PIX/ASA 7.x e later/FWSM: Ajuste o timeout de conexão SSH/Telnet/HTTP usando o exemplo da configuração MPF

ID do Documento: 68332

Atualizado em: outubro 16, 2008

Produtos Relacionados

- Cisco Adaptive Security Device Manager
- Firewall da próxima geração do 5500-X Series de Cisco ASA
- **Cisco PIX 500 Series Security Appliances**

Índice

Introdução

Estes original fornecem uma configuração de exemplo para PIX 7.1(1) e mais atrasado de um intervalo que seja específico a um aplicativo particular tal como SSH/Telnet/HTTP, ao contrário de um que se aplica a todos os aplicativos. Este exemplo de configuração usa a estrutura de política modular nova introduzida em PIX 7.0. Refira a utilização da estrutura de política modular para mais informação.

Nesta configuração de exemplo, o PIX Firewall é configurado para permitir a estação de trabalho (10.77.241.129) a Telnet/SSH/HTTP ao servidor remoto (10.1.1.1) atrás do roteador. Um intervalo de conexão separada ao tráfego Telnet/SSH/HTTP é configurado igualmente. Todo tráfego TCP restante continua a ter o valor de timeout da conexão normal associado com a **conexão 1:00:00 do intervalo**.

Refira AASA 8.3 e mais atrasado: Ajuste o timeout de conexão SSH/Telnet/HTTP usando o exemplo da configuração MPF para obter mais informações sobre da configuração idêntica usando o ASDM com a ferramenta de segurança adaptável de Cisco (ASA) com versão 8.3 e mais recente.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada na versão de software da ferramenta de segurança de Cisco PIX/ASA 7.1(1) com Security Device Manager adaptável (ASDM) 5.1.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

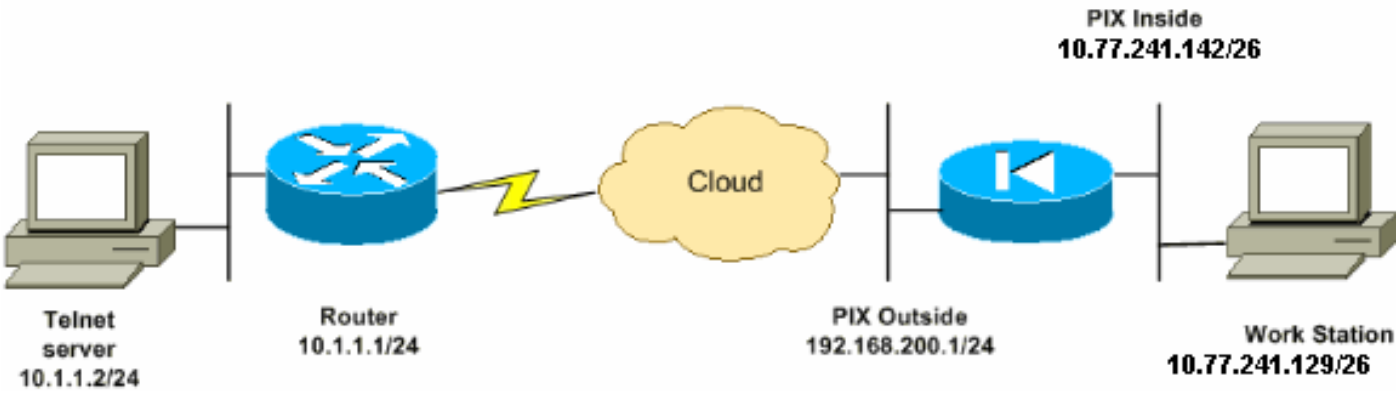
Configurar

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:



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

Configuração

Este documento utiliza esta configuração:

Nota: Este o CLI e as configurações ASDM são aplicáveis ao módulo firewall service (o 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
```

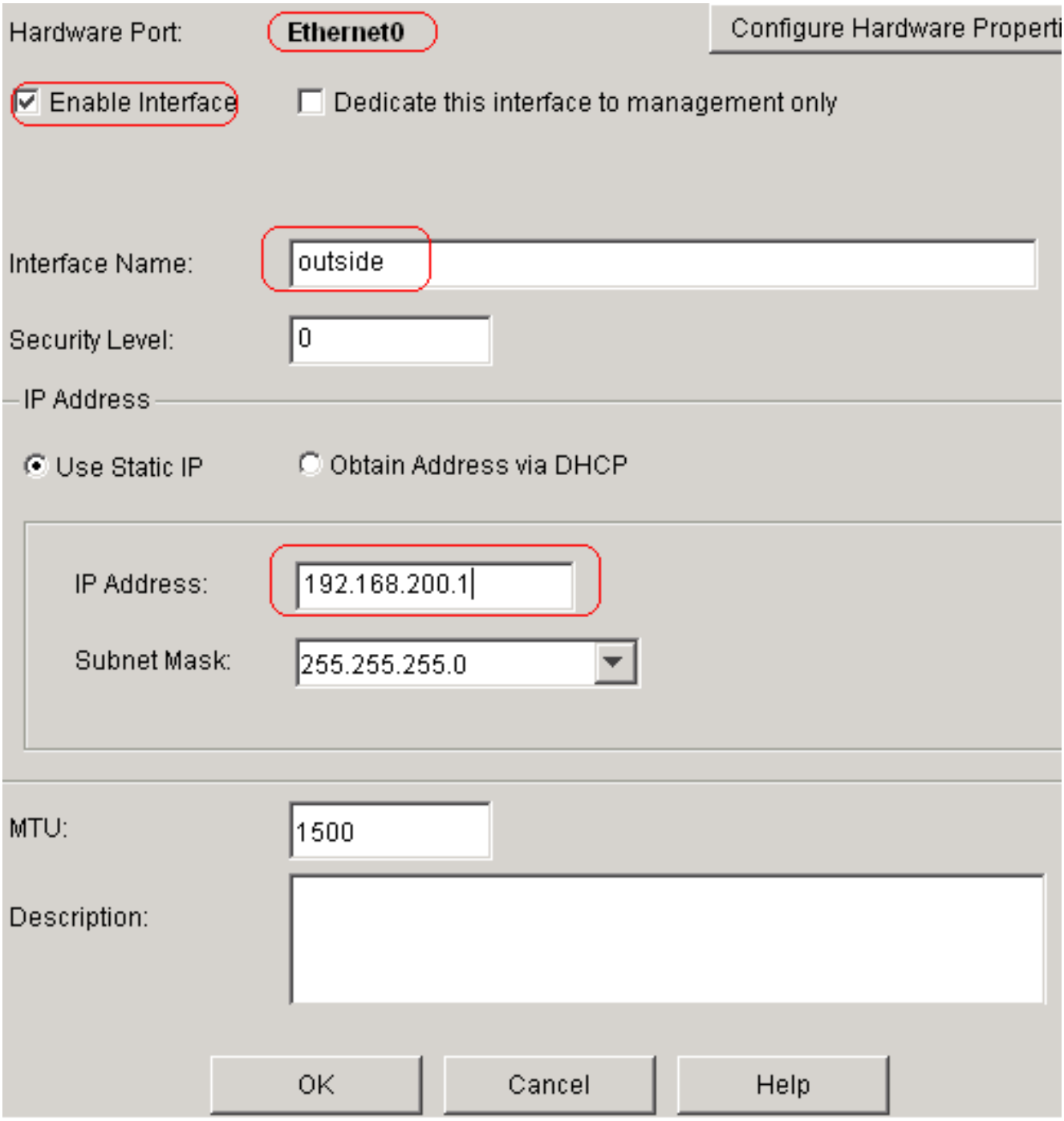
```
!--- Use the pre-defined class map telnet in the policy
map.


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
```

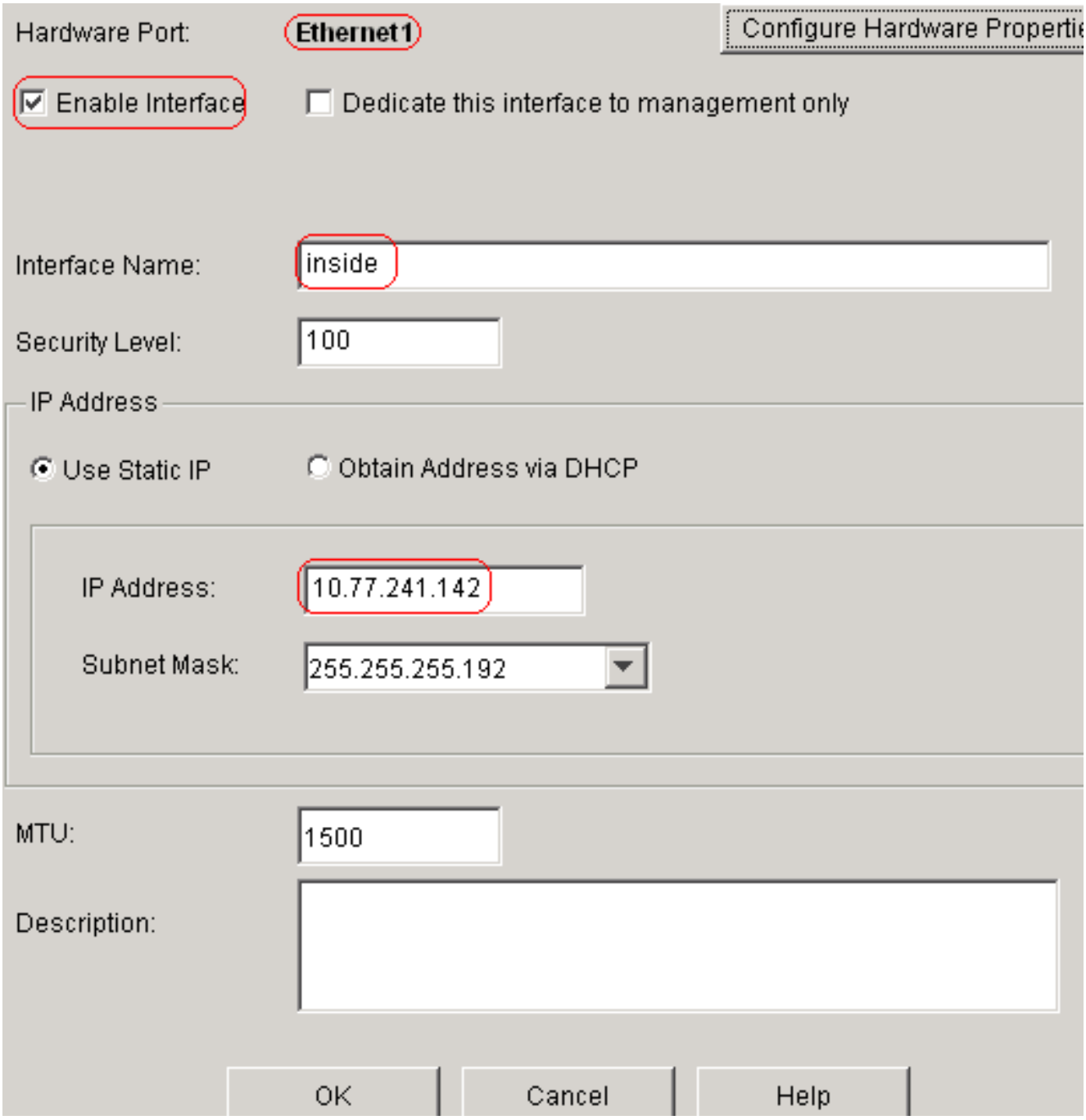
Configuração ASDM:

Termine estas etapas a fim estabelecer o intervalo de conexão de TCP para o tráfego do telnet baseado na lista de acesso que usa o ASDM como mostrado.

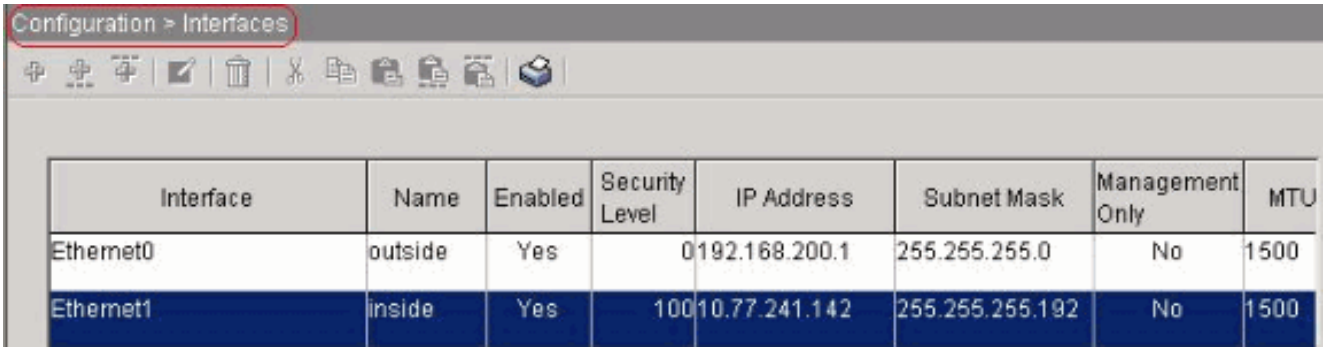
Nota: Refira permitir que o acesso HTTPS para o ASDM para configurações básicas a fim alcançar o PIX/ASA com o ASDM.

1. **Configurar relações**Escolha o **> Add do configuração > interfaces** a fim configurar o ethernet0 das relações (fora) e Ethernet1 (para dentro) como mostrado.


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



Clique em
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

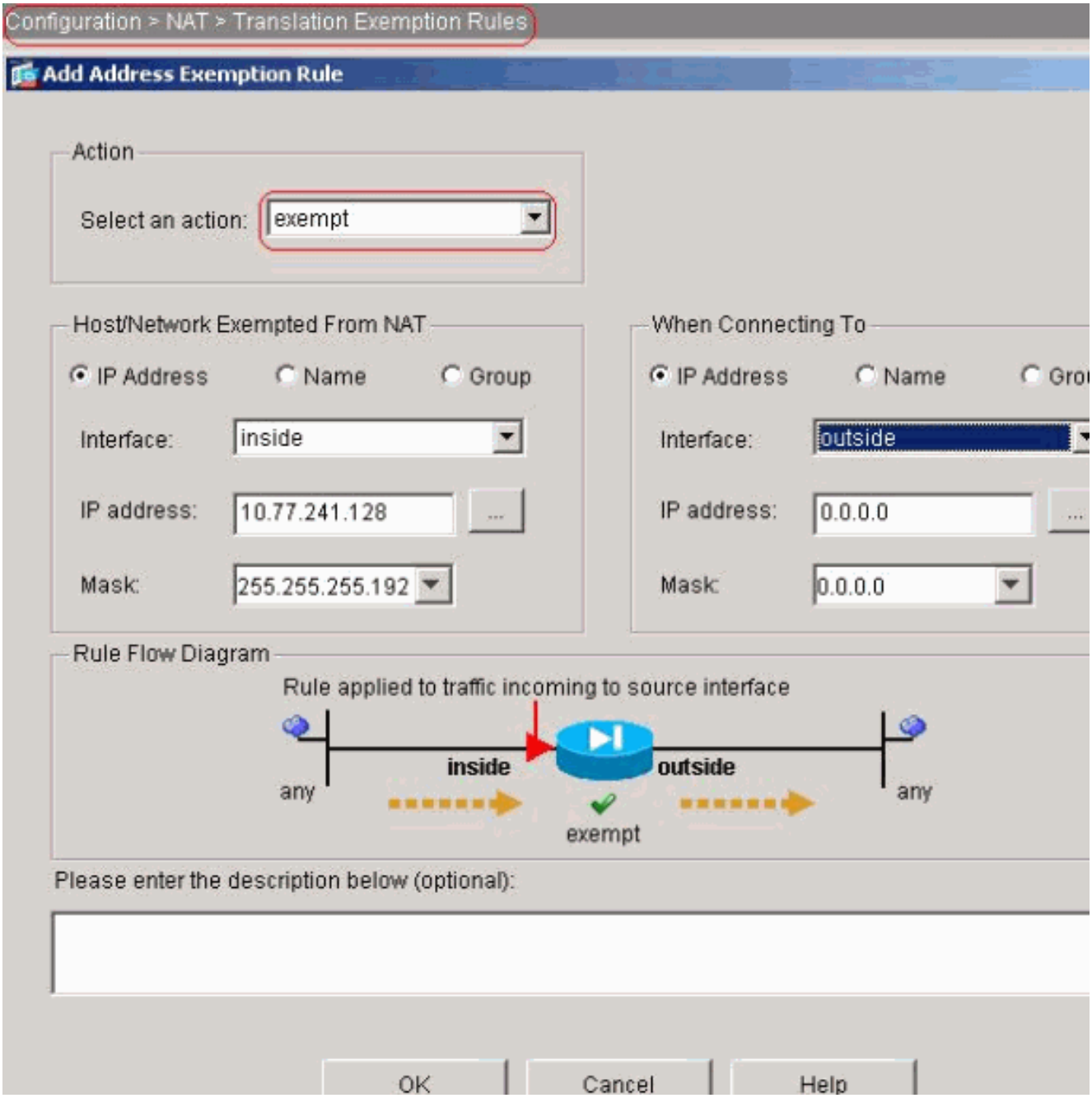
Configuração de CLI equivalente como mostrado:

```
PIX Version - 7.1(1)
!
hostname PIX
domain-name Cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
```

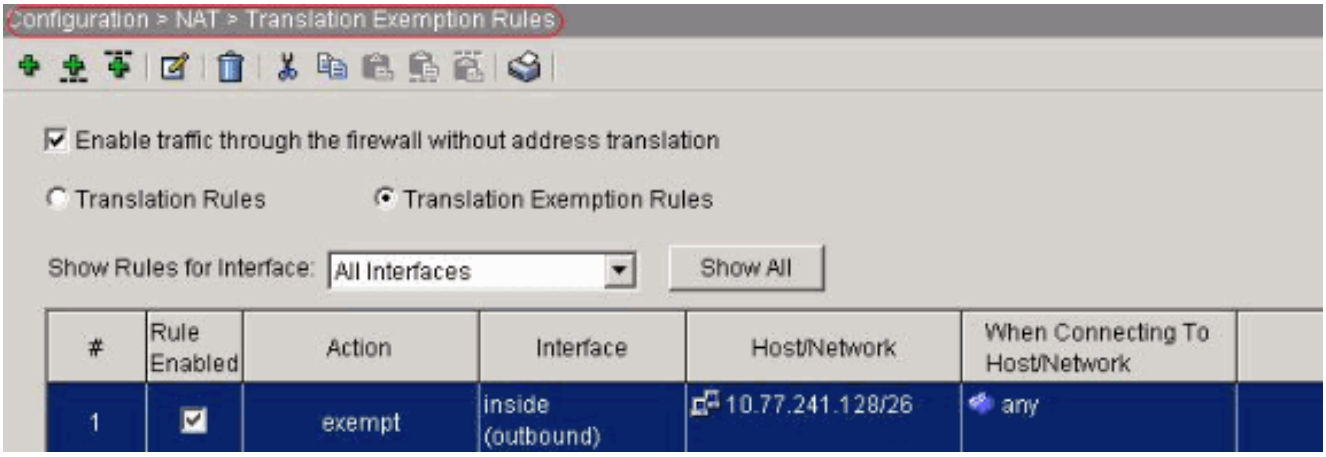
```
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!


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
```

2. Configurar NAT 0Escolha o **> Add das regras da configuração > da isenção NAT > de tradução** a fim permitir que o tráfego da rede 10.77.241.128/26 alcance o Internet sem nenhuma
tradução.



Clique em
OK.



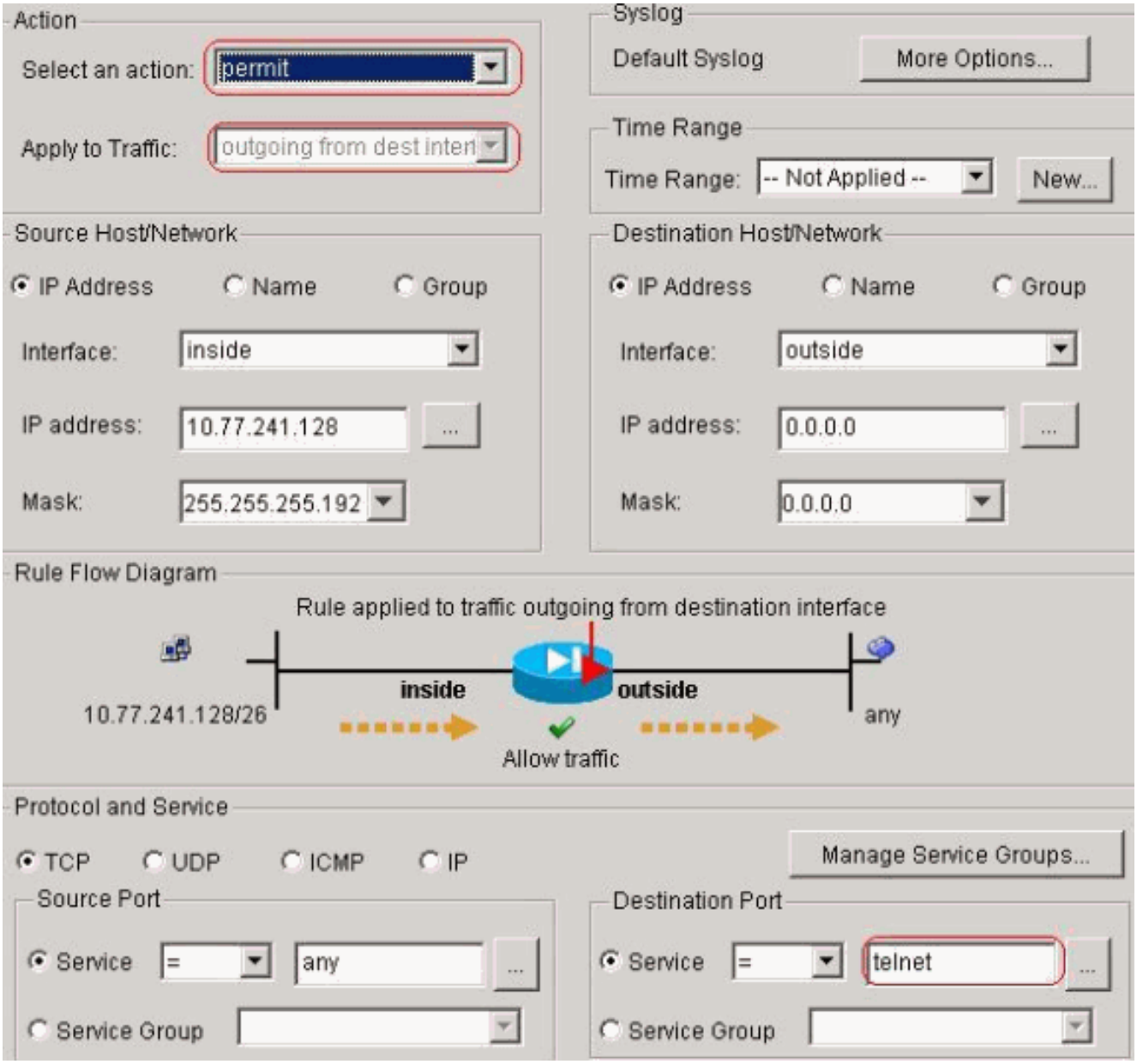
Configuração de CLI equivalente como mostrado:

```
PIX Version - 7.1(1)
!
hostname PIX
domain-name Cisco.com
```

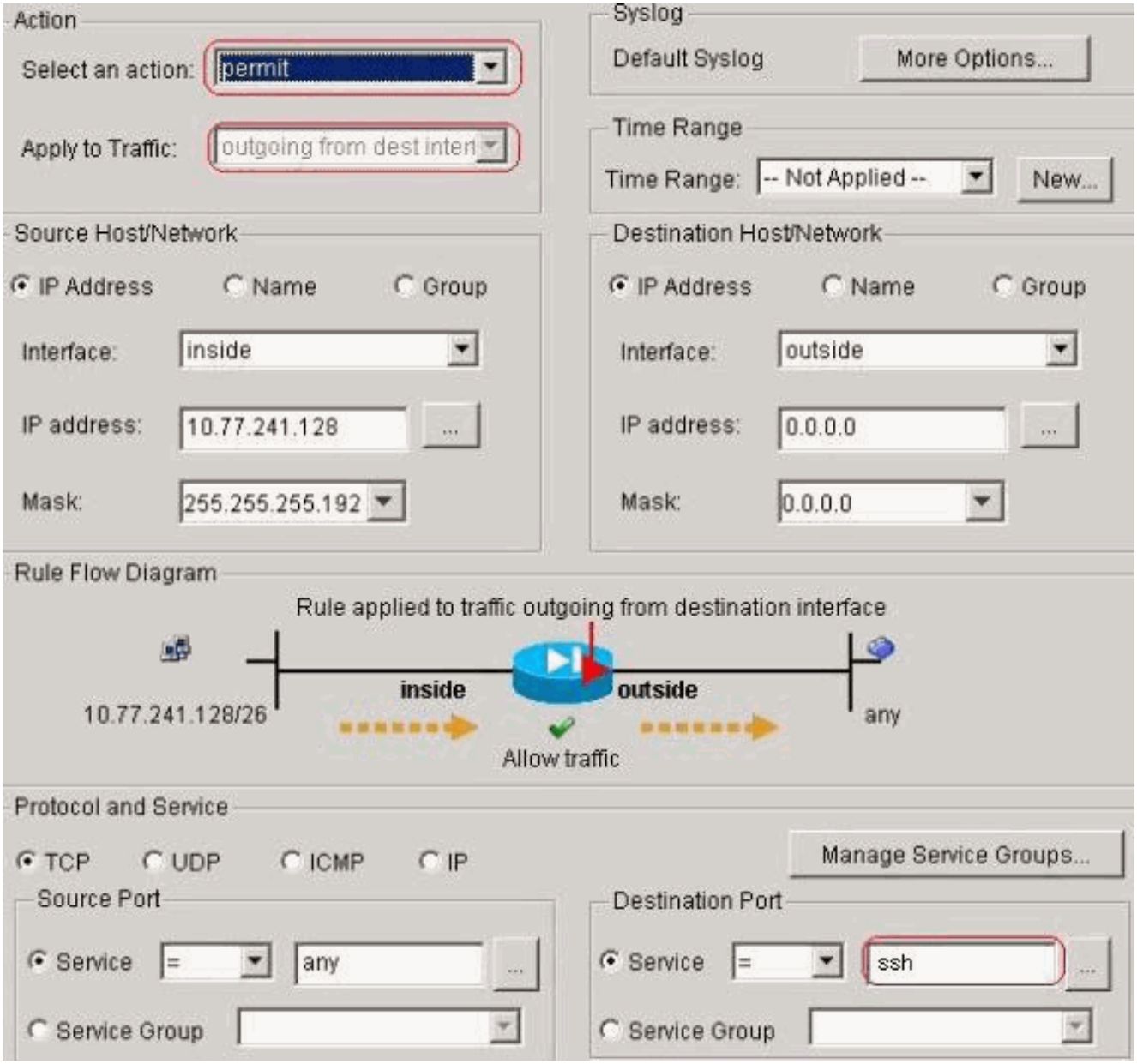
```
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!


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
!
!
```

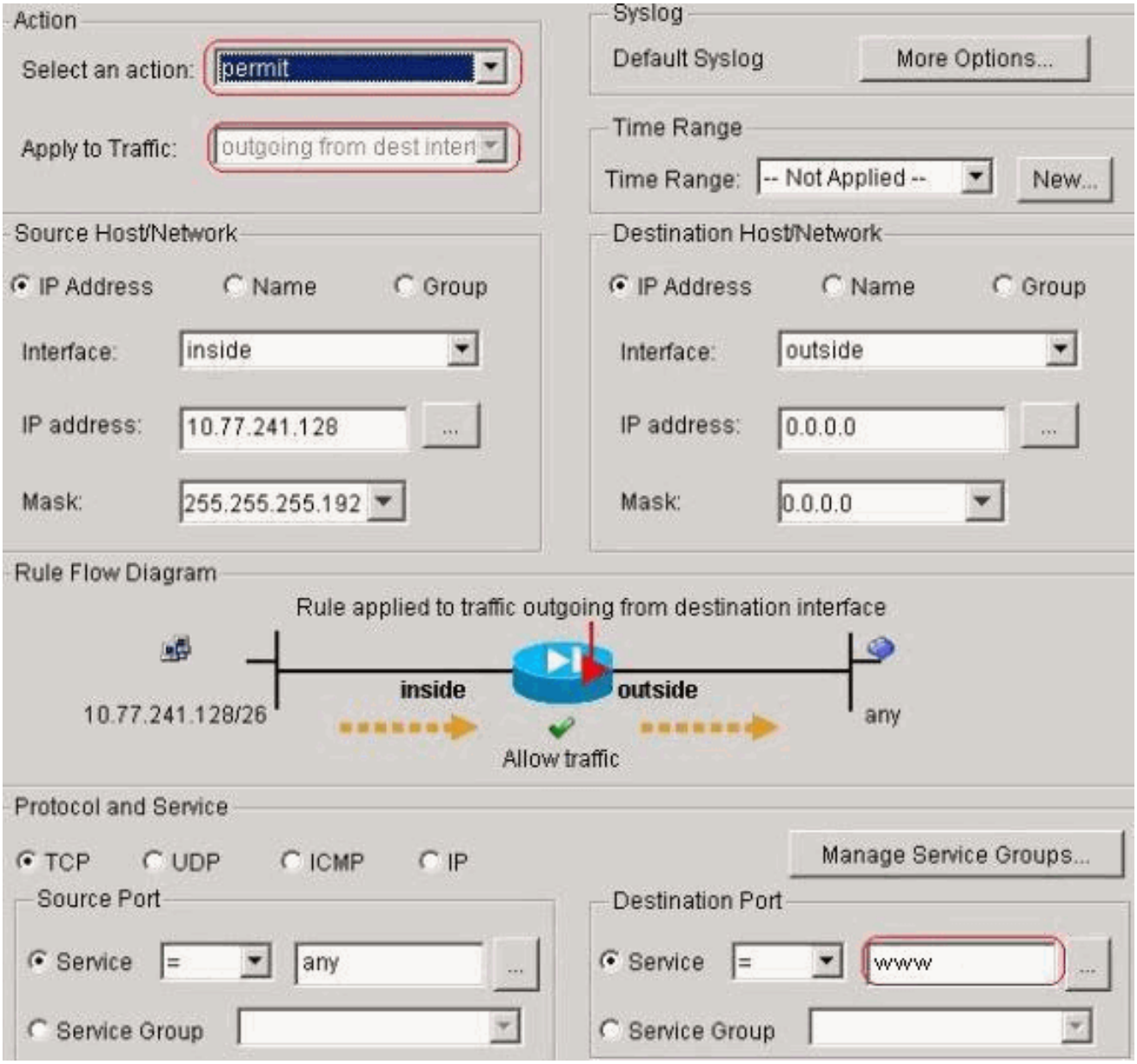
```
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp

!--- 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
```

3. Configurar ACLEscolha regras dos >Access da política do > segurança da configuração a fim configurar como mostrado os ACL.O clique adiciona a fim configurar um ACL 101 que permite o tráfego do telnet originado da rede 10.77.241.128/26 a toda a rede de destino e aplica-a para o tráfego de saída na interface
externa.



Clique em **OK**. Similarmente para o ssh e o tráfego 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



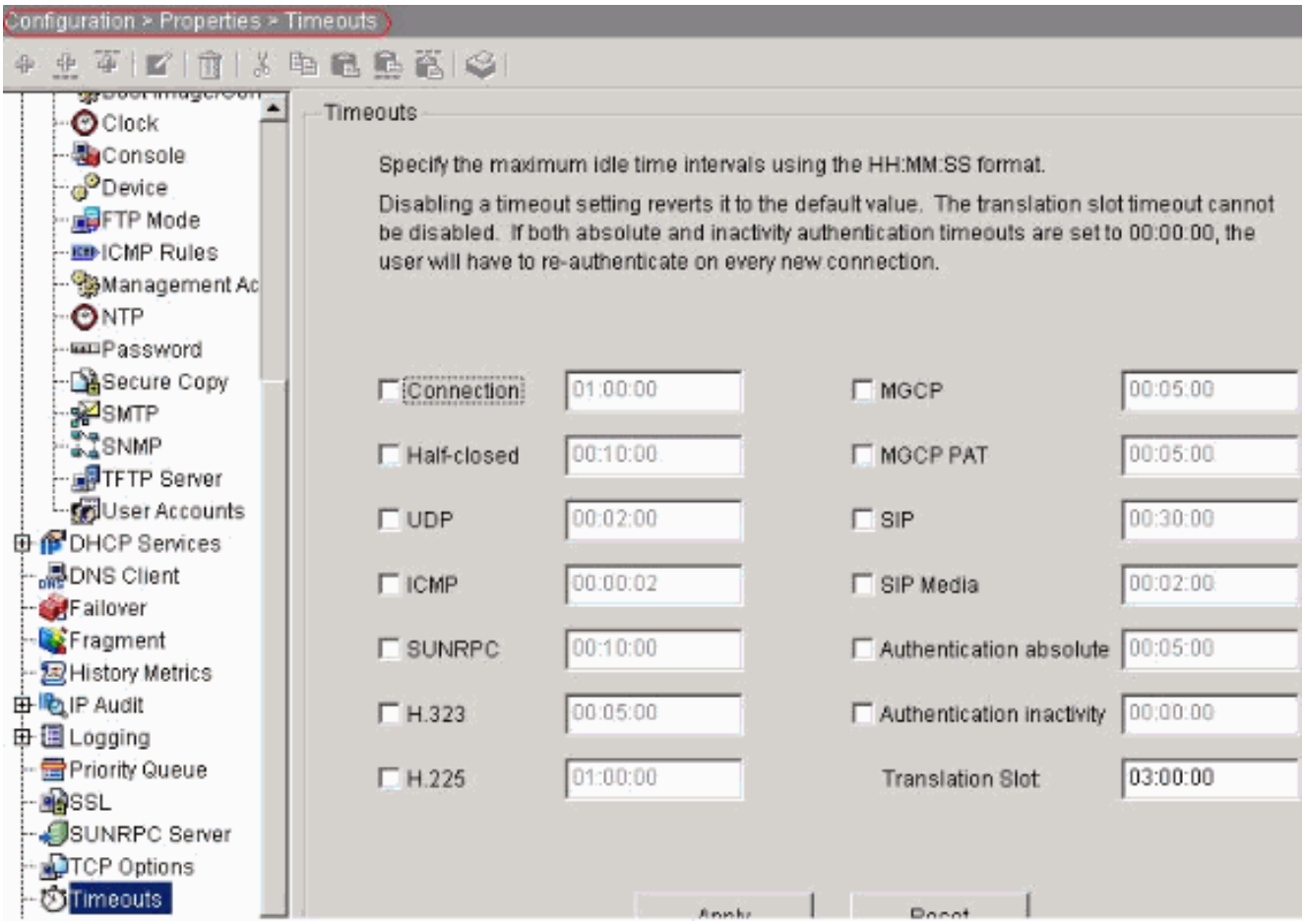
Configuração de CLI equivalente como mostrado:

```
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
```

4. **Configurar intervalos**Escolha a **configuração > as propriedades > os intervalos** a fim configurar os vários intervalos. Nesta encenação, mantenha o valor padrão para todos os intervalos.



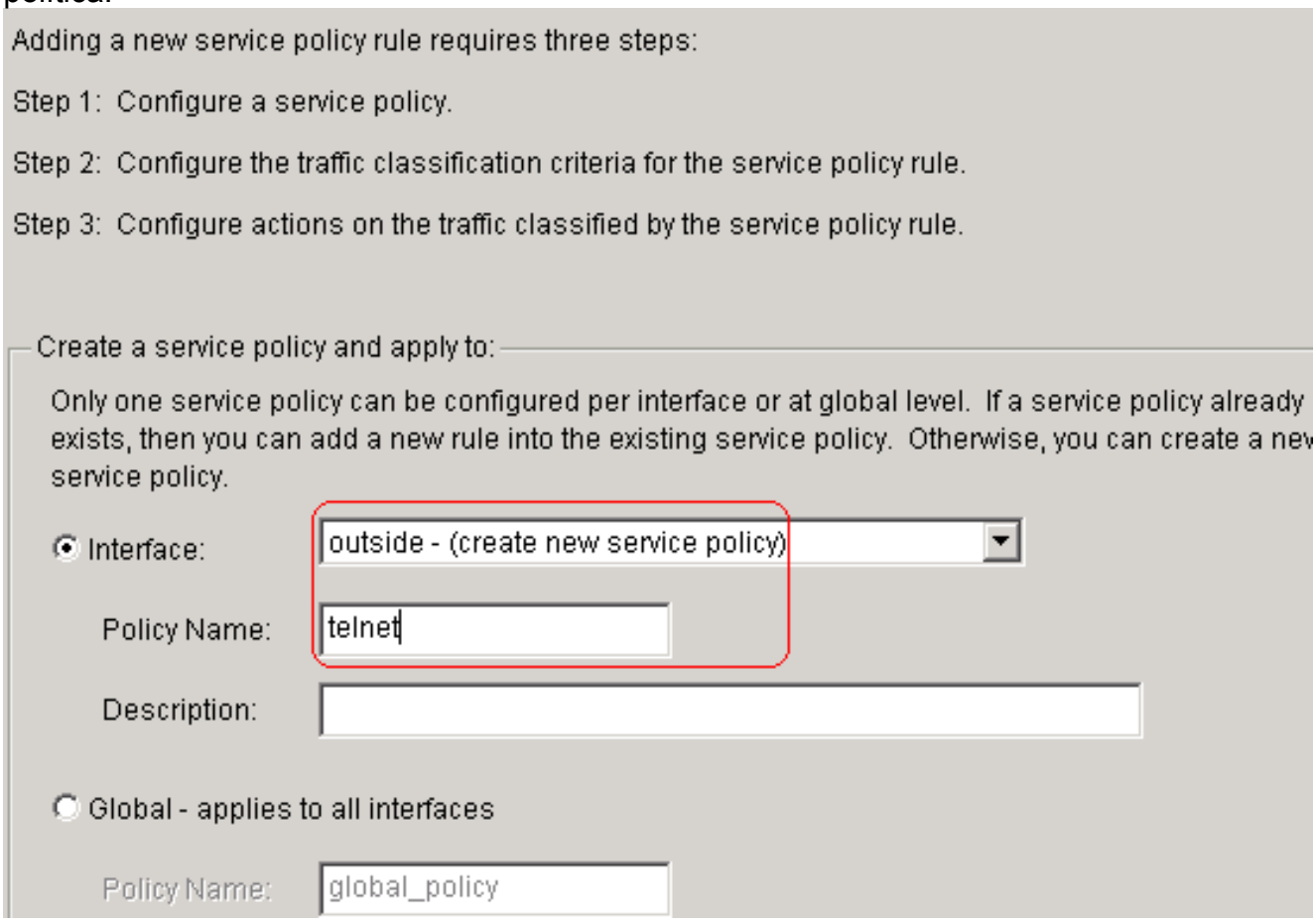
Configuração de CLI equivalente como mostrado:

```
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
```

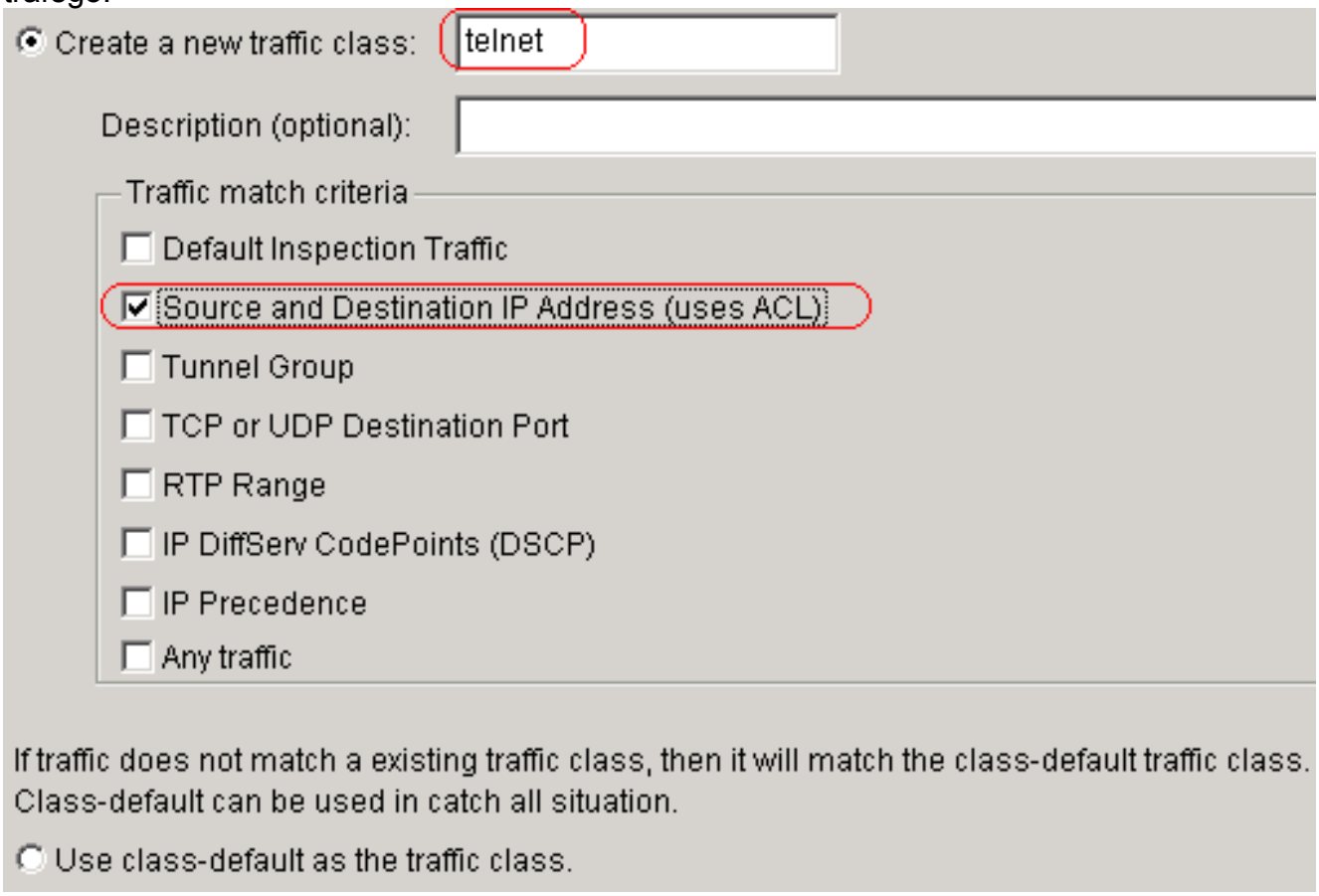
```
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!


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
```

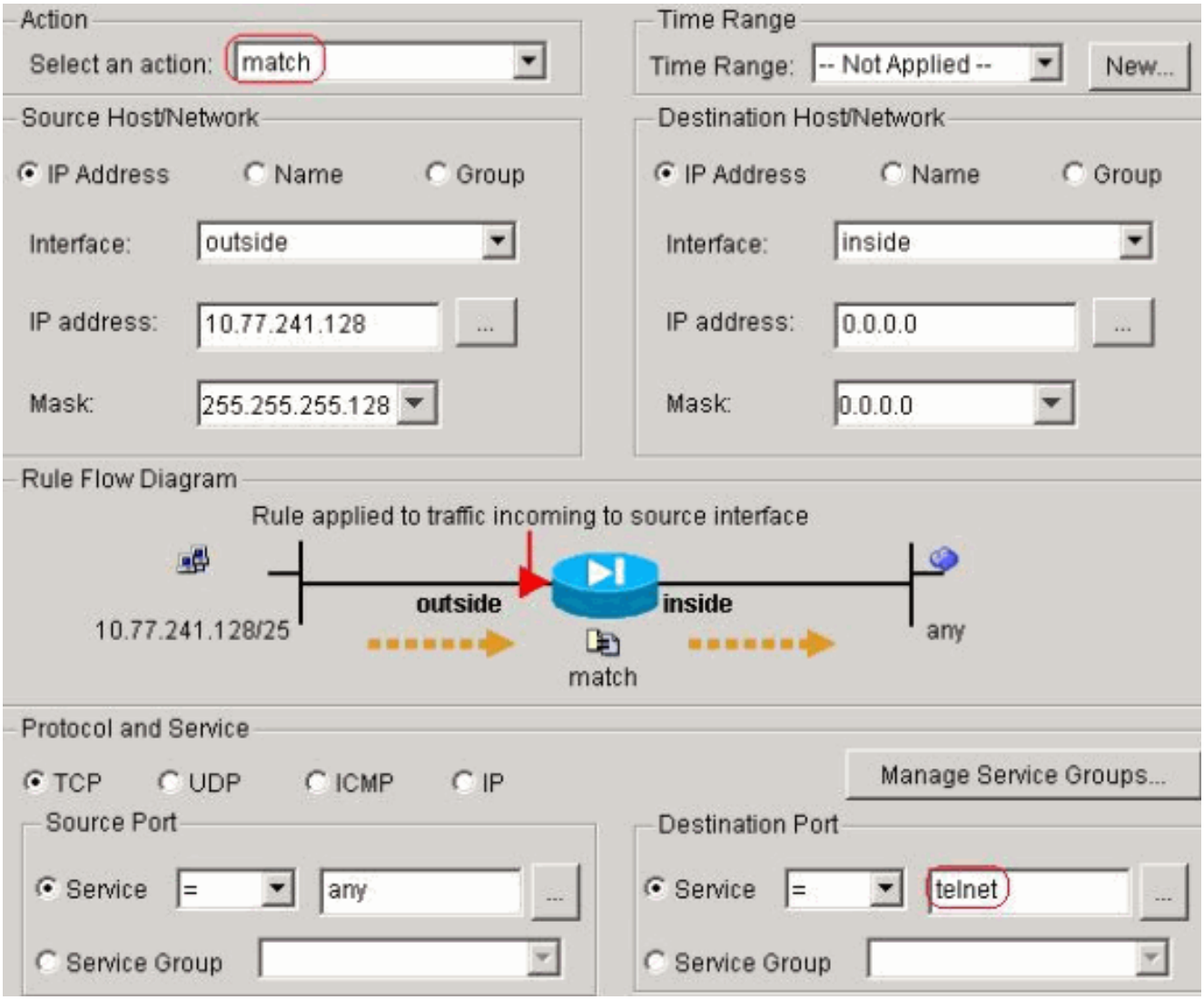
5. Configurar **regras da política de serviços**.Escolha o **> Add das regras da política > da política de serviços do > segurança da configuração** a fim configurar o mapa da classe, mapa de política para o estabelecimento o intervalo de conexão de TCP como os minutos 10, e aplique a política de serviços na interface externa como mostrada.Escolha o botão de rádio da **relação** a fim escolher a **parte externa - (crie a política de serviços nova)**, que deve ser criada, e atribuir o **telnet** como o nome da política.



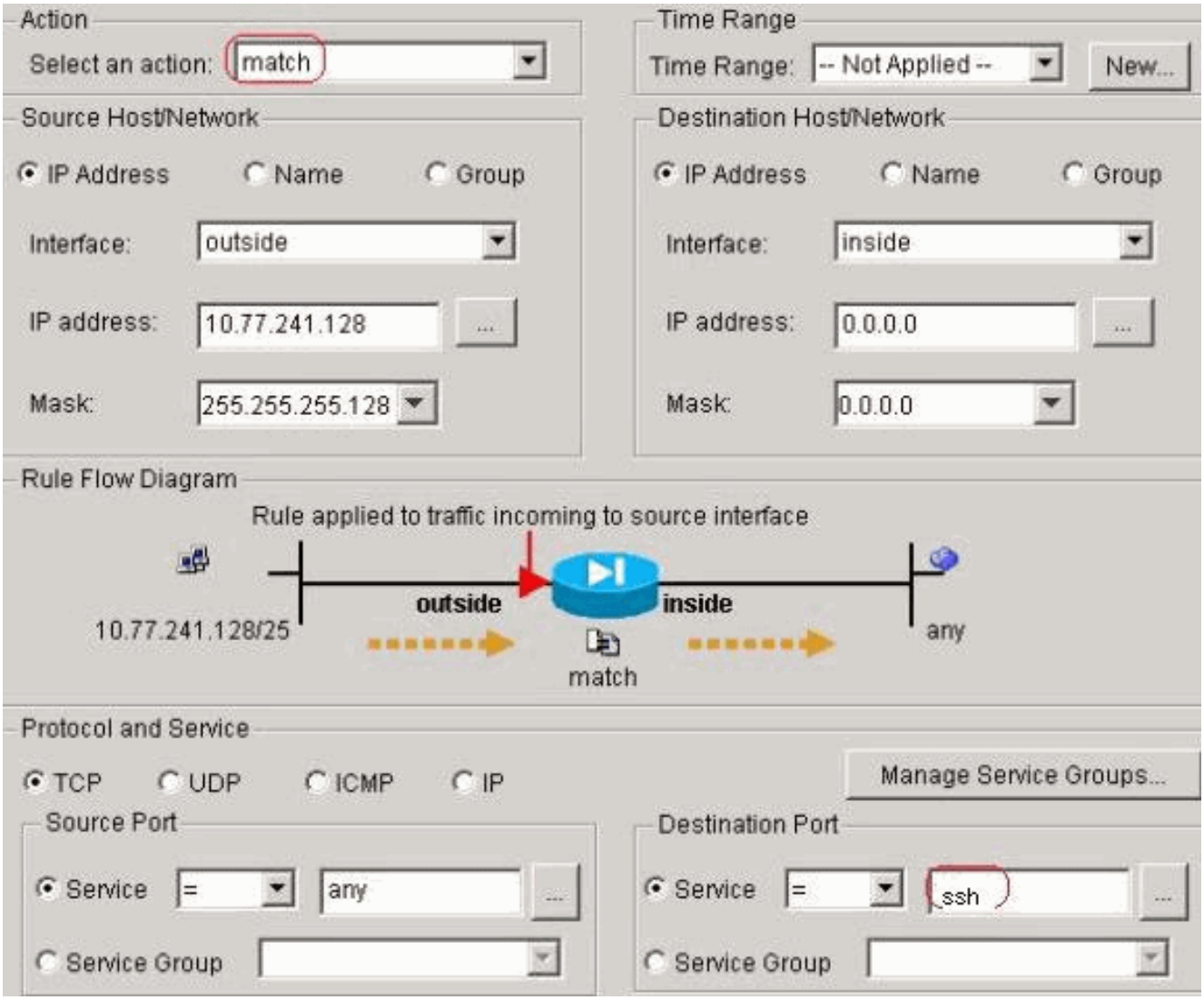
Clique em Next.Crie um **telnet do** nome de mapa da classe e escolha a caixa de verificação do **endereço IP de origem e de destino (usos ACL) nos** critérios de verificação de repetição de dados do
tráfego.

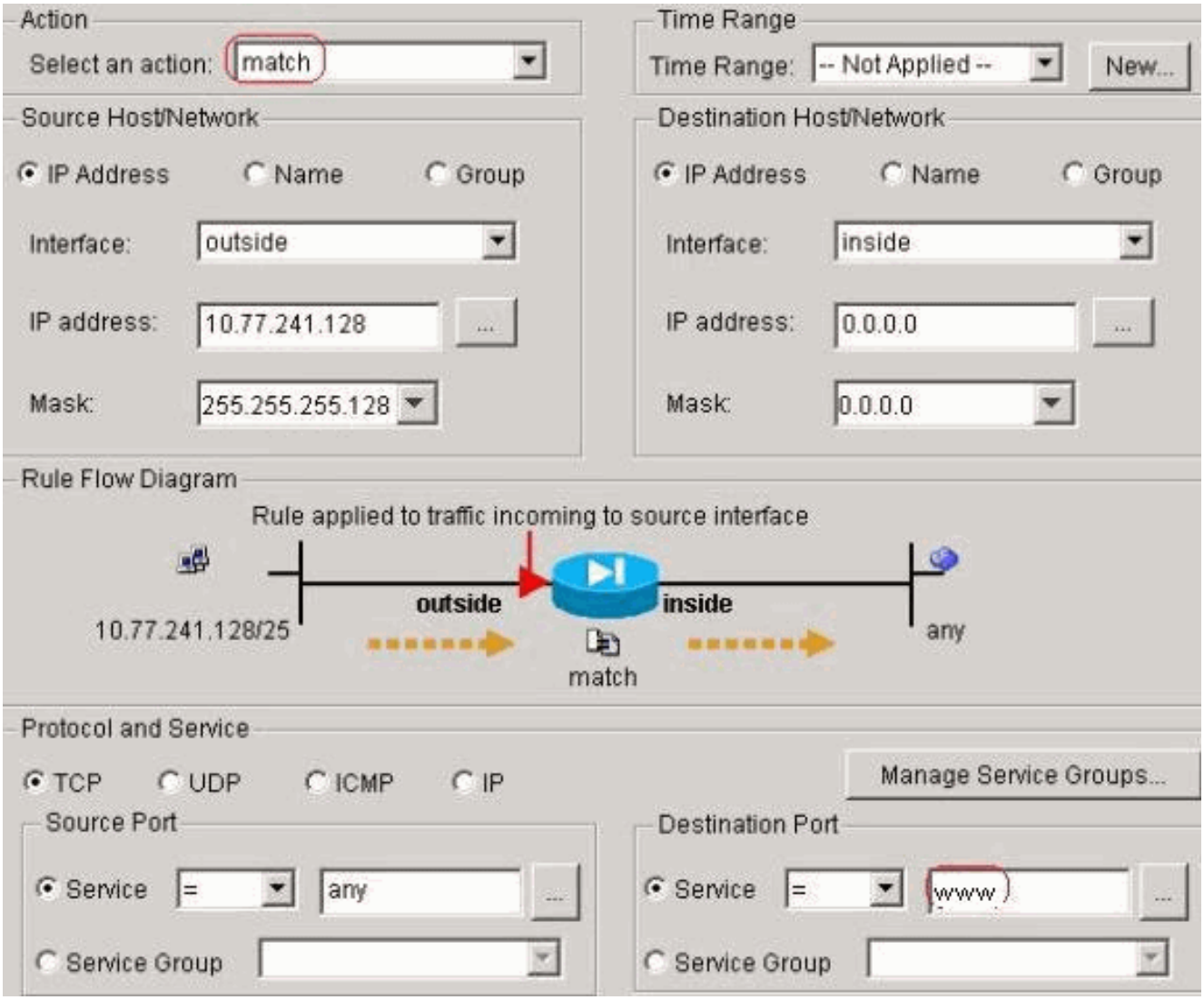


Clique em Next.Crie um ACL a fim combinar o tráfego do telnet originado da rede 10.77.241.128/26 a toda a rede de destino e aplicá-lo para classificar o
telnet.

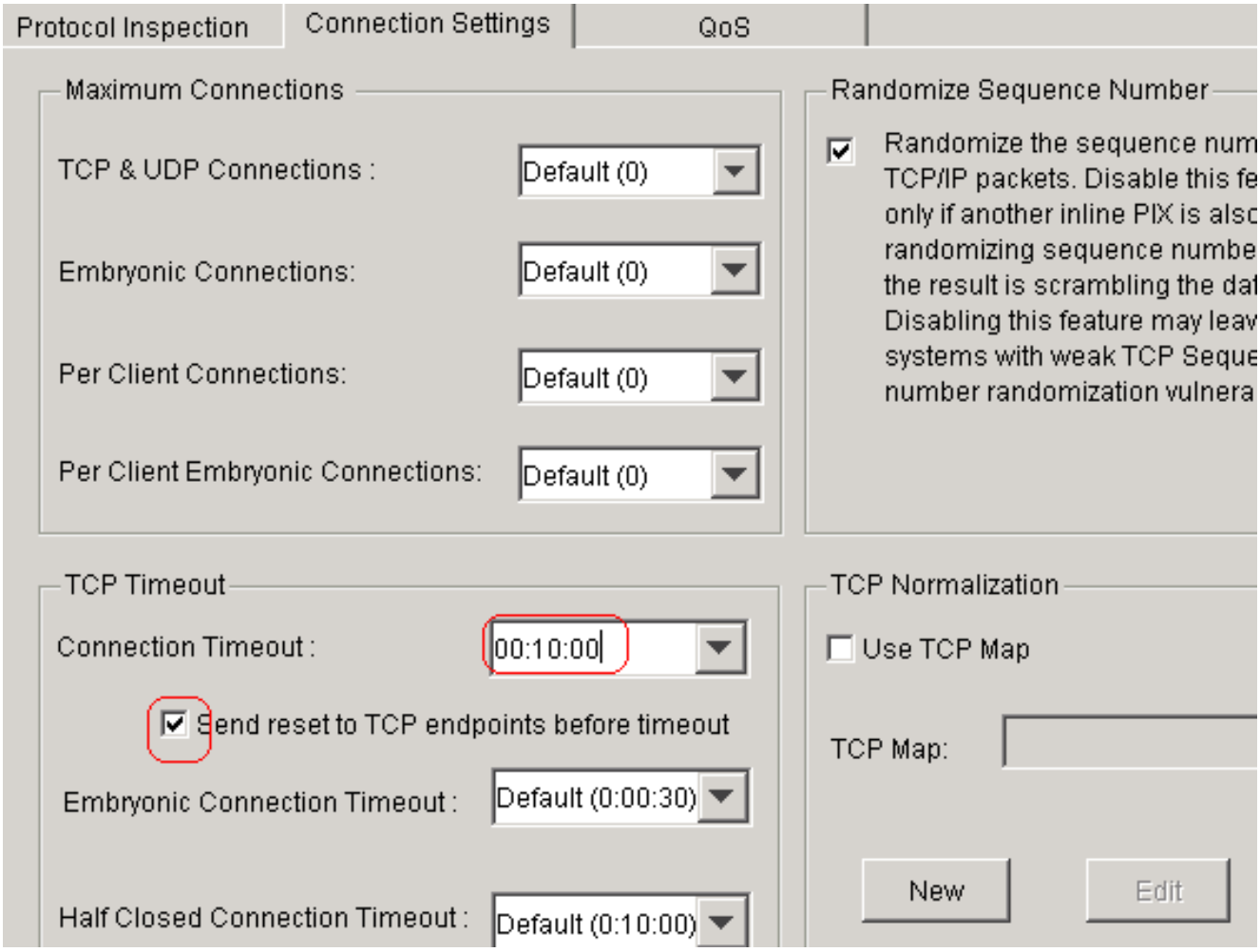


Clique em Next. Similarmente para o ssh e o tráfego HTTP:

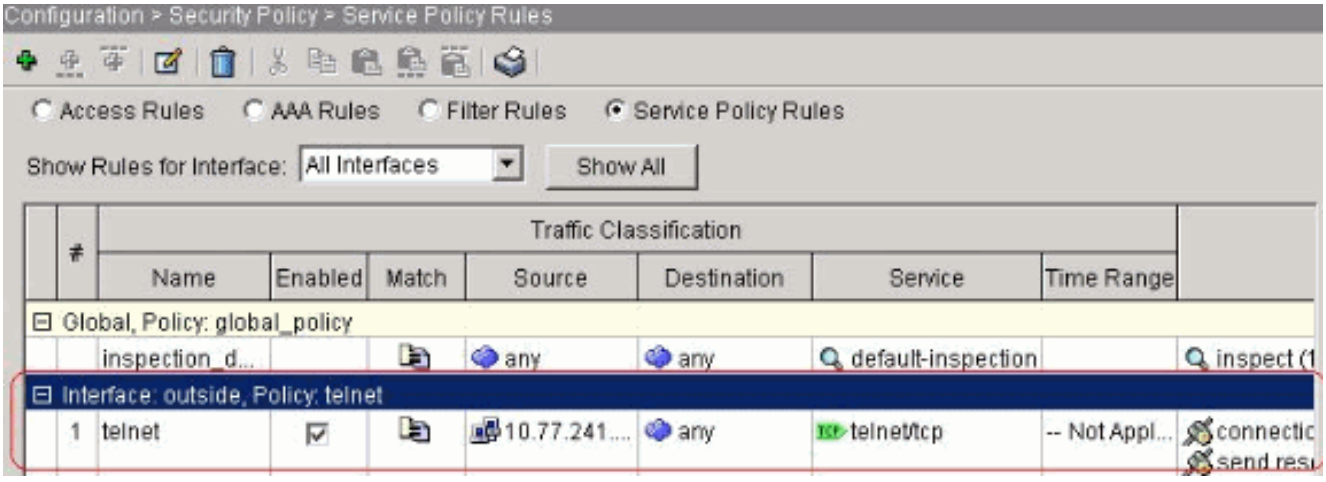

Action
Select an action: match
Time Range
Time Range: -- Not Applied --
New...
Source Host/Network
IP Address
Name
Group
Interface: outside
IP address: 10.77.241.128
Mask: 255.255.255.128
Destination Host/Network
IP Address
Name
Group
Interface: inside
IP address: 0.0.0.0
Mask: 0.0.0.0
Rule Flow Diagram
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



Escolha **configurações de conexão** a fim estabelecer o intervalo de conexão de TCP como os minutos 10, e igualmente escolha a **emissão restaurada aos pontos finais de TCP antes da** caixa de verificação do
intervalo.



Clique em
Finish.



Configuração de CLI equivalente como mostrado:

```
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
```

Intervalo de Ebryonic

Uma conexão embriônica é a conexão que é meia abre ou, por exemplo, o cumprimento de três vias não foi terminado para ele. É definido como o Intervalo de SYN no ASA; à revelia o Intervalo de SYN no ASA é 30 segundos. Esta é a maneira de configurar o intervalo embrionário:

```
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
```

Verificar

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

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use o OIT a fim ver uma análise do emissor de comando de execução.

Emita o **comando show service-policy interface outside** a fim 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 do fluxo da serviço-política da mostra a fim verificar que o tráfego particular combina as configurações da política de serviços.

Esta saída do 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
```

Troubleshooting

Se você encontra que o timeout de conexão não trabalha com a estrutura de política modular (MPF), a seguir verifique a conexão da iniciação TCP. A edição pode ser uma reversão do endereço IP de origem e de destino ou um endereço IP de Um ou Mais Servidores Cisco ICM NT desconfigurado na lista de acessos não combina no MPF para ajustar o valor de timeout novo ou para mudar o timeout padrão para o aplicativo. Crie uma entrada de lista de acesso (fonte e

destino) de acordo com a iniciação de conexão a fim ajustar o timeout de conexão com MPF.

Informações Relacionadas

- Cisco PIX 500 Series Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)

Cisco relacionado apoia discussões da comunidade

Atualizado em: outubro 16, 2008
ID do Documento: 68332