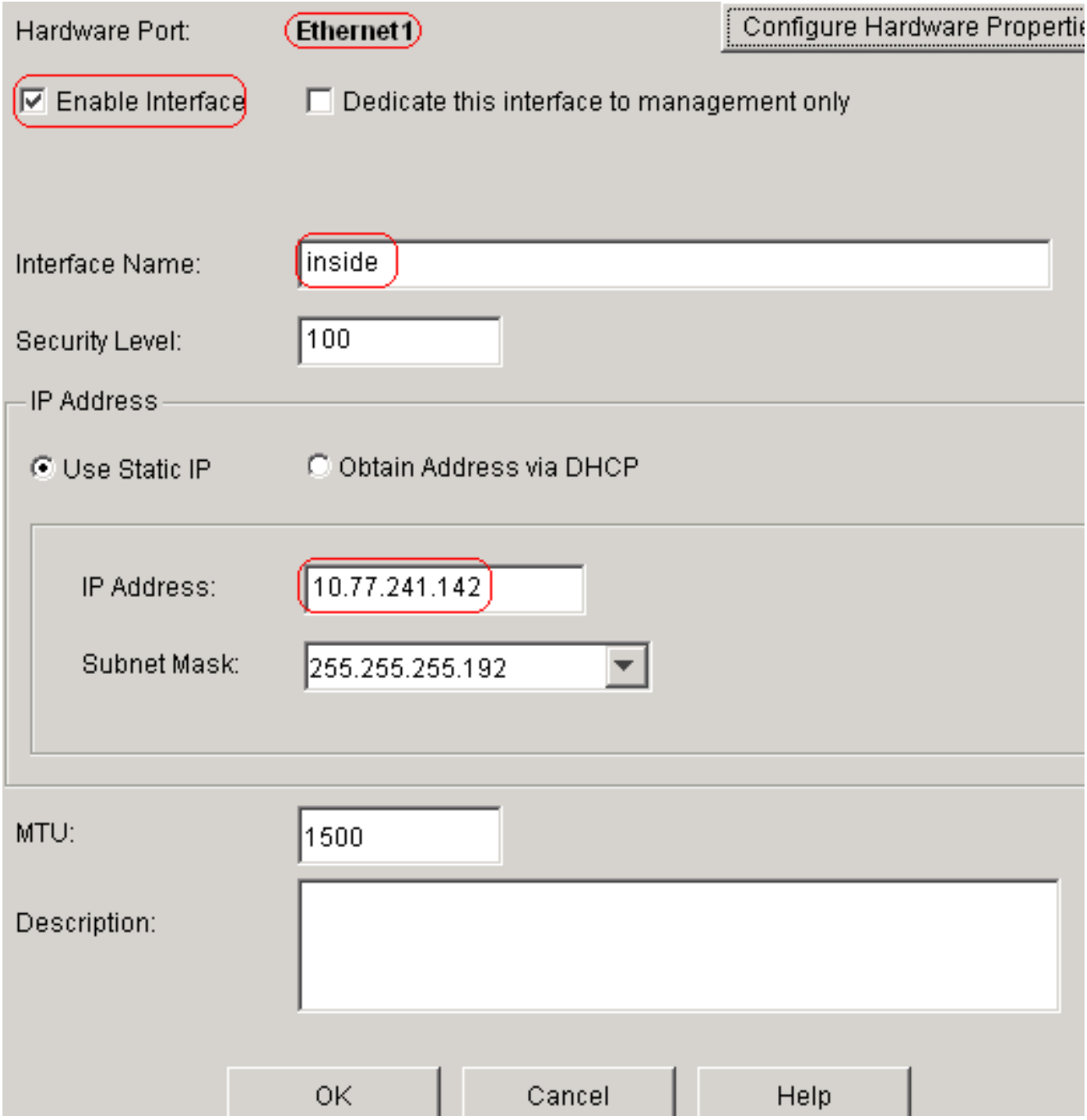
Configuration ASDM :

Terminez-vous ces étapes afin d'installer le délai d'attente de connexion TCP pour le trafic de telnet basé sur la liste d'accès qui utilise l'ASDM comme affiché.

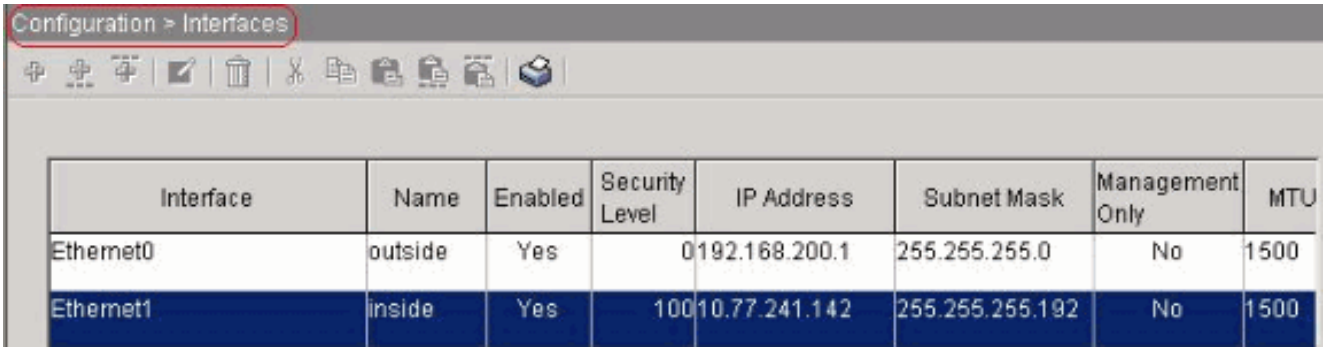
Remarque: Référez-vous à permettre à HTTPS Access pour l'ASDM pour des paramètres de base afin d'accéder au PIX/ASA par l'ASDM.

1. **Configurez les interfaces**Choisissez le **Configuration > Interfaces > ajoutent** afin de configurer les interfaces Ethernet0 (dehors) et Ethernet1 (à l'intérieur) comme affiché.


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



Cliquez sur
OK.



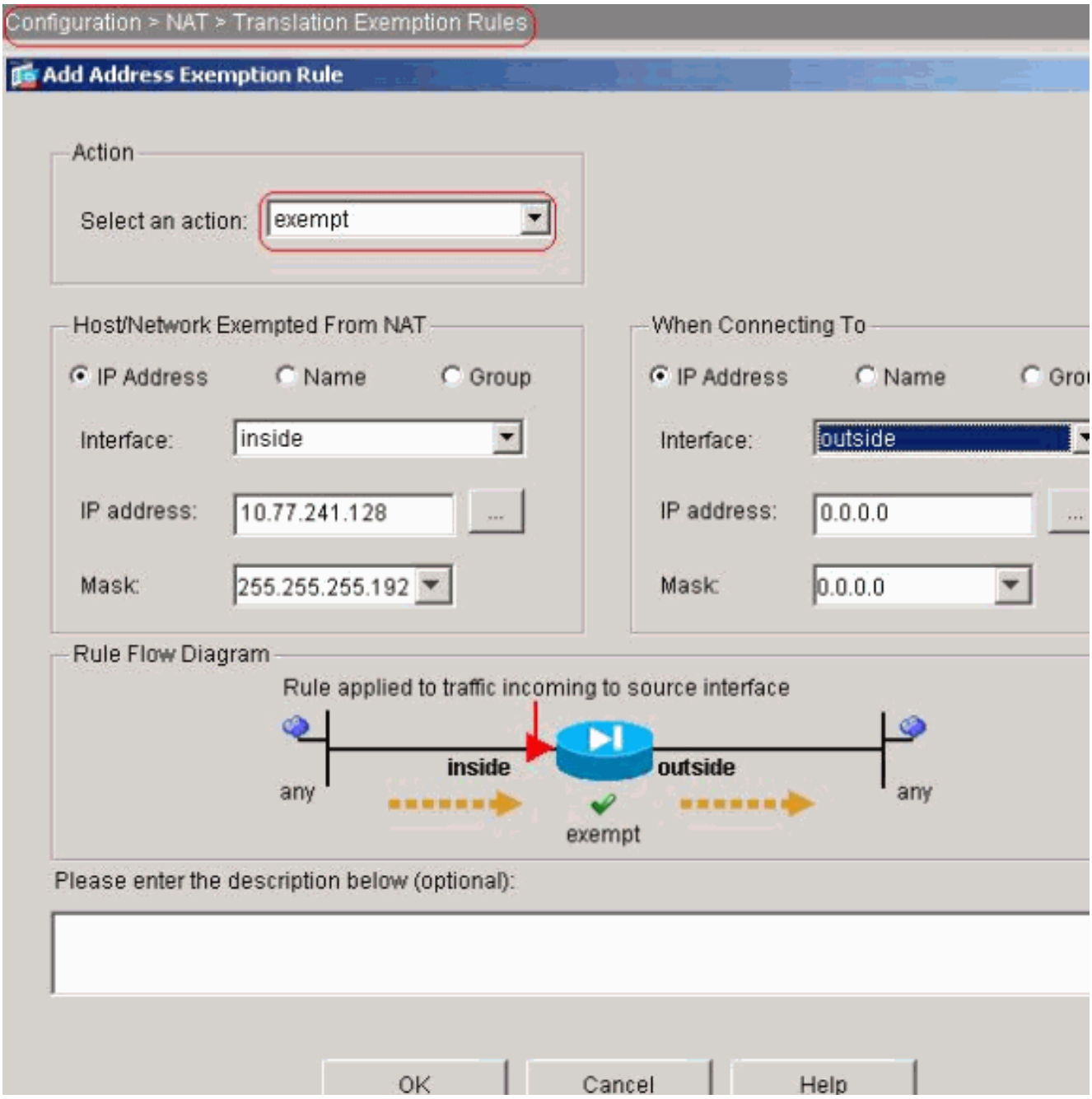
Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU
Ethernet0	outside	Yes	0	192.168.200.1	255.255.255.0	No	1500
Ethernet1	inside	Yes	100	10.77.241.142	255.255.255.192	No	1500

Configuration équivalente CLI comme affiché :

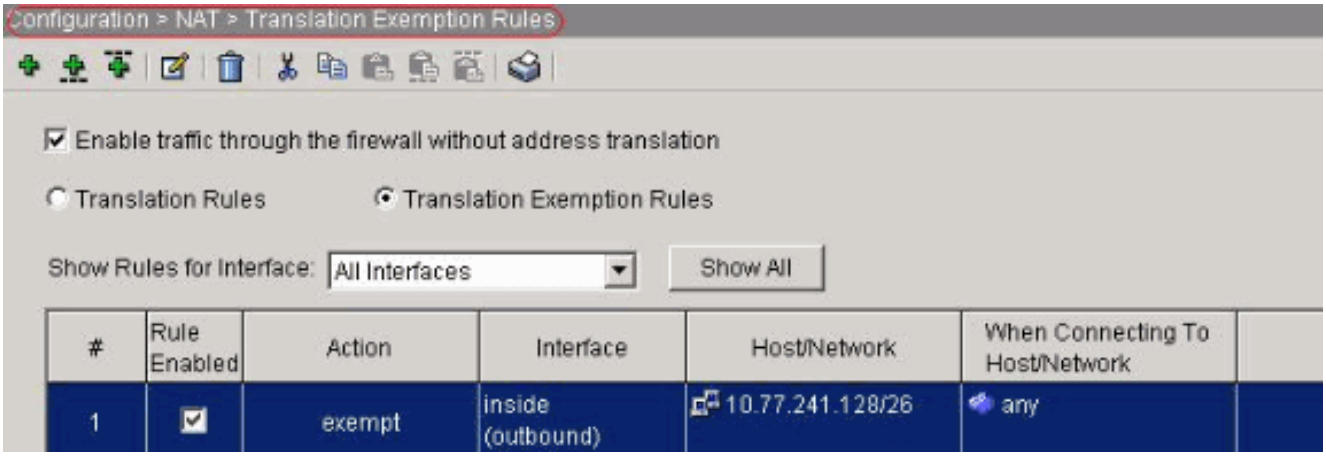
```
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
 nameif inside
```

```
security-level 100
ip address 10.77.241.142 255.255.255.192
```

2. **Configurez 0 NAT**Choisissez le **Configuration > NAT > la Translation Exemption Rules > ajoutent** afin de permettre au trafic du réseau 10.77.241.128/26 pour accéder à l'Internet sans n'importe quelle
traduction.

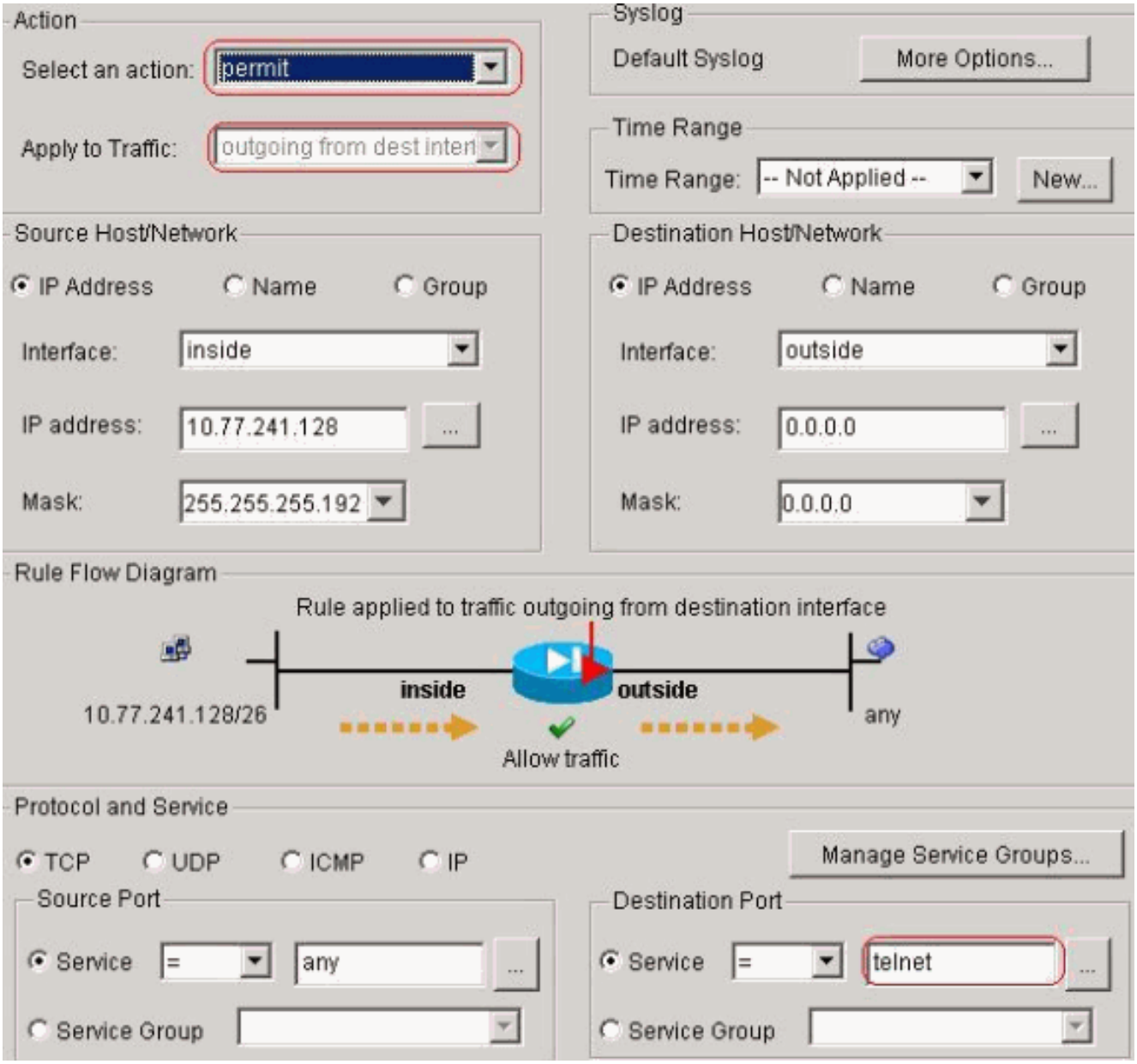


Cliquez sur
OK.



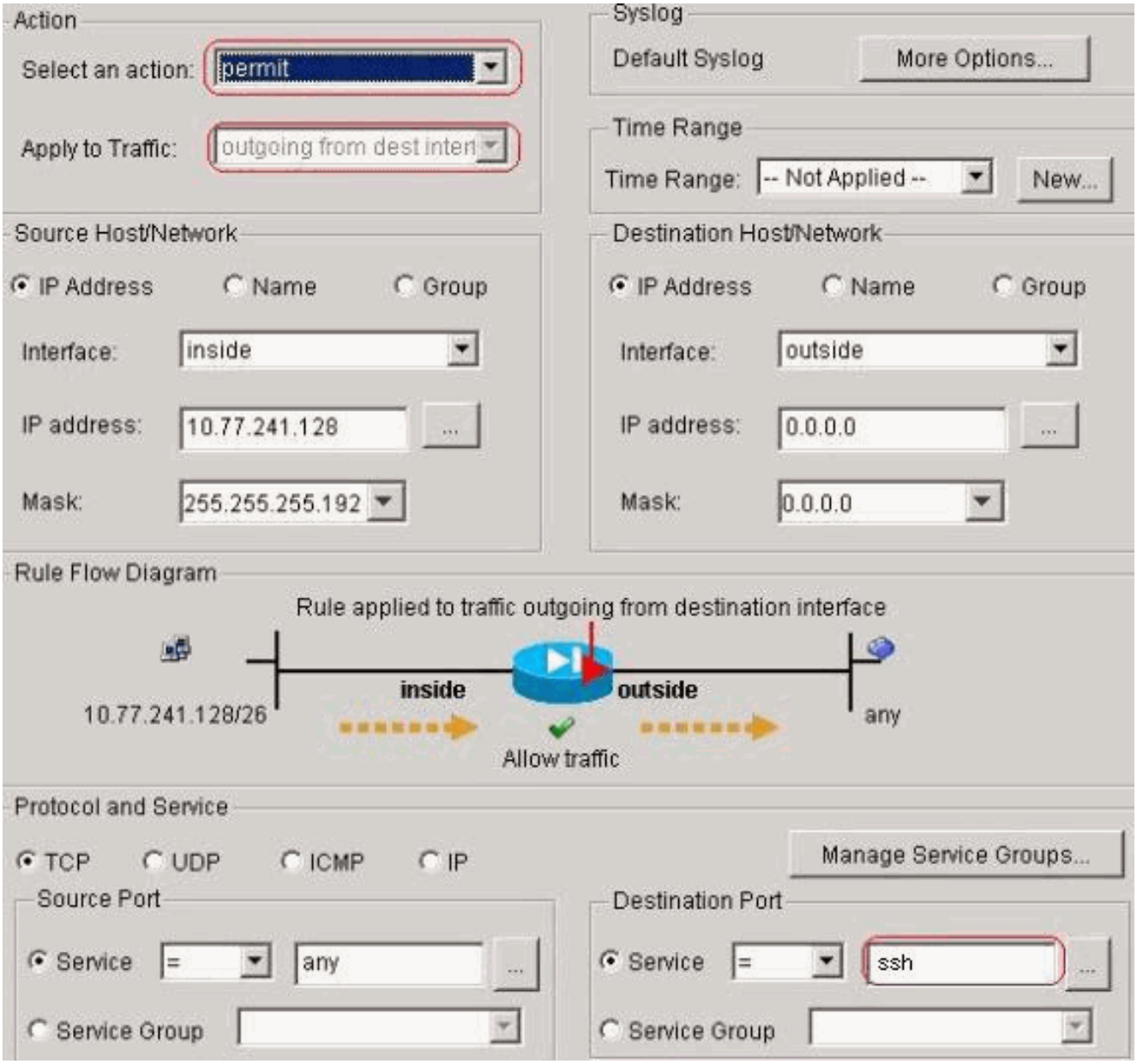
Configuration équivalente CLI comme affiché :`access-list inside_nat0_outbound extended permit ip 10.77.241.128 255.255.255.192 any`
`nat (inside) 0 access-list inside_nat0_outbound`

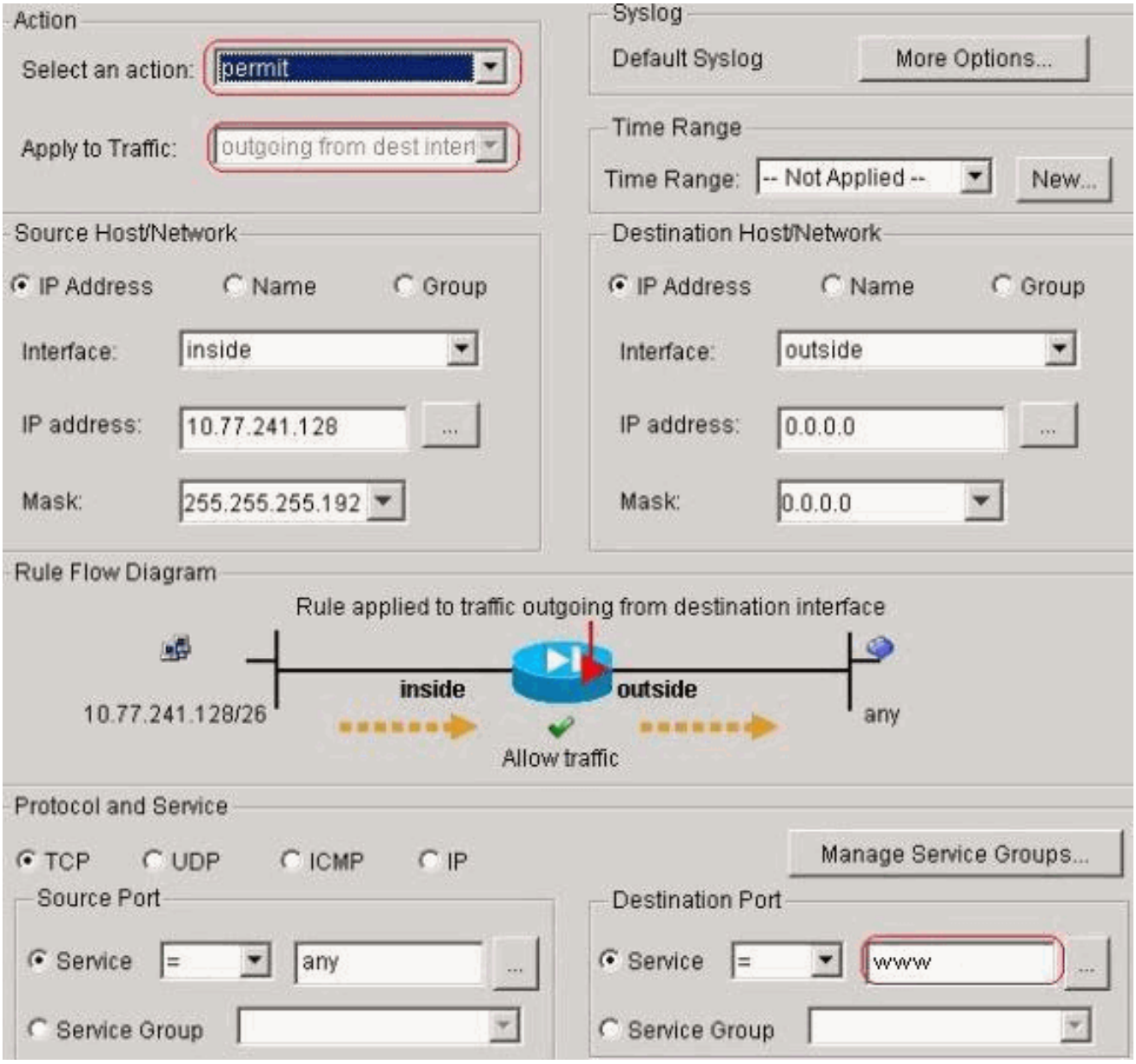
3. **Configurez ACLsDes règles** choisissez de **configuration > de stratégie de sécurité >Access** afin de configurer l'ACLs comme affiché.Cliquez sur Add afin de configurer un ACL 101 qui permet le trafic de telnet provenu du réseau 10.77.241.128/26 à n'importe quel réseau de destination et appliquez-le pour le trafic sortant sur l'interface extérieure.



Cliquez sur **OK**. De même pour le ssh et le trafic http

:

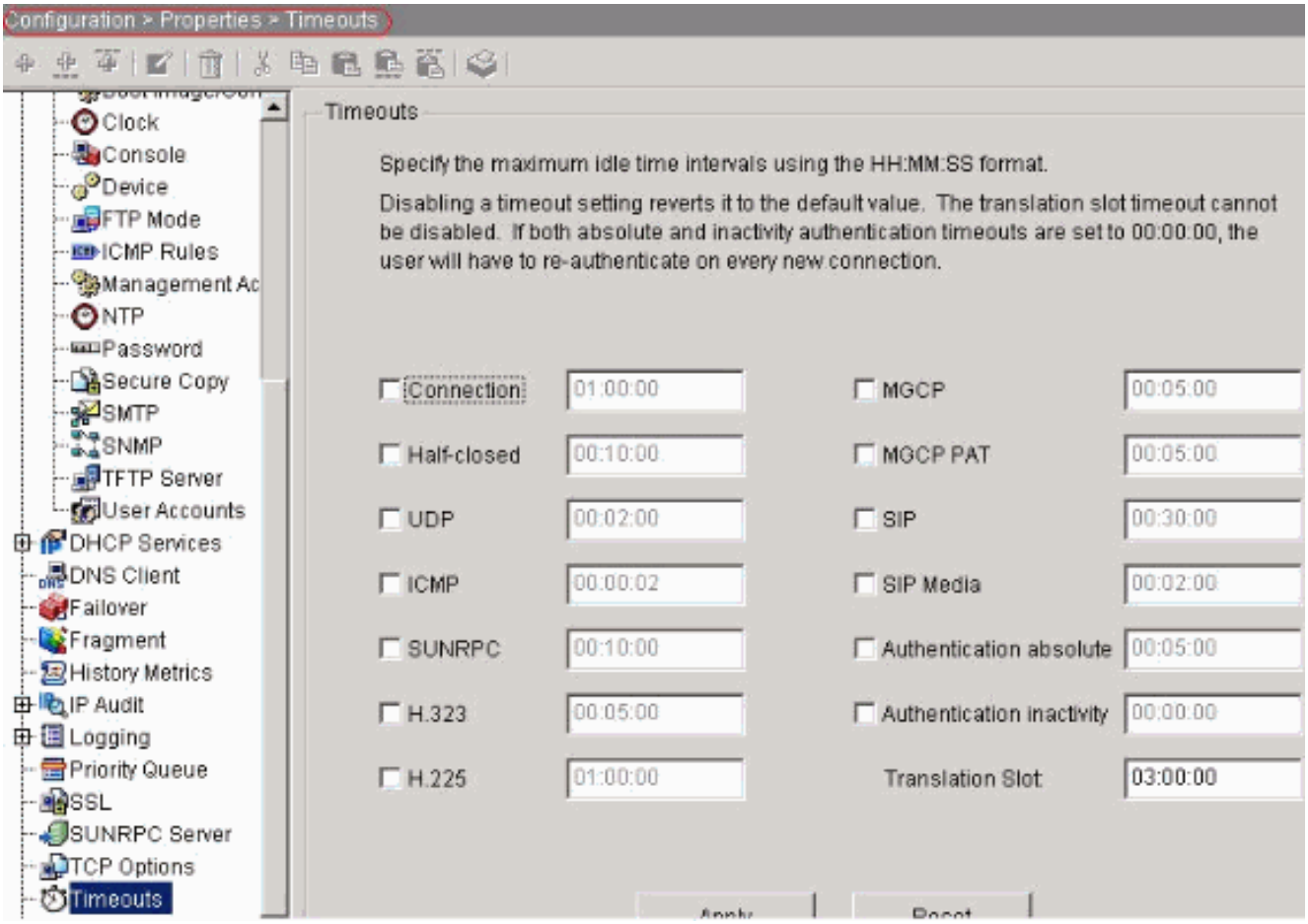

Action
Select an action:
permit
Apply to Traffic:
outgoing from dest inter
Syslog
Default Syslog
More Options...
Time Range
Time Range:
-- Not Applied --
New...
Source Host/Network
IP Address
Name
Group
Interface:
inside
IP address:
10.77.241.128
Mask:
255.255.255.192
Destination Host/Network
IP Address
Name
Group
Interface:
outside
IP address:
0.0.0.0
Mask:
0.0.0.0
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
Manage Service Groups...
Source Port
Service
=
any
Service Group
Destination Port
Service
=
ssh
Service Group



Configuration équivalente CLI comme affiché :

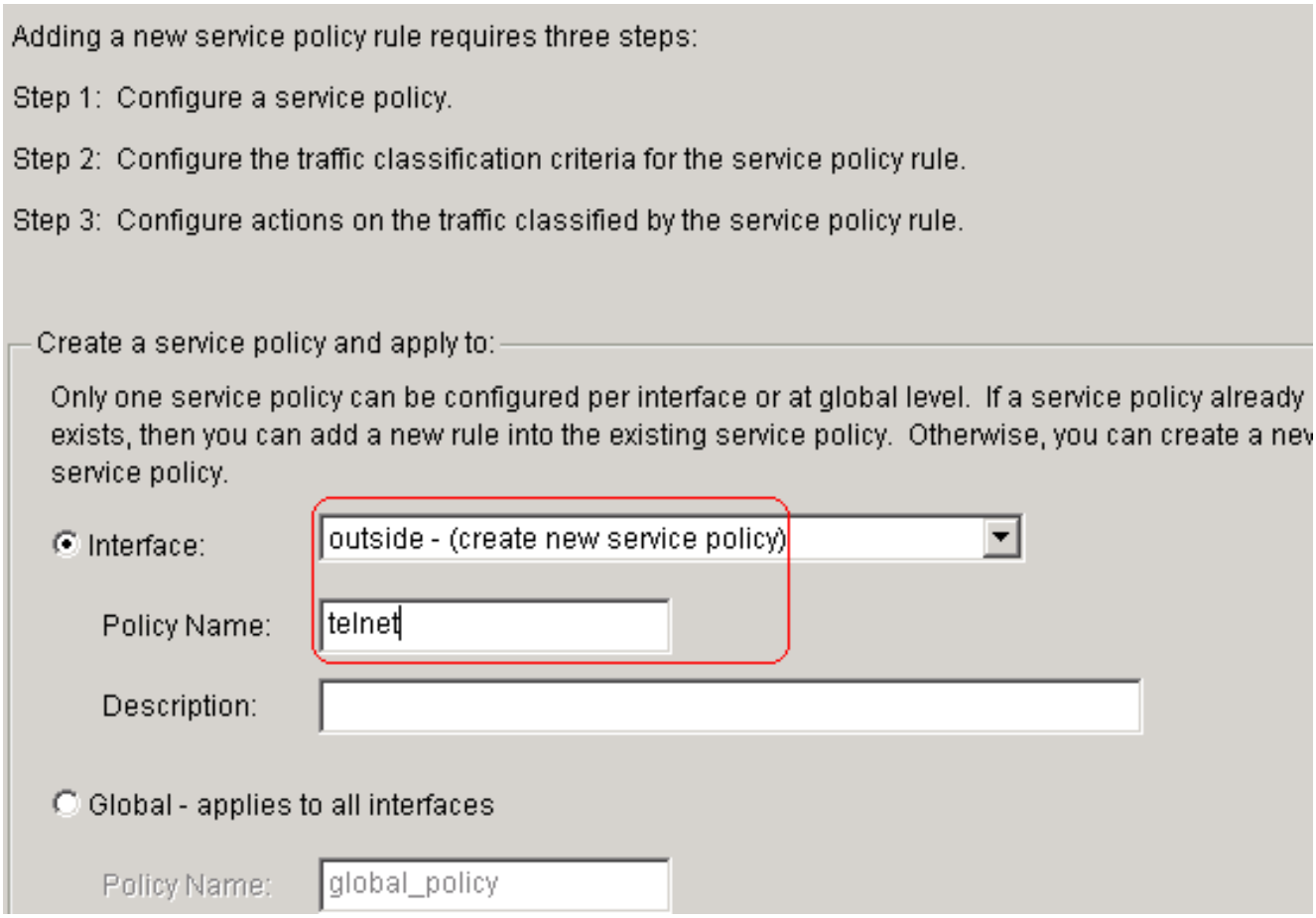
```
access-list 101 extended permit tcp
10.77.241.128 255.255.255.192 any eq telnet
access-list 101 extended permit tcp 10.77.241.128 255.255.255.192 any eq ssh
access-list 101 extended permit tcp 10.77.241.128 255.255.255.192 any eq www
access-group 101 out interface outside
```

4. **Configurez les délais d'attente**Choisissez la **configuration > le Properties > les délais d'attente** afin de configurer les divers délais d'attente. Dans ce scénario, gardez la valeur par défaut pour tous les délais
d'attente.

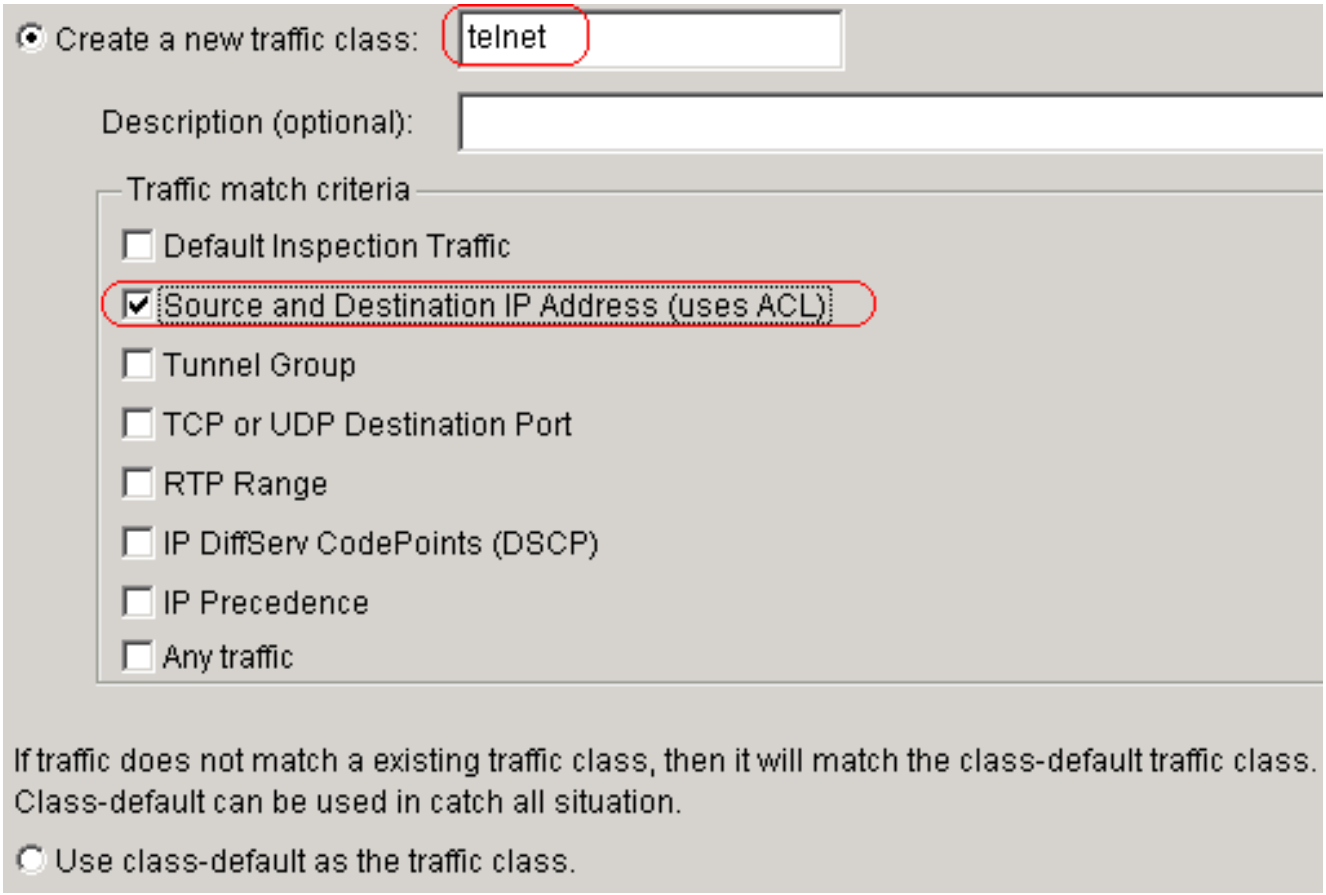


Configuration équivalente CLI comme affiché :`timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02`

5. Configurez les **règles de stratégie de service**.Choisissez les **règles de stratégie de configuration > de stratégie de sécurité > de service > ajoutent** afin de configurer le class map, carte de stratégie pour l'établissement le délai d'attente de connexion TCP en tant que 10 minutes, et appliquent la stratégie de service sur l'interface extérieure comme affichée.Choisissez la case d'option d'**interface** afin de choisir l'**extérieur - (créez la nouvelle stratégie de service)**, qui doit être créé, et assigner le **telnet** comme nom de stratégie.

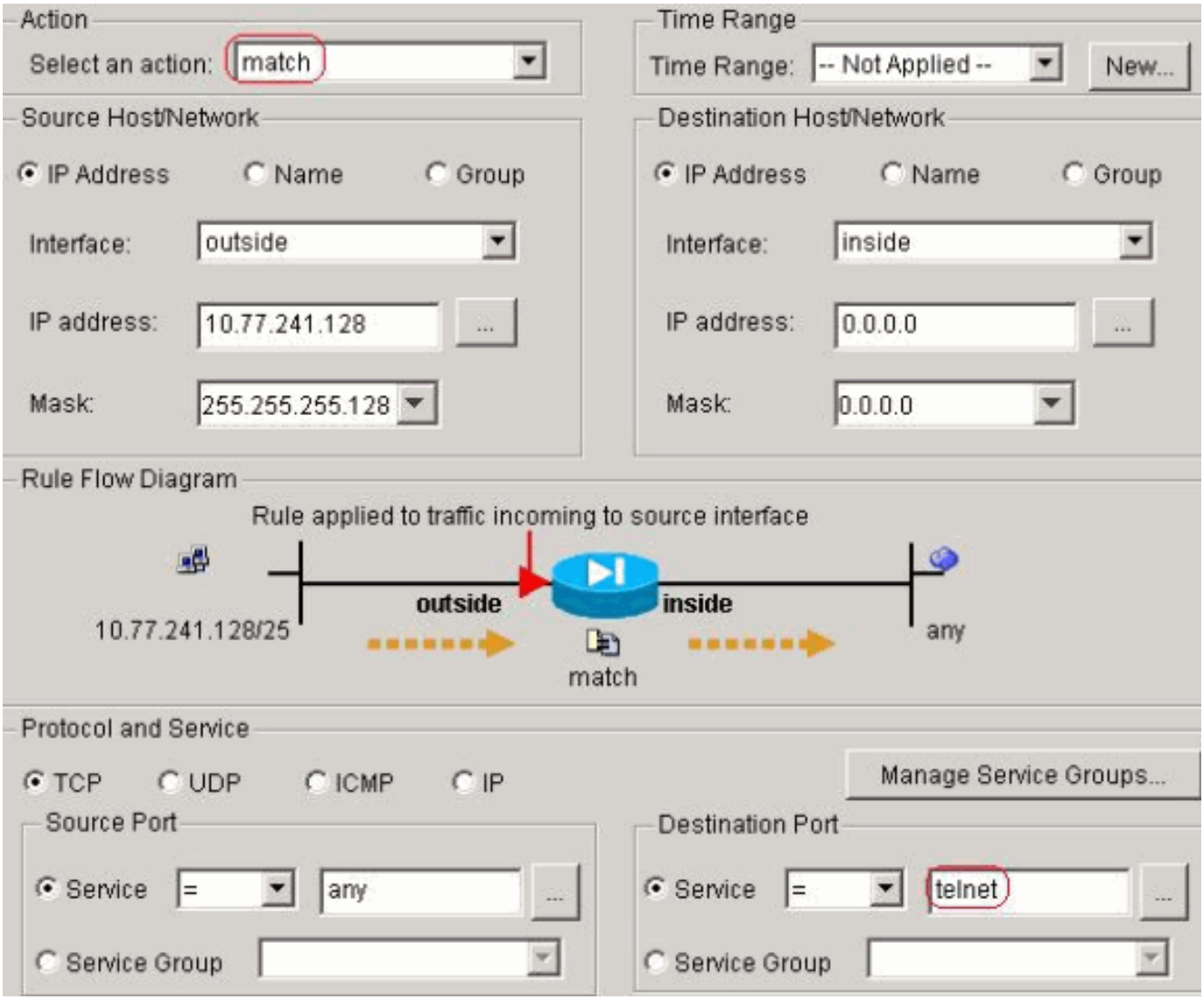


Cliquez sur **Next** (Suivant).Créez un **telnet de** nom de class map et choisissez la case de **source et d'adresse IP de destination (ACL d'utilisations)** dans le critère de correspondance du
trafic.

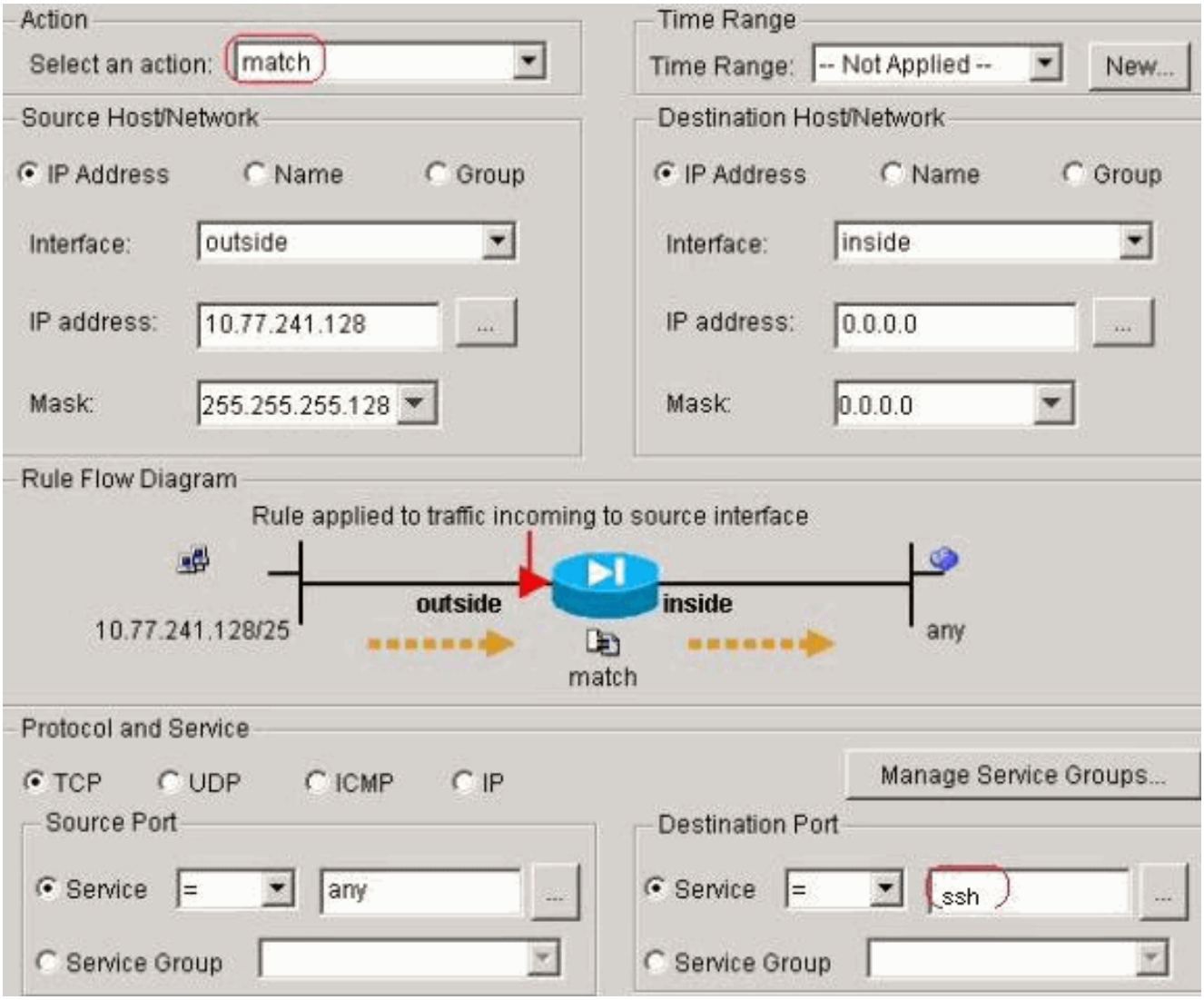


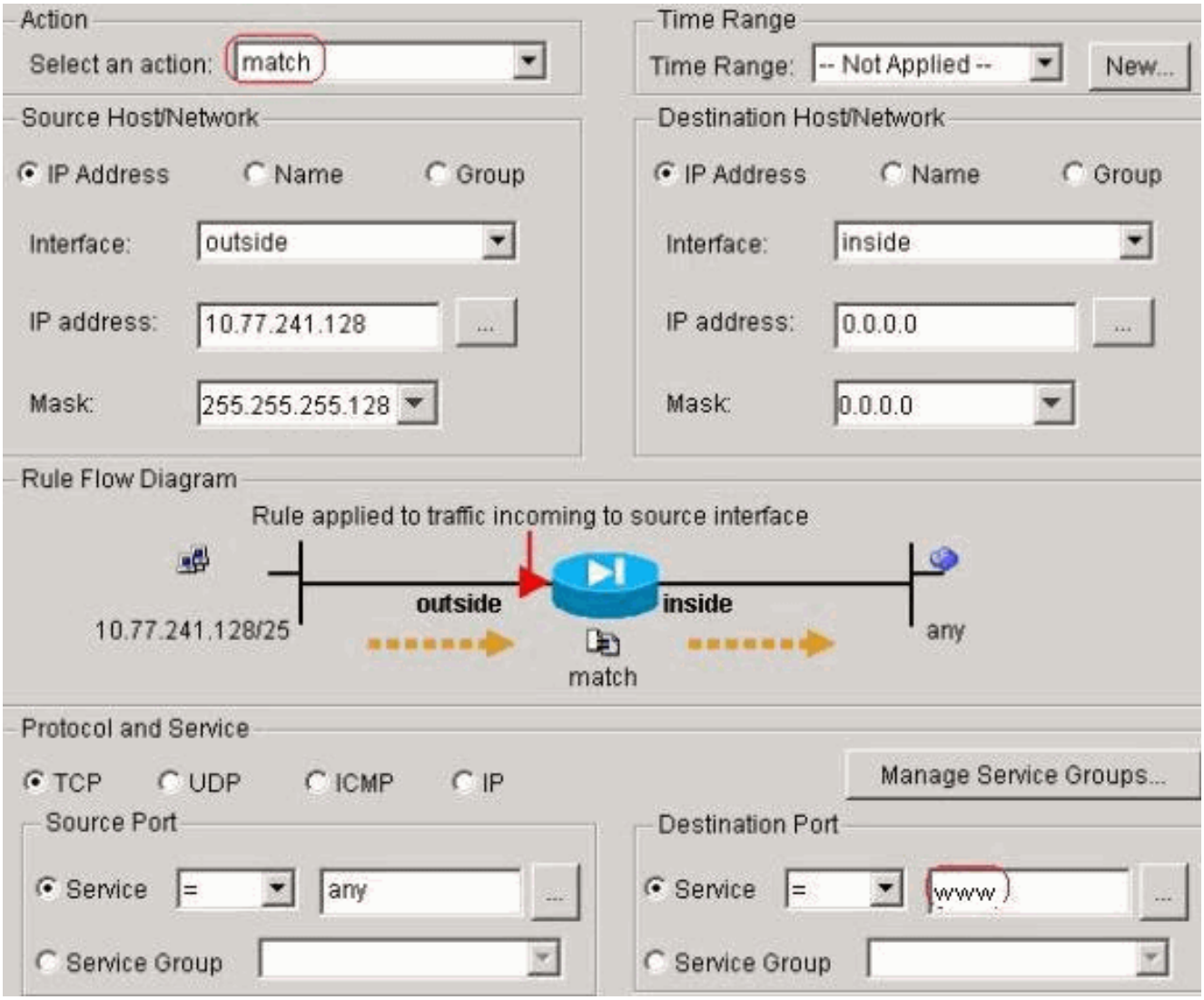
Cliquez sur **Next** (Suivant).Créez un ACL afin d'apparier le trafic de telnet provenu du réseau

10.77.241.128/26 à n'importe quel réseau de destination et l'appliquer pour classer le telnet.

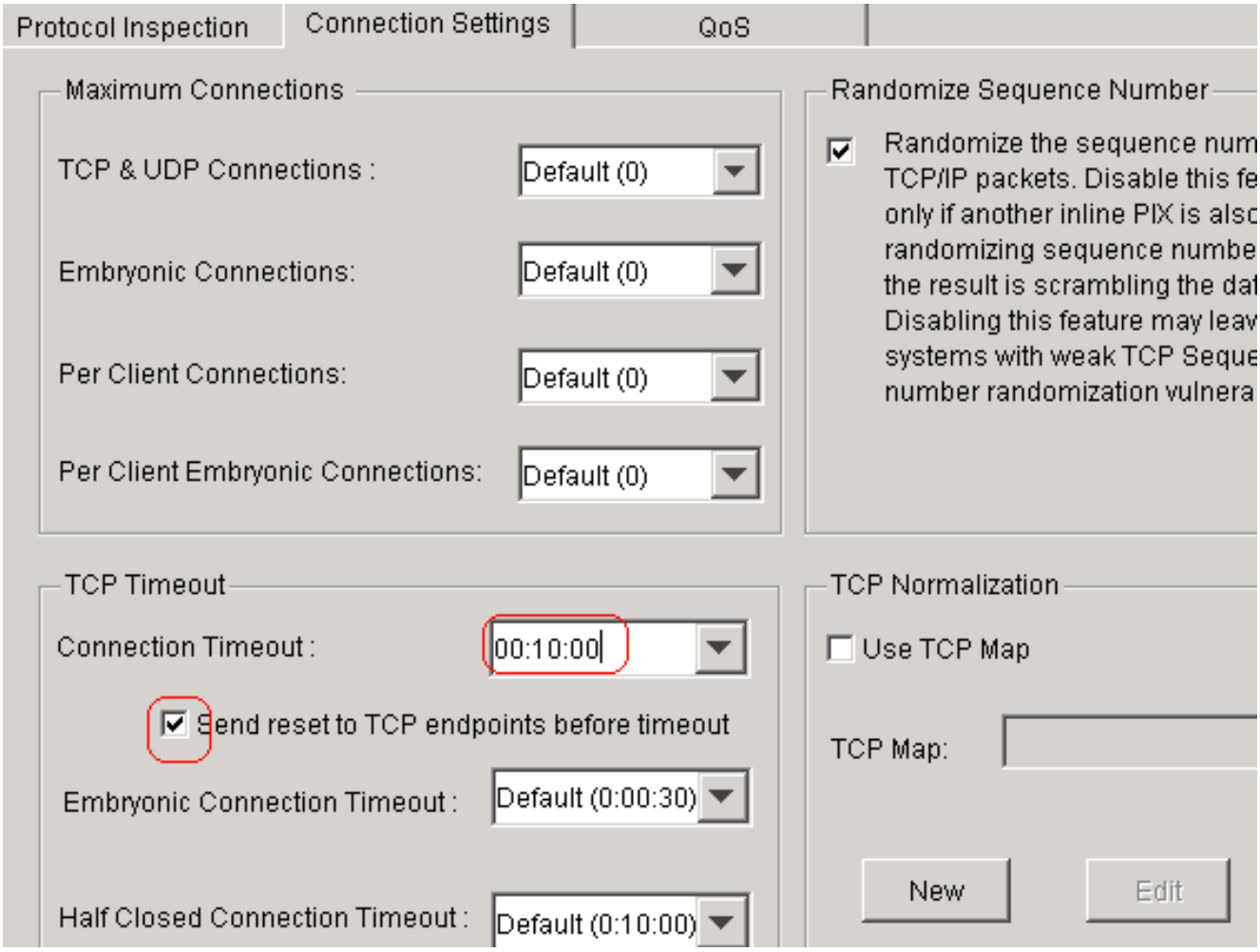


Cliquez sur **Next** (Suivant). De même pour le ssh et le trafic http
:

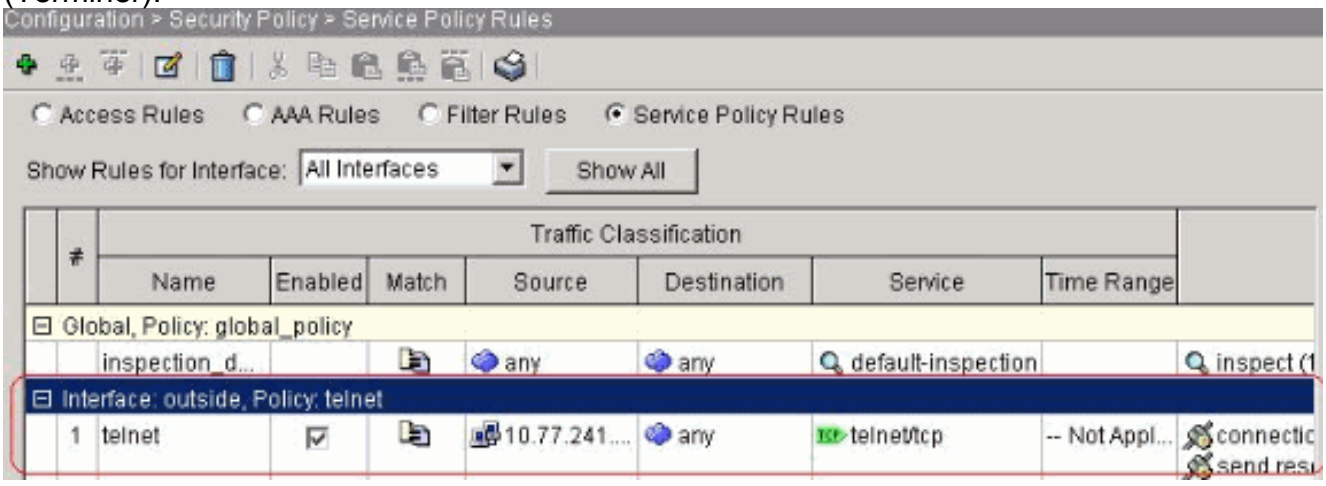

Action
Select an action: match
Time Range
Time Range: -- Not Applied --
New...
Source Host/Network
IP Address
Name
Group
Interface: outside
IP address: 10.77.241.128
Mask: 255.255.255.128
Destination Host/Network
IP Address
Name
Group
Interface: inside
IP address: 0.0.0.0
Mask: 0.0.0.0
Rule Flow Diagram
Rule applied to traffic incoming to source interface
10.77.241.128/25
outside
inside
any
match
Protocol and Service
TCP
UDP
ICMP
IP
Manage Service Groups...
Source Port
Service = any
Service Group
Destination Port
Service = ssh
Service Group



Choisissez les **paramètres de connexion** afin d'installer le délai d'attente de connexion TCP en tant que 10 minutes, et choisissez également l'**envoi remis à l'état initial aux points finaux de TCP avant** case de **délai d'attente**.



Cliquez sur **Finish** (Terminer).



Configuration équivalente CLI comme affiché :

```
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'attente d'Ebryonic

Une connexion embryonnaire est la connexion qui est demi s'ouvrent ou, par exemple, la connexion en trois étapes n'a pas été terminée pour elle. Il est défini comme délai d'attente de synchronisation sur l'ASA ; par défaut le délai d'attente de synchronisation sur l'ASA est de 30 secondes. C'est la manière de configurer le délai d'attente embryonnaire :

```
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
```

Vérifiez

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 l'**interface de show service-policy en dehors de la** commande 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 d'écoulement de show service-policy afin de vérifier que le trafic particulier apparie les configurations de politique de service.

Cette sortie de commande affiche 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
```

Dépannez

Si vous constatez que le délai d'attente de connexion ne fonctionne pas avec le cadre de stratégie modulaire (MPF), alors vérifiez la connexion d'initiation de TCP. La question peut être une inversion de la source et l'adresse IP de destination ou une adresse IP misconfigured dans la liste d'accès ne s'assortit pas dans le MPF pour placer la nouvelle valeur du dépassement de durée ou pour changer le délai d'attente par défaut pour l'application. Créez une entrée de liste d'accès (source et destination) selon la demande de connexion afin de placer 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
- Notes de mise à jour en dispositifs de sécurité de Cisco PIX
- 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)
- Support et documentation techniques - Cisco Systems

Cisco relatif prennent en charge des discussions de la Communauté

Référez-vous au Conventions relatives aux conseils techniques Cisco pour les informations sur des conventions utilisées dans ce document.

Mis à jour : Oct. 16, 2008
ID de document : 68332