PIX/ASA 7.x and later/FWSM: Set SSH/Telnet/HTTP Connection Timeout using MPF Configuration Example

Document ID: 68332

Updated: Oct 16, 2008

Download PDF
Print
[+] Feedback

Related Products

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco PIX 500 Series Security Appliances

Contents

Introduction

This document provides a sample configuration for PIX 7.1(1) and later of a timeout that is specific to a particular application such as SSH/Telnet/HTTP, as opposed to one that applies to all applications. This configuration example uses the new Modular Policy Framework introduced in PIX 7.0. Refer to Using Modular Policy Framework for more information.

In this sample configuration, the PIX Firewall is configured to allow the workstation

(10.77.241.129) to Telnet/SSH/HTTP to the remote server (10.1.1.1) behind the router. A separate connection timeout to Telnet/SSH/HTTP traffic is also configured. All other TCP traffic continues to have the normal connection timeout value associated with **timeout conn 1:00:00**.

Refer to AASA 8.3 and Later: Set SSH/Telnet/HTTP Connection Timeout using MPF Configuration Example for more information on identical configuration using ASDM with Cisco Adaptive Security Appliance (ASA) with version 8.3 and later.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco PIX/ASA Security Appliance Software Version 7.1(1) with 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

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

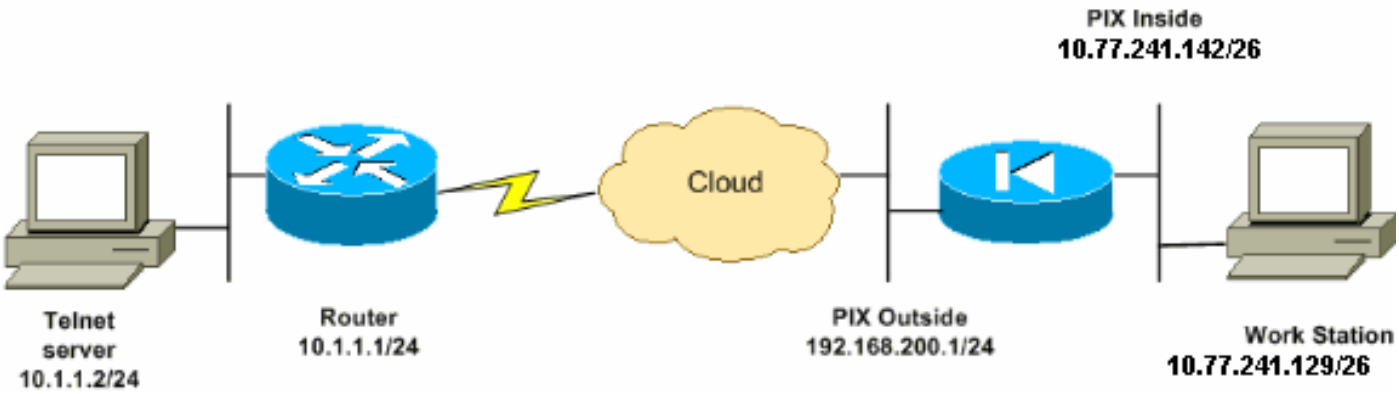
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses, which have been used in a lab environment.

Configuration

This document uses this configuration:

Note: These CLI and ASDM configurations are applicable to the Firewall Service Module (FWSM)

CLI Configuration:

PIX Configuration

```
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
```

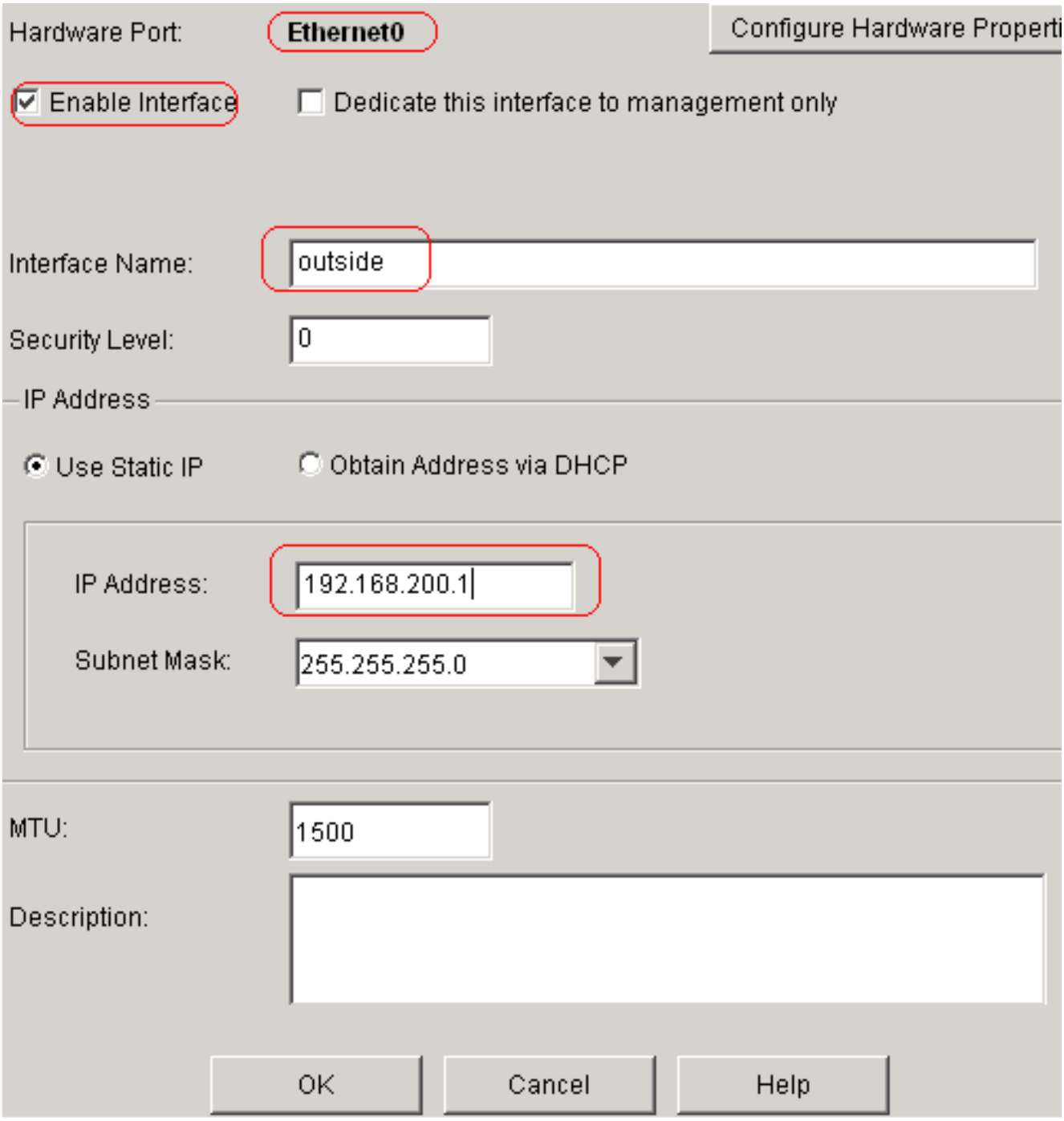
```
Telnet/ssh/http traffic when you use Modular Policy
Framework !--- to configure a security feature. !---
Assign the parameters to be matched by class map. class-
map telnet description telnet match access-list
outside_mpc_in class-map inspection_default match
default-inspection-traffic ! ! policy-map 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
```

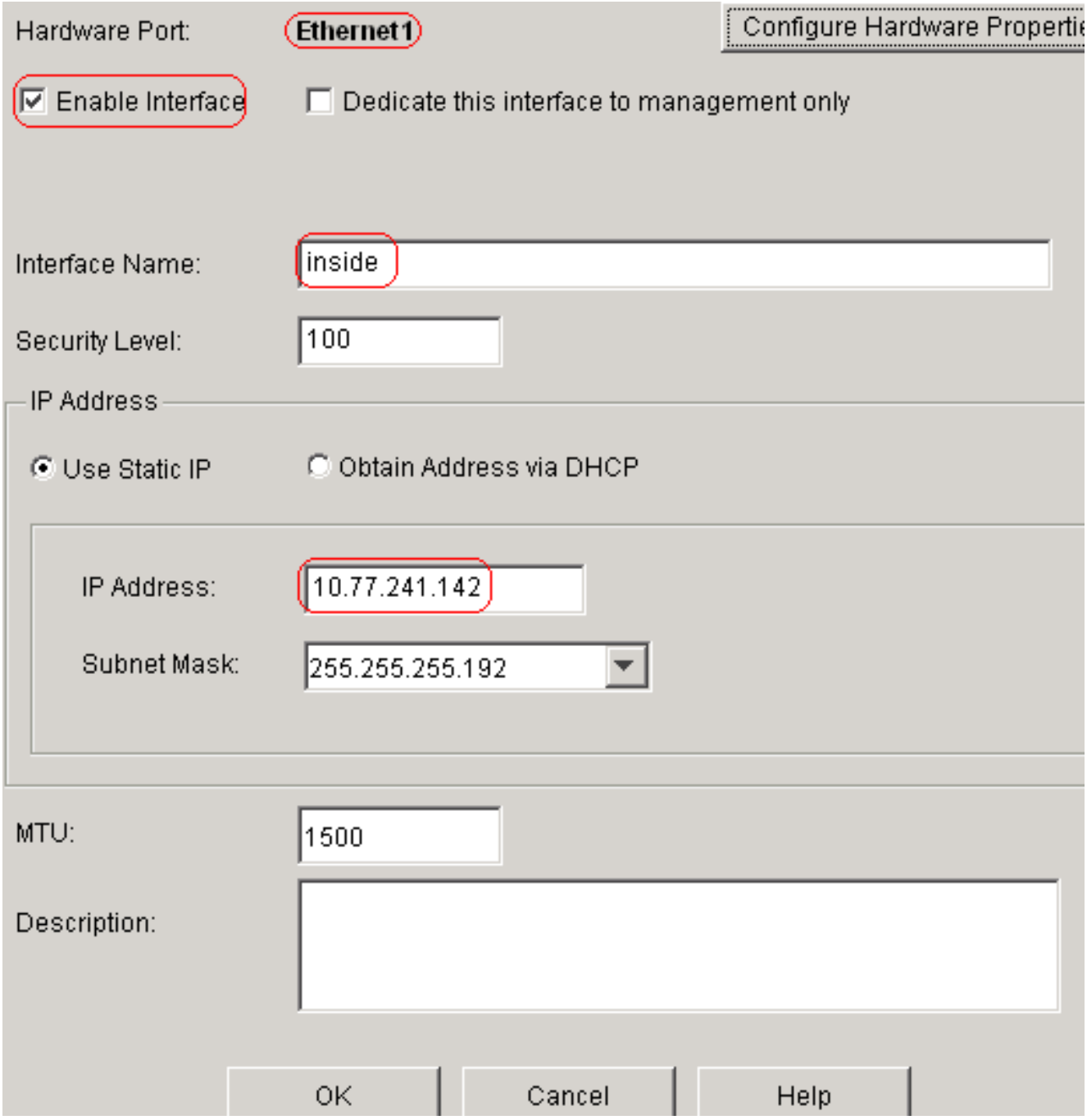
ASDM Configuration:

Complete these steps in order to set up TCP connection timeout for Telnet traffic based on access-list that uses ASDM as shown.

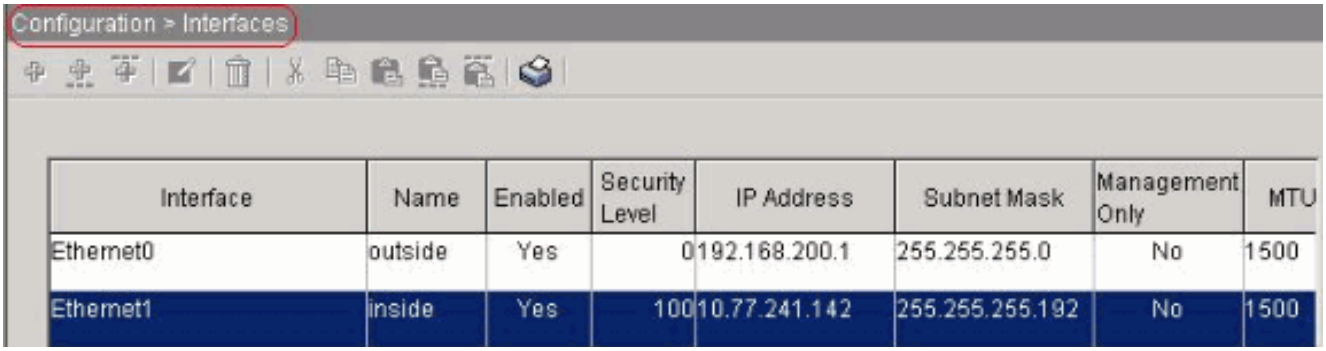
Note: Refer to Allowing HTTPS Access for ASDM for basic settings in order to access the PIX/ASA through ASDM.

1. **Configure Interfaces**Choose **Configuration > Interfaces > Add** in order to configure the interfaces Ethernet0 (outside) and Ethernet1 (inside) as shown.


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



Click
OK.

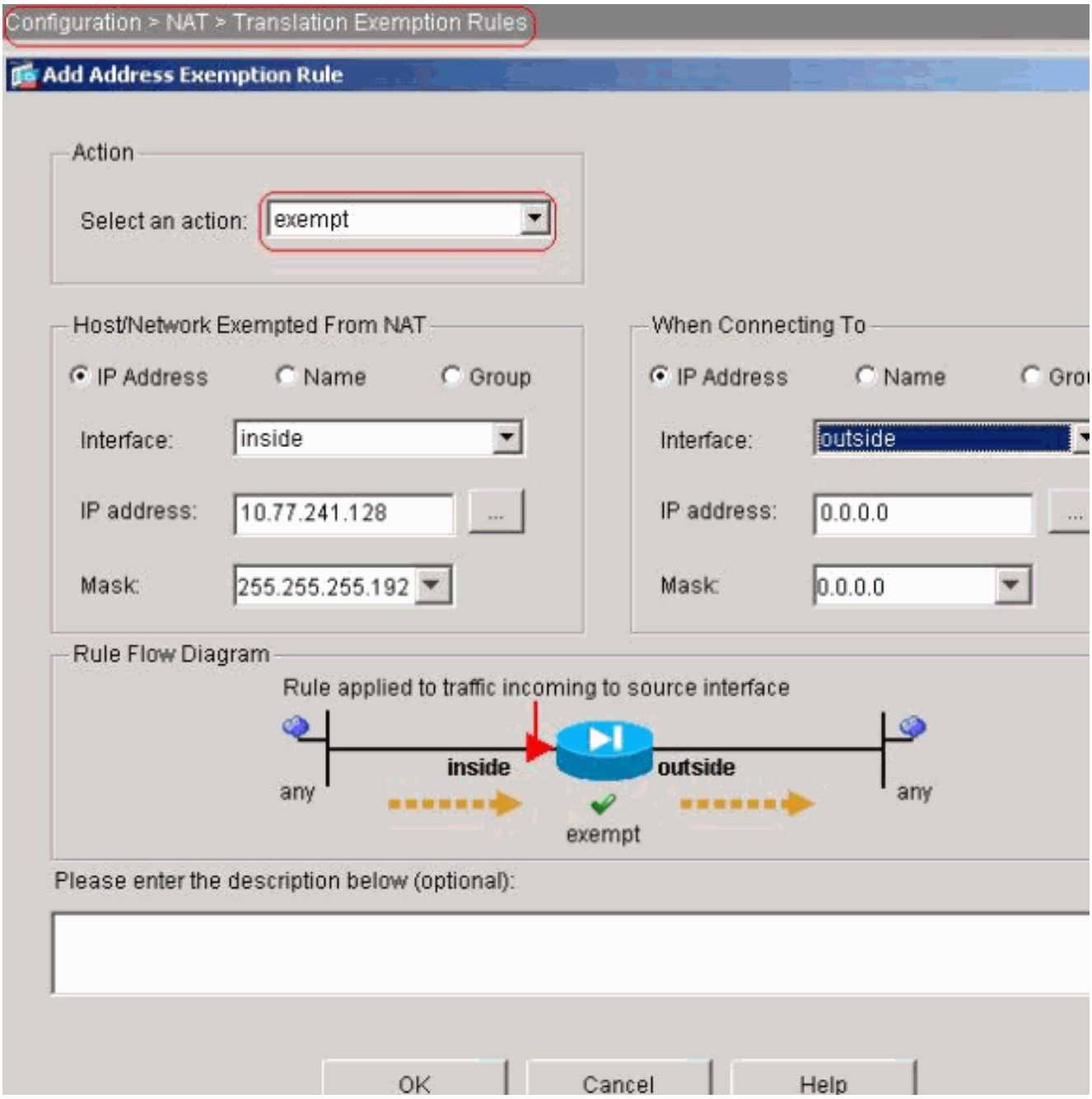


Equivalent CLI configuration as shown:

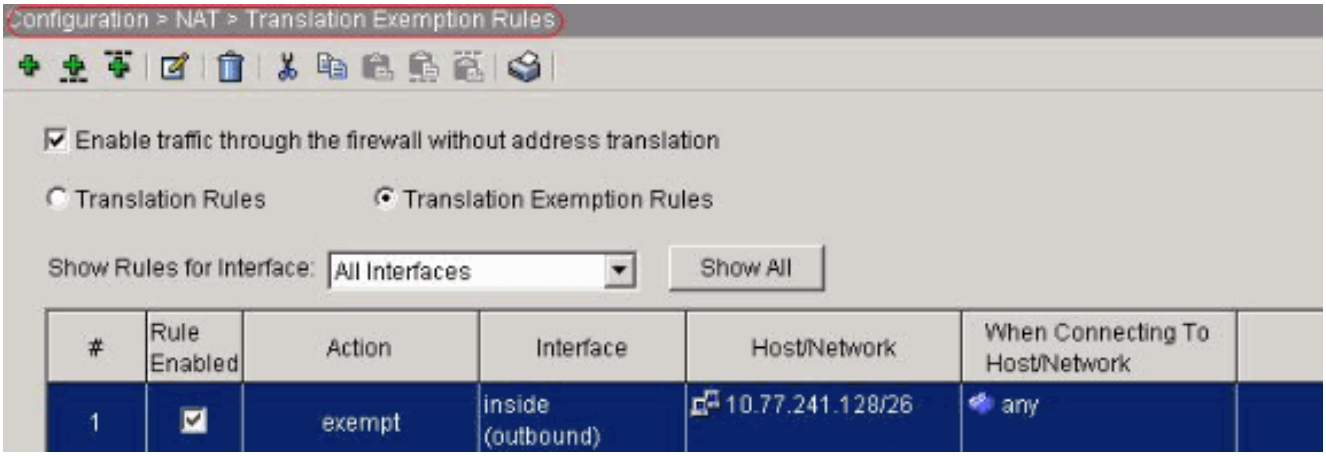
```
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
 nameif inside
```

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

2. **Configure NAT 0**Choose **Configuration > NAT > Translation Exemption Rules > Add** in order to allow the traffic from the network 10.77.241.128/26 to access the internet without any
translation.

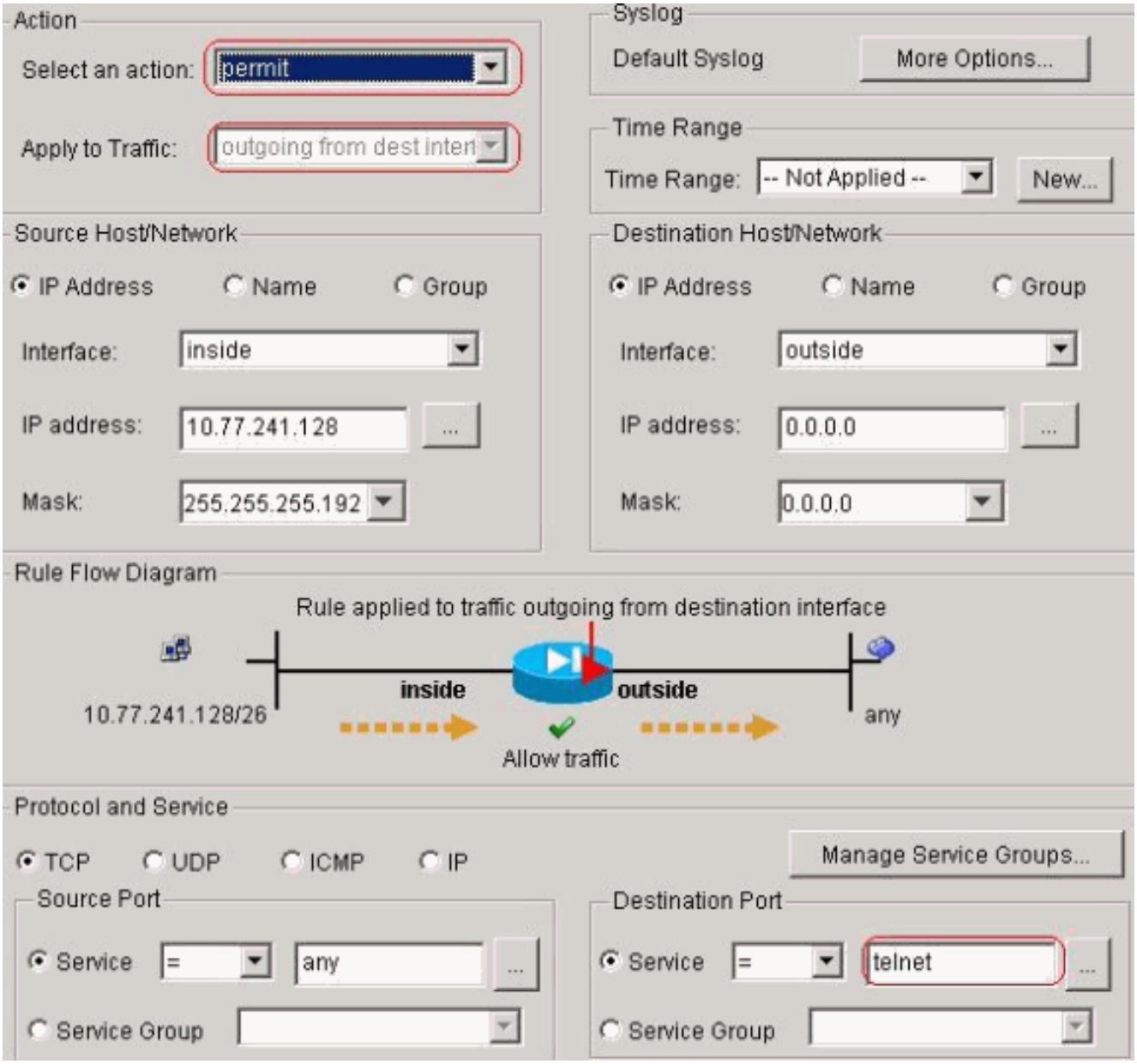


Click
OK.



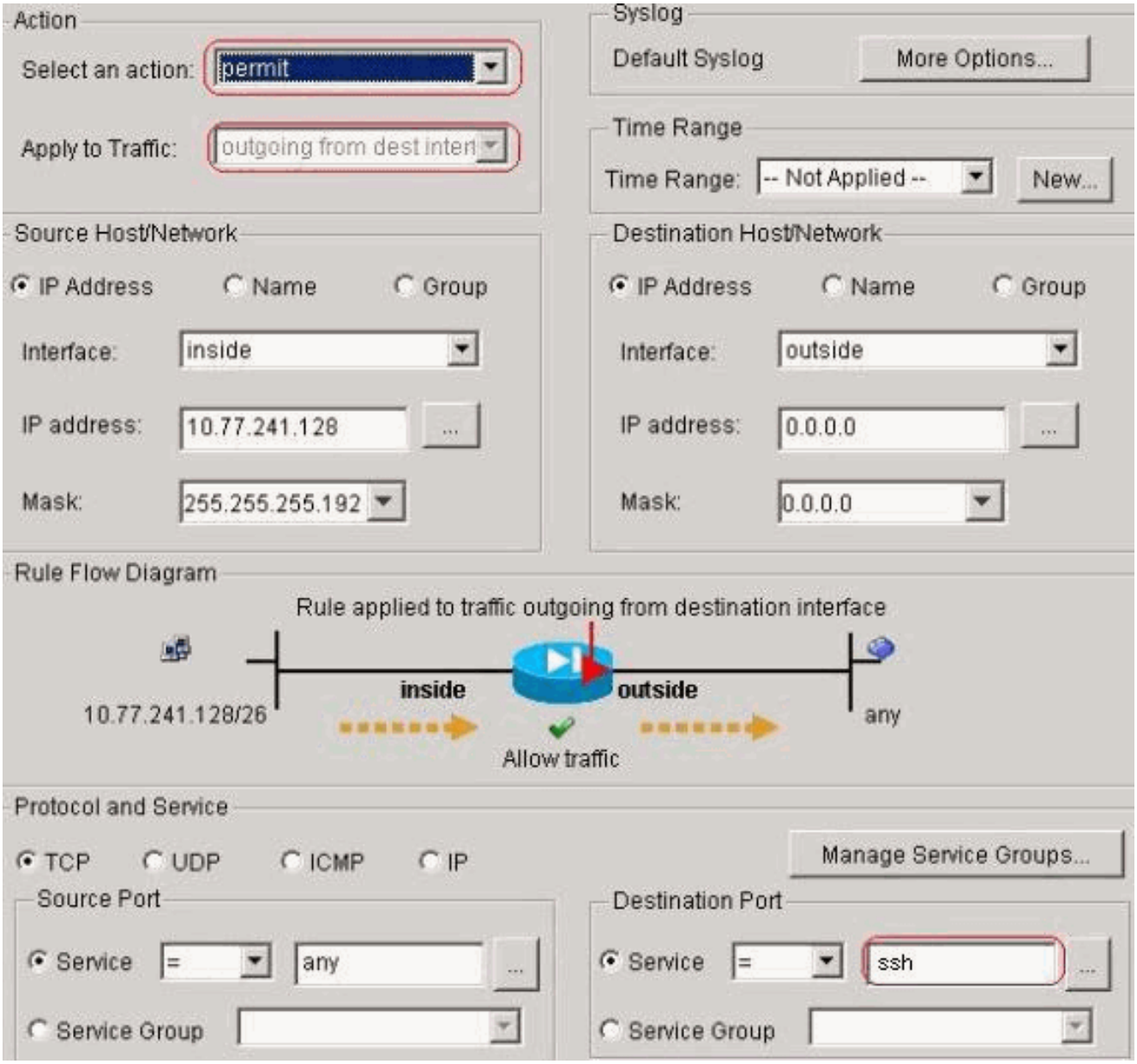
Equivalent CLI configuration as shown:`access-list inside_nat0_outbound extended permit ip 10.77.241.128 255.255.255.192 any`
`nat (inside) 0 access-list inside_nat0_outbound`

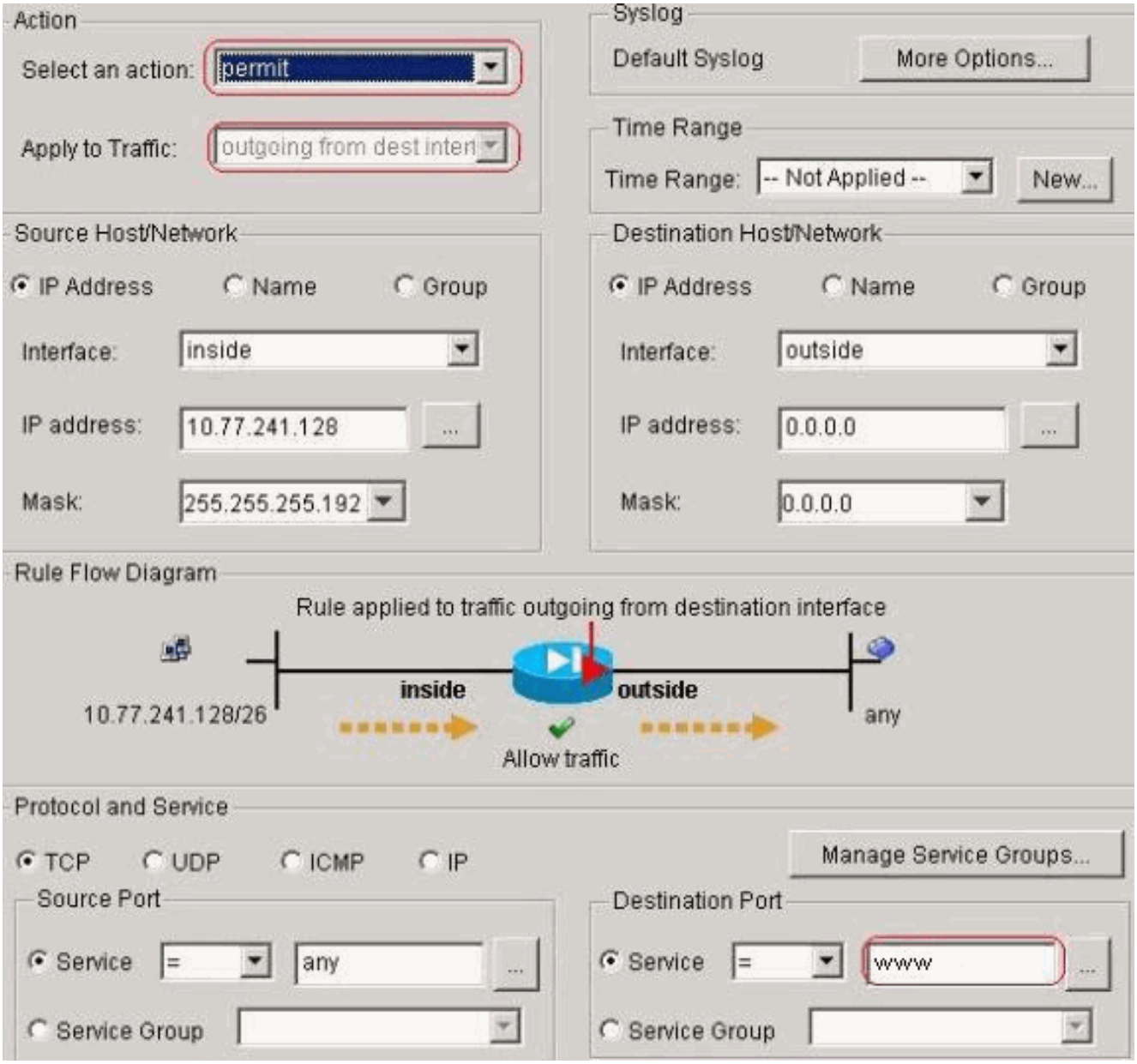
3. **Configure ACLs**Choose **Configuration > Security Policy >Access Rules** in order to configure the ACLs as shown.Click **Add** in order to configure an ACL 101 that allows the Telnet traffic originated from the network 10.77.241.128/26 to any destination network and apply it for outbound traffic on the outside interface.



Click **OK**. Similarly for the ssh and http

traffic:

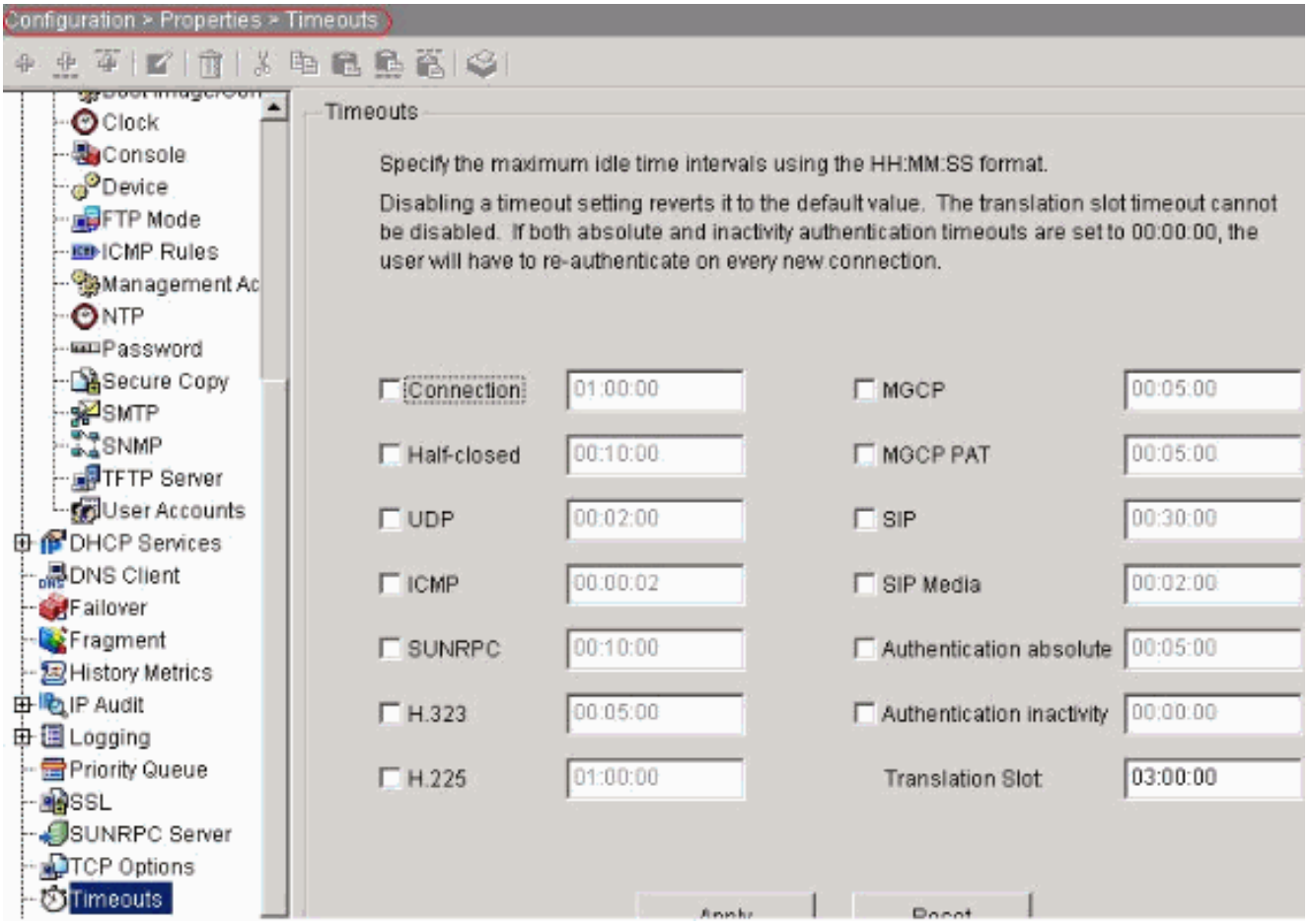

Action
Select an action:
permit
Apply to Traffic:
outgoing from dest inter
Syslog
Default Syslog
More Options...
Time Range
Time Range:
-- Not Applied --
New...
Source Host/Network
IP Address
Name
Group
Interface:
inside
IP address:
10.77.241.128
Mask:
255.255.255.192
Destination Host/Network
IP Address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



Equivalent CLI configuration as shown:

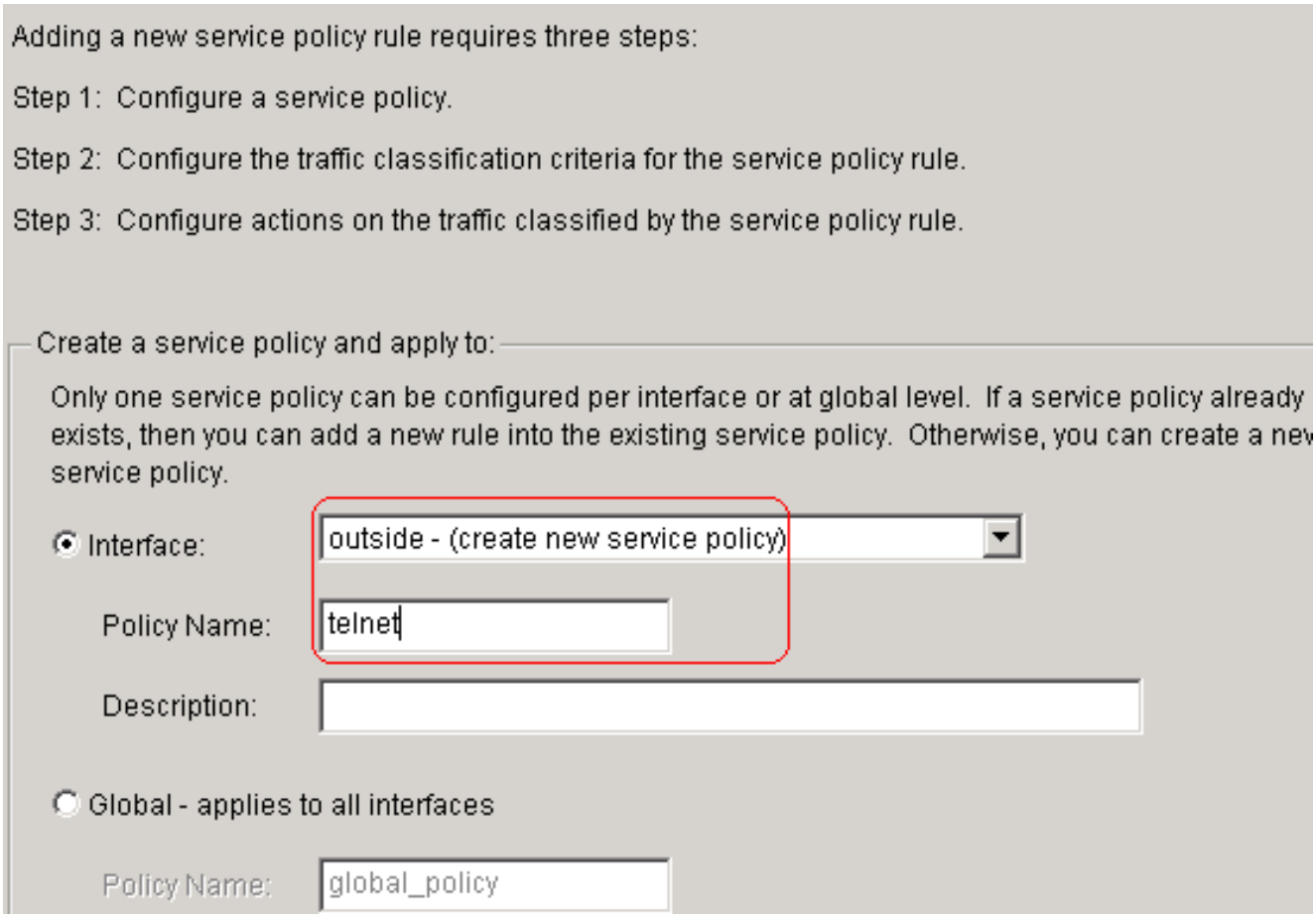
```
access-list 101 extended permit tcp 10.77.241.128
255.255.255.192 any eq telnet
access-list 101 extended permit tcp 10.77.241.128 255.255.255.192 any eq ssh
access-list 101 extended permit tcp 10.77.241.128 255.255.255.192 any eq www
access-group 101 out interface outside
```

4. **Configure Timeouts**Choose **Configuration > Properties > Timeouts** in order to configure the various timeouts. In this scenario, keep the default value for all timeouts.

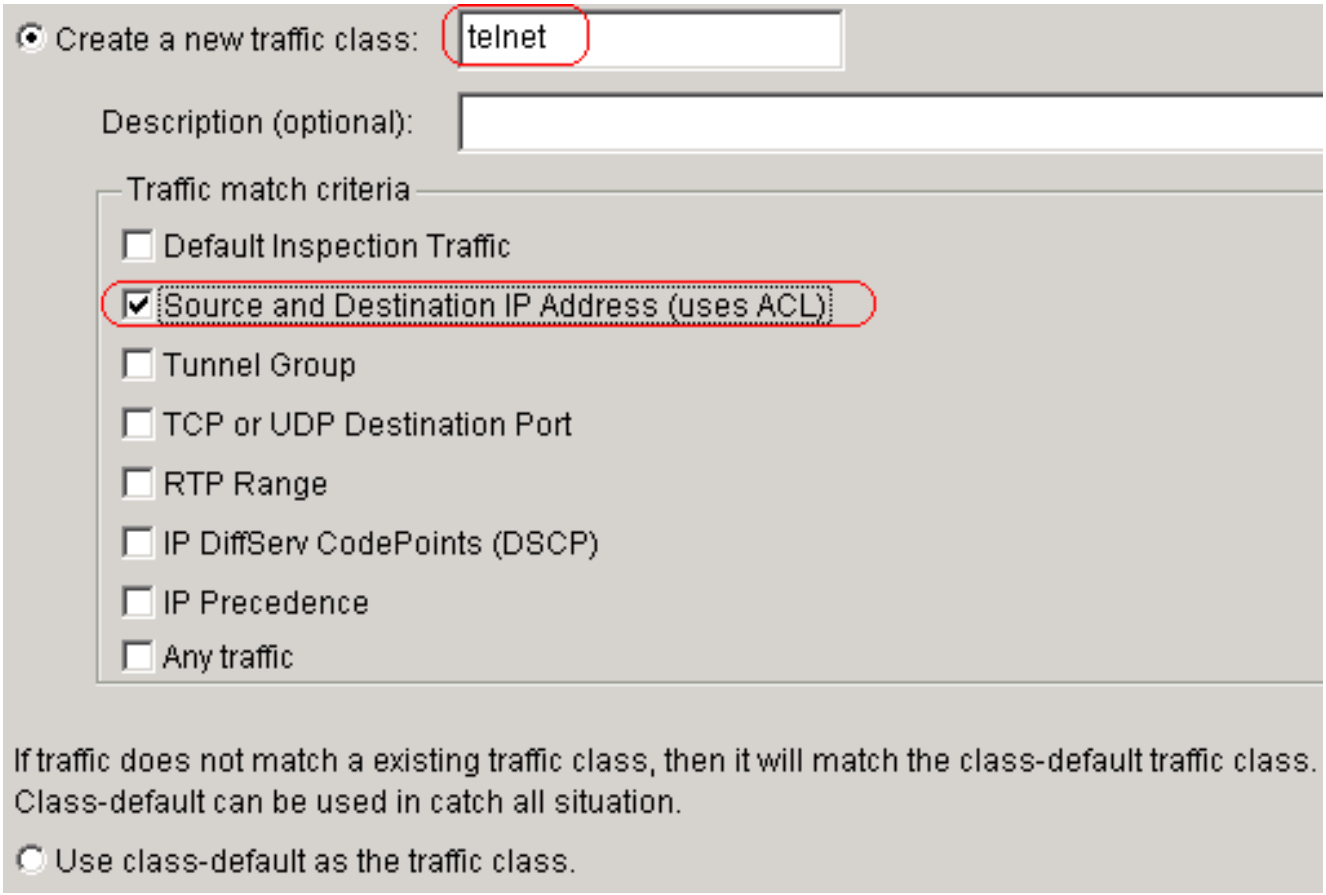


Equivalent CLI configuration as shown:`timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02`

5. Configure **Service Policy Rules**.Choose **Configuration > Security Policy > Service Policy Rules > Add** in order to configure class map, policy map for the setting up the TCP connection timeout as 10 minutes, and apply the service policy on the outside interface as shown.Choose the **Interface** radio button in order to choose **outside - (create new service policy)**, which is to be created, and assign **telnet** as the policy name.

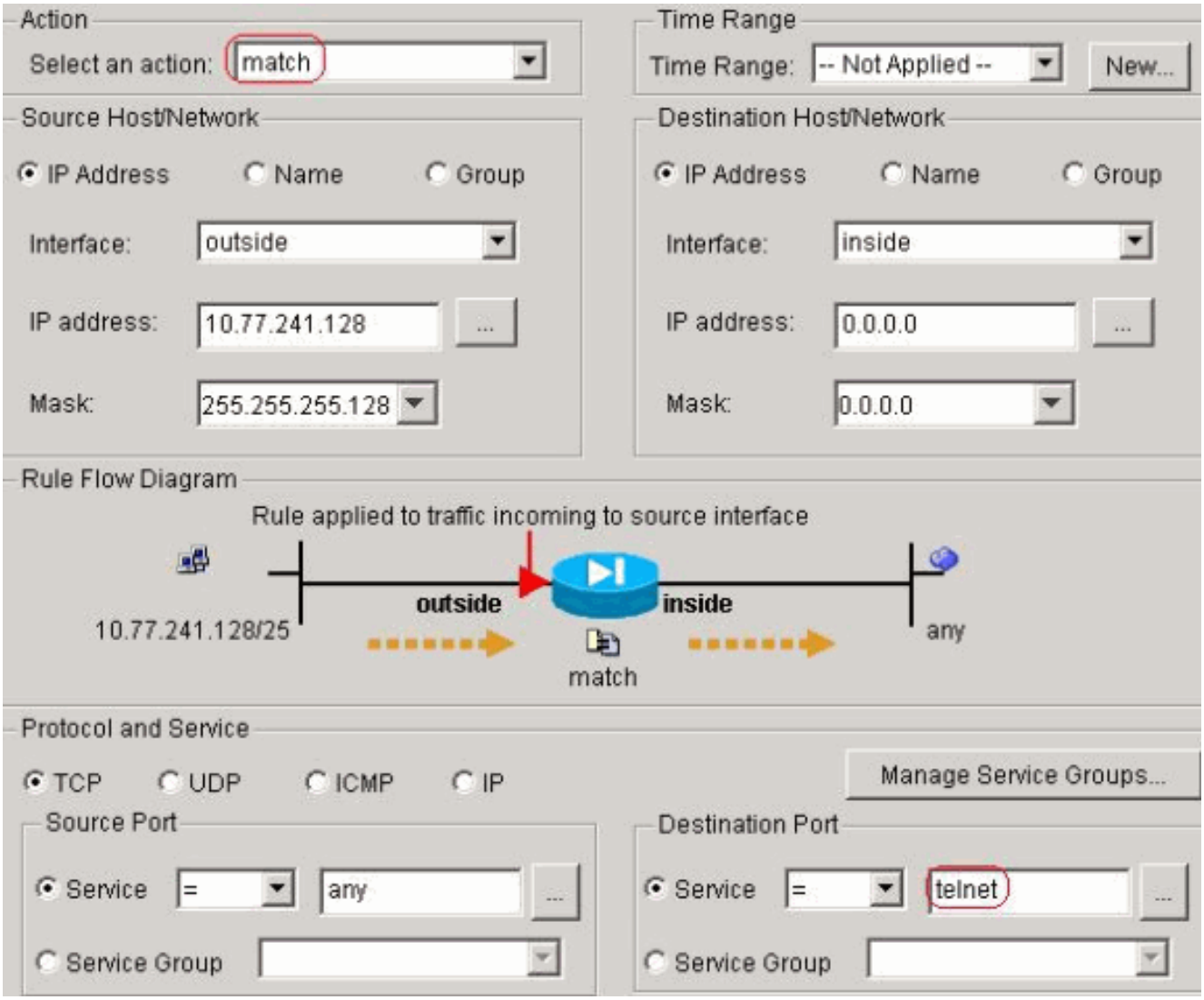


Click **Next**.Create a class map name **telnet** and choose the **Source and Destination IP address (uses ACL)** check box in the Traffic match criteria.

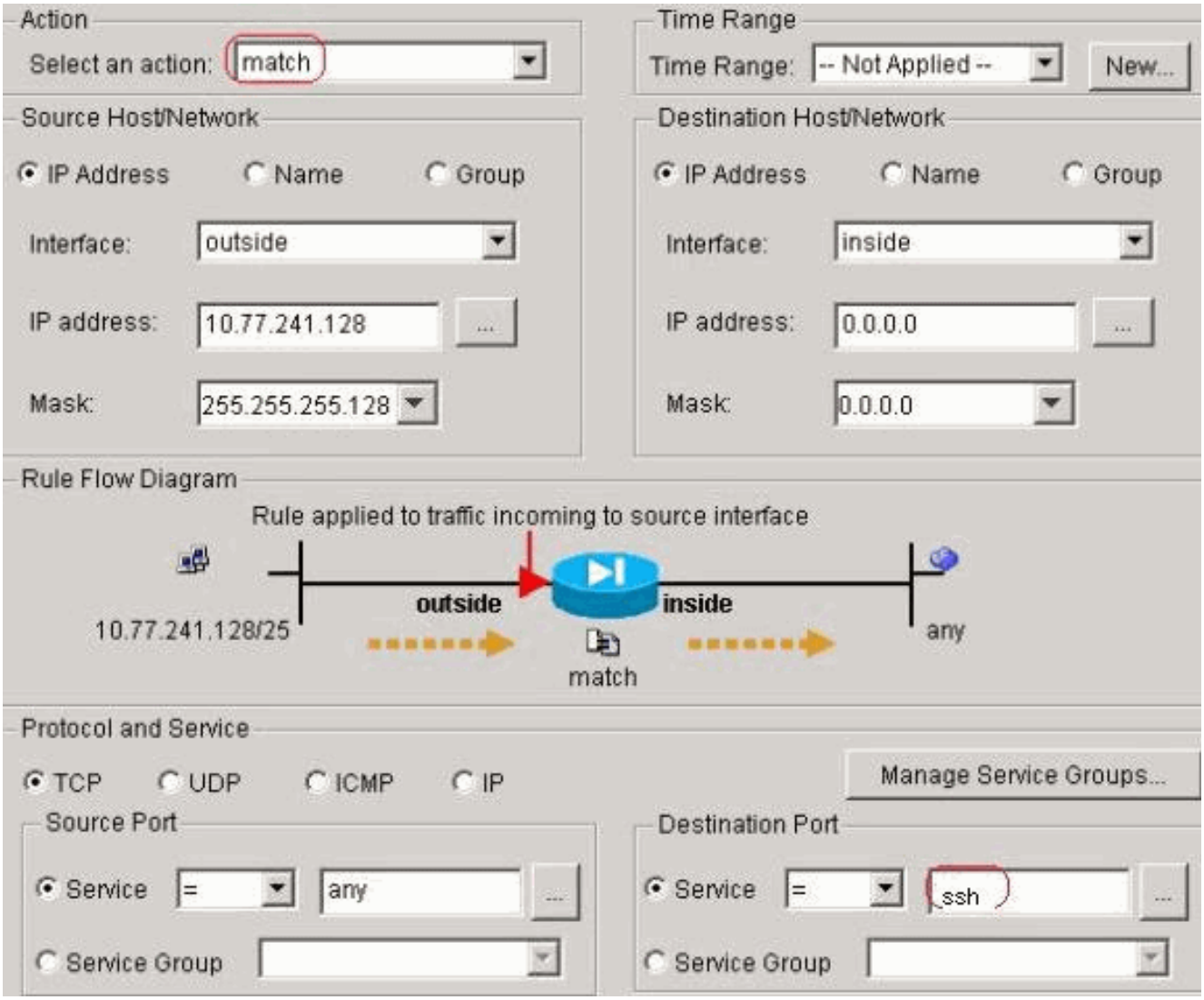


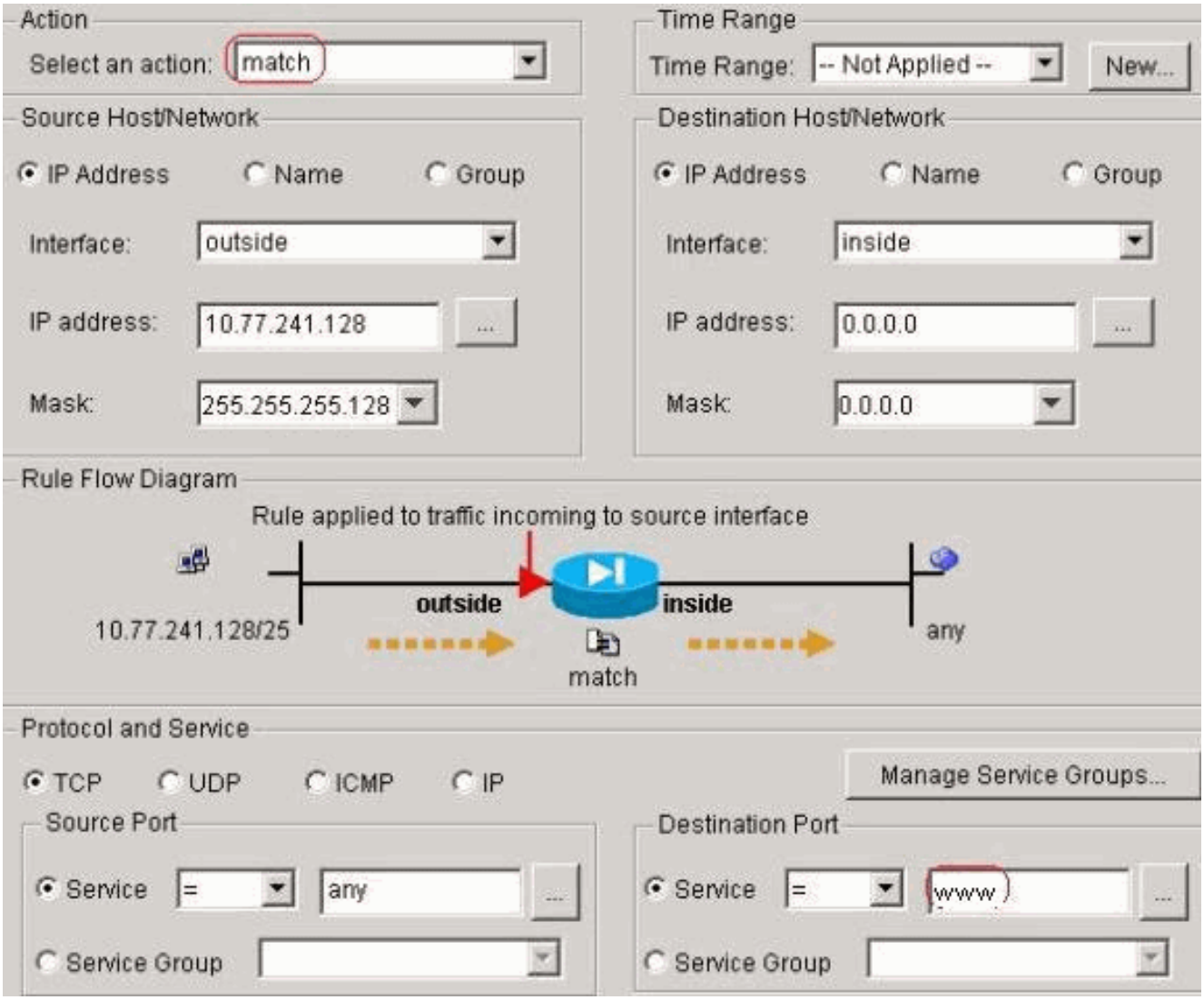
Click **Next**.Create an ACL in order to match the Telnet traffic originated from the network 10.77.241.128/26 to any destination network and apply it to class

telnet.

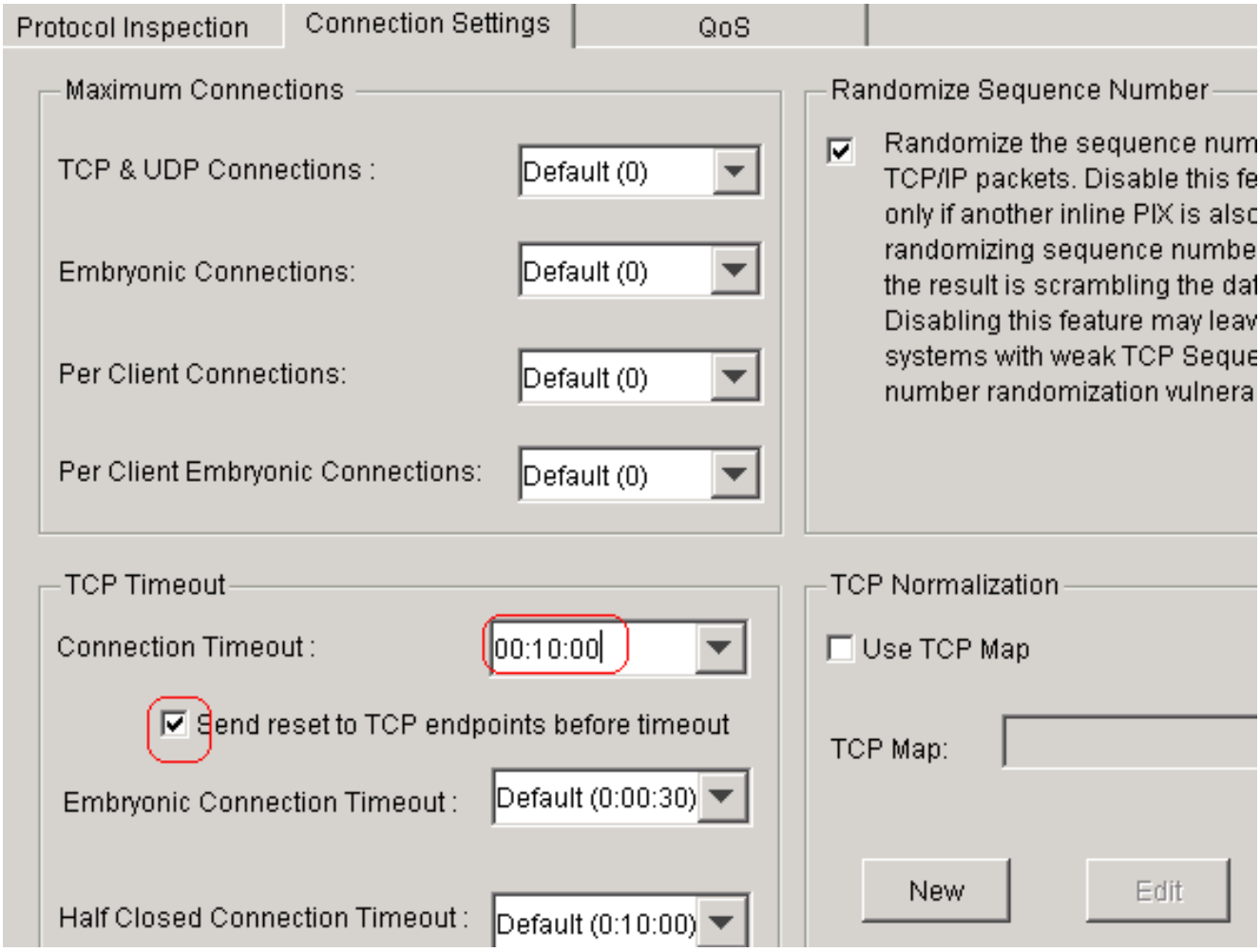


Click **Next**. Similarly for the ssh and http traffic:

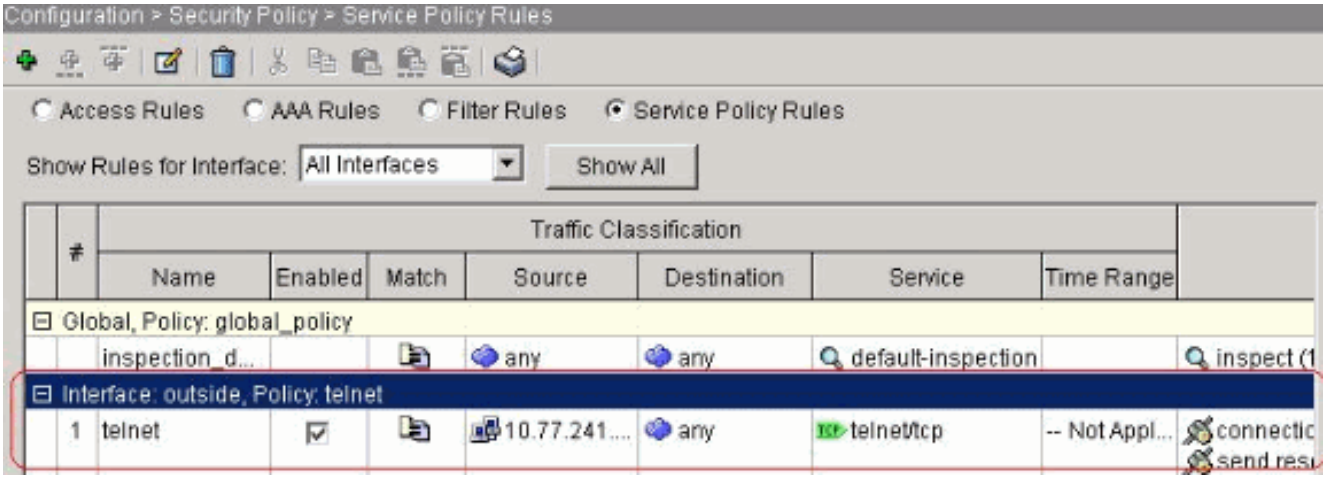

Action
Select an action: match
Time Range
Time Range: -- Not Applied --
New...
Source Host/Network
IP Address
Name
Group
Interface: outside
IP address: 10.77.241.128
Mask: 255.255.255.128
Destination Host/Network
IP Address
Name
Group
Interface: inside
IP address: 0.0.0.0
Mask: 0.0.0.0
Rule Flow Diagram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



Choose **Connection Settings** in order to set up the TCP Connection Timeout as 10 minutes, and also choose the **Send reset to TCP endpoints before timeout** check box.



Click
Finish.



Equivalent CLI configuration as shown:

```
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
```

Ebryonic Timeout

An embryonic connection is the connection that is half open or, for example, the three-way handshake has not been completed for it. It is defined as SYN timeout on the ASA; by default the SYN timeout on the ASA is 30 seconds. This is the way to configure 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
```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT in order to view an analysis of **show** command output.

Issue the **show service-policy interface outside** command in order to verify your 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
```

Issue the **show service-policy flow** command in order to verify that the particular traffic matches the service policy configurations.

This command output shows an example:

```
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

If you find that the connection timeout does not work with the Modular Policy Framework (MPF), then check the TCP initiation connection. The issue can be a reversal of the source and destination IP address or a misconfigured IP address in the access list does not match in the MPF to set the new timeout value or to change the default timeout for the application. Create an access list entry (source and destination) in accordance with the connection initiation in order to set the connection timeout with MPF.

Related Information

- **Cisco PIX 500 Series Security Appliances**

- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **Cisco PIX Security Appliance Release Notes**
- **Cisco PIX Firewall Software**
- **Cisco Secure PIX Firewall Command References**
- **Security Product Field Notices (including PIX)**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation - Cisco Systems**

Was this document helpful? Yes No

Thank you for your feedback.

Open a Support Case (Requires a Cisco Service Contract.)

Related Cisco Support Community Discussions

The Cisco Support Community is a forum for you to ask and answer questions, share suggestions, and collaborate with your peers.

Refer to Cisco Technical Tips Conventions for information on conventions used in this document.

Updated: Oct 16, 2008
Document ID: 68332