PIX/ASA 7.x及更高版本/FWSM:使用MPF配置設定SSH/Telnet/HTTP連線超時示例

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[設定](#)
[網路圖表](#)
[組態](#)
[Ebryonic超時](#)
[驗證](#)
[疑難排解](#)

簡介

本文檔提供了PIX 7.1(1)及更高版本的超時配置示例，該超時配置特定於特定應用程式（如SSH/Telnet/HTTP），而不是應用於所有應用程式的超時配置。此配置示例使用PIX 7.0中引入的新模組化策略框架。有關詳細資訊，請參閱使用模組化策略框架。

在此示例配置中，PIX防火牆配置為允許工作站(10.77.241.129)通過Telnet/SSH/HTTP連線到路由器後面的遠端伺服器(10.1.1.1)。還配置了Telnet/SSH/HTTP流量的單獨連線超時。所有其他TCP流量繼續具有與**timeout conn 1:00:00關聯的正常連線超時值**。

請參閱ASA 8.3及更高版本：使用MPF設定SSH/Telnet/HTTP連線超時配置示例以瞭解有關使用帶8.3版及更高版本的思科自適應安全裝置(ASA)的ASDM進行相同配置的詳細資訊。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於採用自適應安全裝置管理器(ASDM)5.1的Cisco PIX/ASA安全裝置軟體版本7.1(1)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

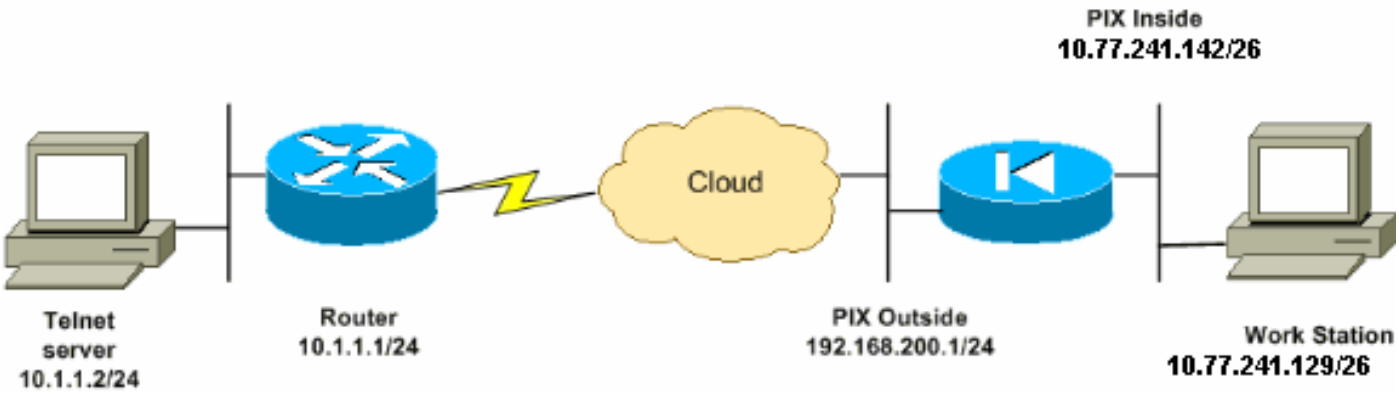
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用 Command Lookup Tool(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



注意：此配置中使用的IP編址方案在Internet上不能合法路由。它們是RFC 1918地址，已在實驗室環境中使用。

組態

本檔案會使用以下設定：

注意：這些CLI和ASDM配置適用於防火牆服務模組(FWSM)

CLI配置：

PIX配置

```
PIX Version - 7.1(1)
!
hostname PIX
domain-name Cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
```

```
 ip address 10.77.241.142 255.255.255.192
!


access-list inside_nat0_outbound extended permit ip
10.77.241.128 255.255.255.192 any

!--- Define the traffic that has to be matched in the
class map. !--- Telnet is defined in this example.
access-list outside_mpc_in extended permit tcp host
10.77.241.129 any eq telnet
access-list outside_mpc_in extended permit tcp host
10.77.241.129 any eq ssh
access-list outside_mpc_in extended permit tcp host
10.77.241.129 any eq www
access-list 101 extended permit tcp 10.77.241.128
255.255.255.192 any eq telnet
access-list 101 extended permit tcp 10.77.241.128
255.255.255.192 any eq ssh
access-list 101 extended permit tcp 10.77.241.128
255.255.255.192 any eq www

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list inside_nat0_outbound
access-group 101 in interface outside

route outside 0.0.0.0 0.0.0.0 192.168.200.2 1
timeout xlate 3:00:00

!--- The default connection timeout value of one hour is
applicable to !--- all other TCP applications. timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!

!--- Define the class map telnet in order !--- to
classify Telnet/ssh/http traffic when you use Modular
Policy Framework !--- to configure a security feature.
!--- Assign the parameters to be matched by class map.


class-map telnet
 description telnet
  match access-list outside_mpc_in

class-map inspection_default
 match default-inspection-traffic
!
```

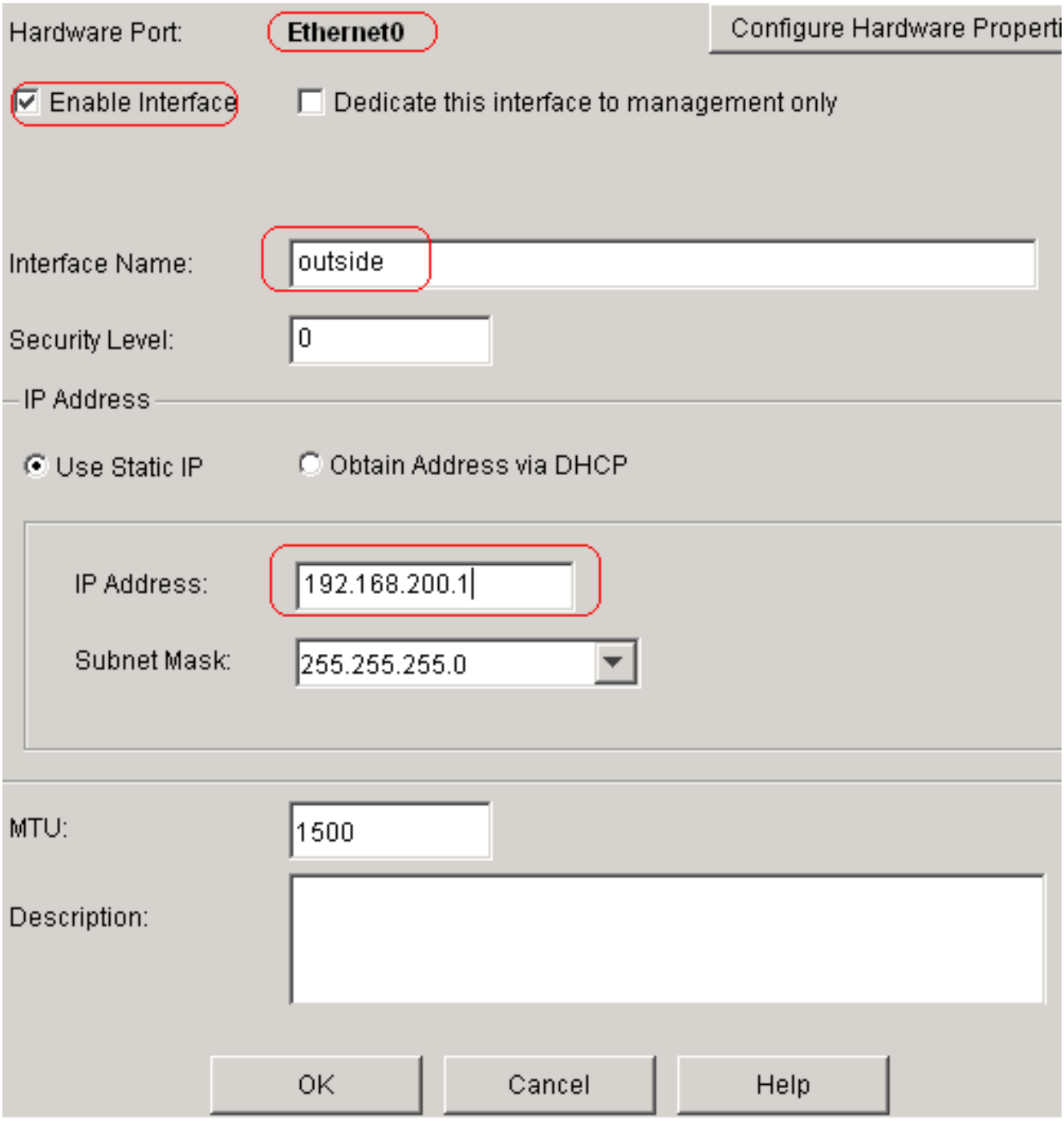
```
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp

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


policy-map telnet

!--- Set the connection timeout under the class mode in
which !--- the idle TCP (Telnet/ssh/http) connection is
disconnected. !--- There is a set value of ten minutes
in this example. !--- The minimum possible value is five
minutes. class telnet
  set connection timeout tcp 00:10:00 reset
!
!
service-policy global_policy global

!--- Apply the policy-map telnet on the interface. !---
You can apply the service-policy command to any
interface that !--- can be defined by the nameif
command.

service-policy telnet interface outside
end
```

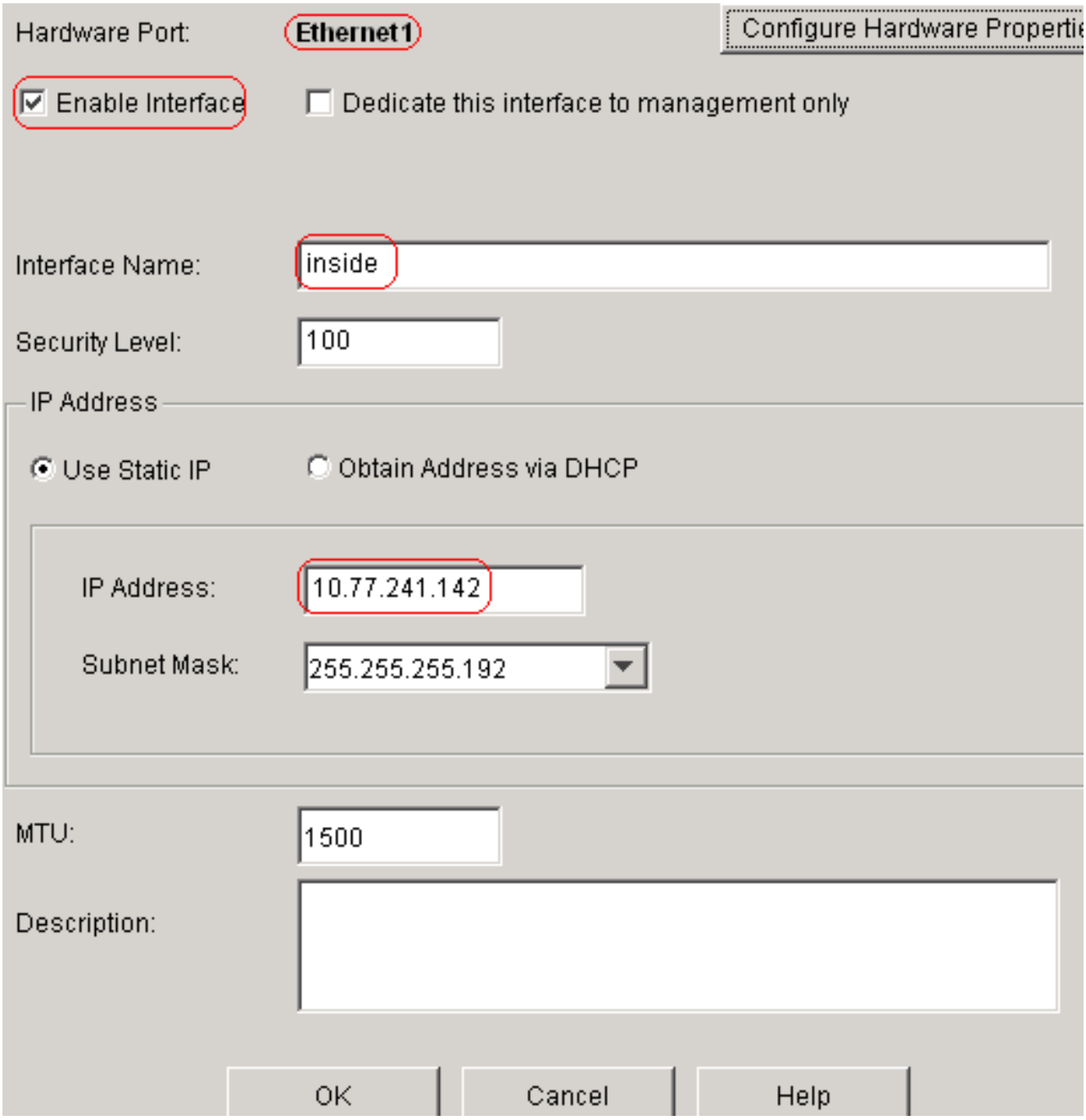
ASDM配置：

完成這些步驟，以便根據使用ASDM的訪問清單為Telnet流量設定TCP連線超時，如下所示。

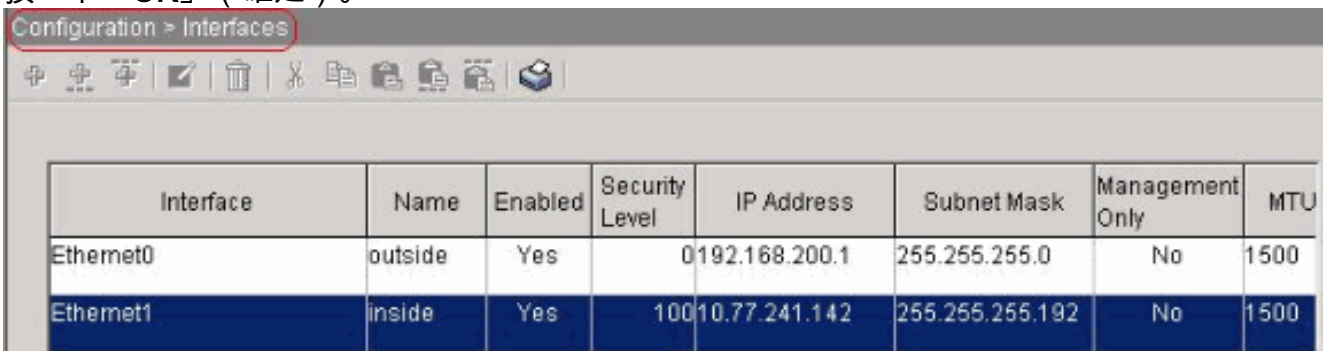
注意：請參閱允許ASDM的HTTPS訪問以瞭解基本設定，以便通過ASDM訪問PIX/ASA。

1. **配置介面**選擇**Configuration > Interfaces > Add**以配置介面Ethernet0（外部）和Ethernet1（內部），如下所示。


Hardware Port:
Ethernet0
Configure Hardware Properti
Enable Interface
Dedicate this interface to management only
Interface Name:
outside
Security Level:
0
IP Address
Use Static IP
Obtain Address via DHCP
IP Address:
192.168.200.1
Subnet Mask:
255.255.255.0
MTU:
1500
Description:
OK
Cancel
Help



按一下「**OK**」（確定）。



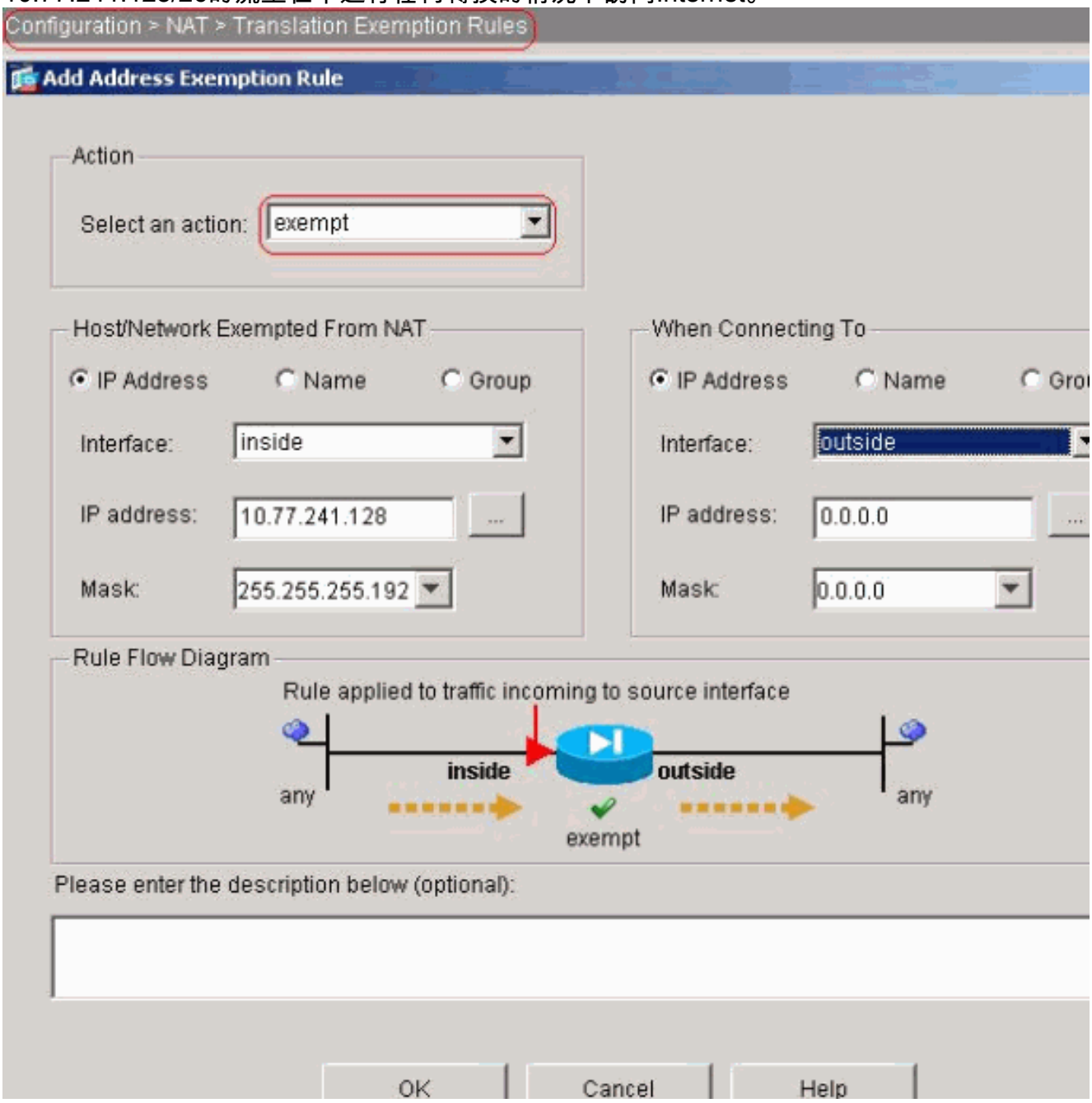
Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU
Ethernet0	outside	Yes	0	192.168.200.1	255.255.255.0	No	1500
Ethernet1	inside	Yes	100	10.77.241.142	255.255.255.192	No	1500

等效的CLI配置，如下所示：

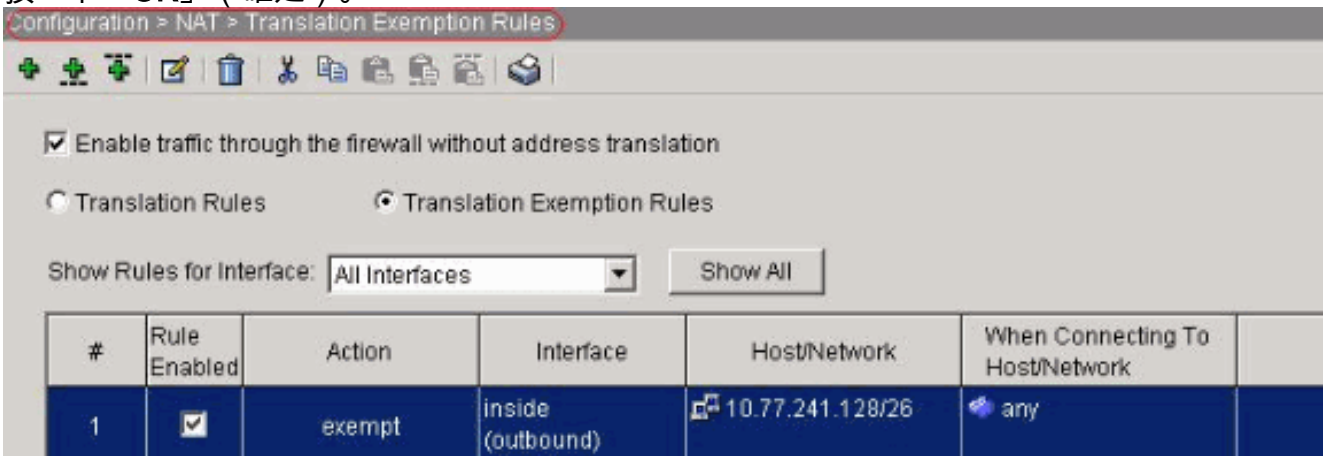
```
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
```

```
ip address 10.77.241.142 255.255.255.192
```

2. **配置NAT 0選擇Configuration > NAT > Translation Exemption Rules > Add**，以允許來自網路10.77.241.128/26的流量在不進行任何轉換的情況下訪問Internet。



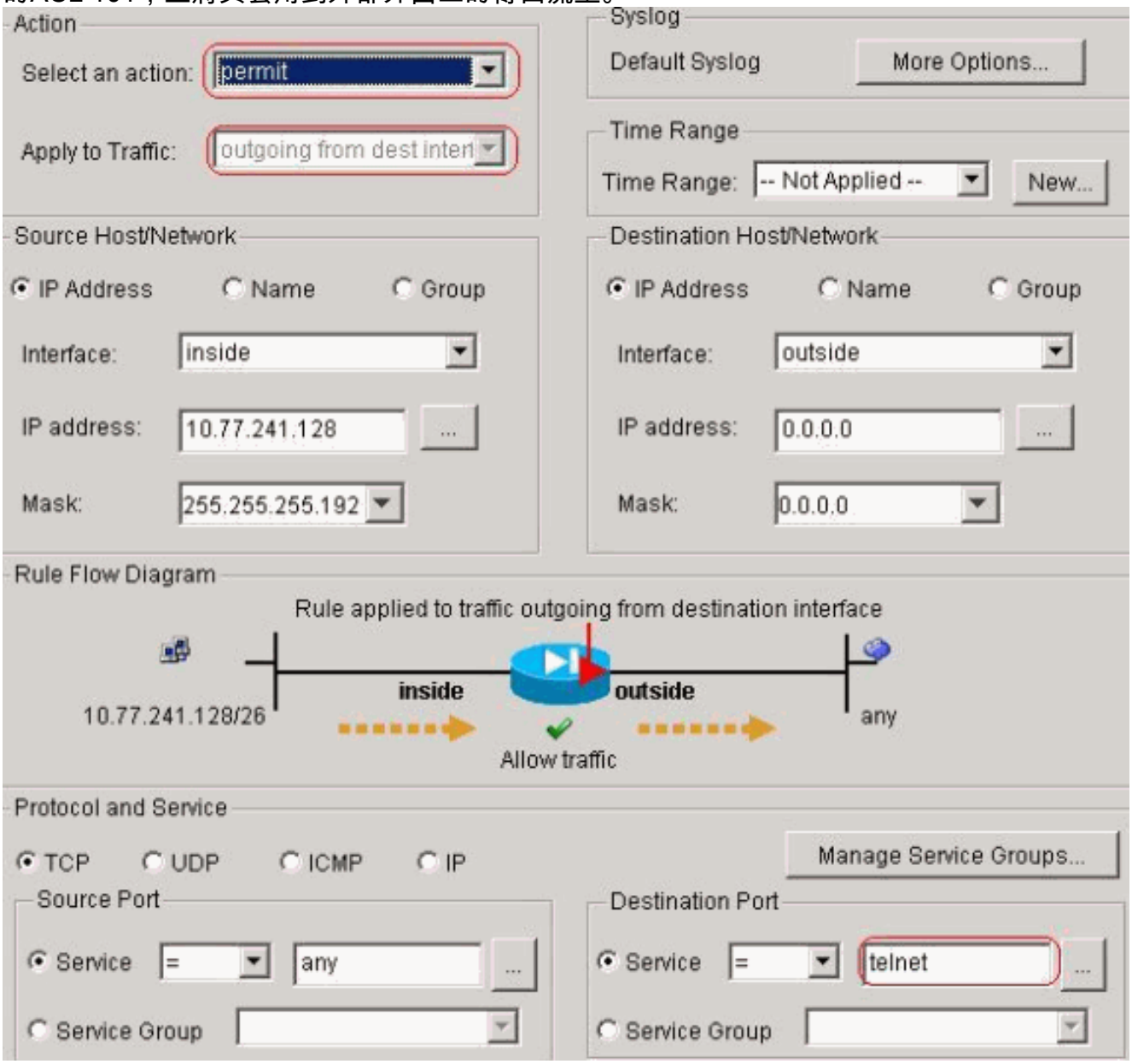
按一下「**OK**」（確定）。



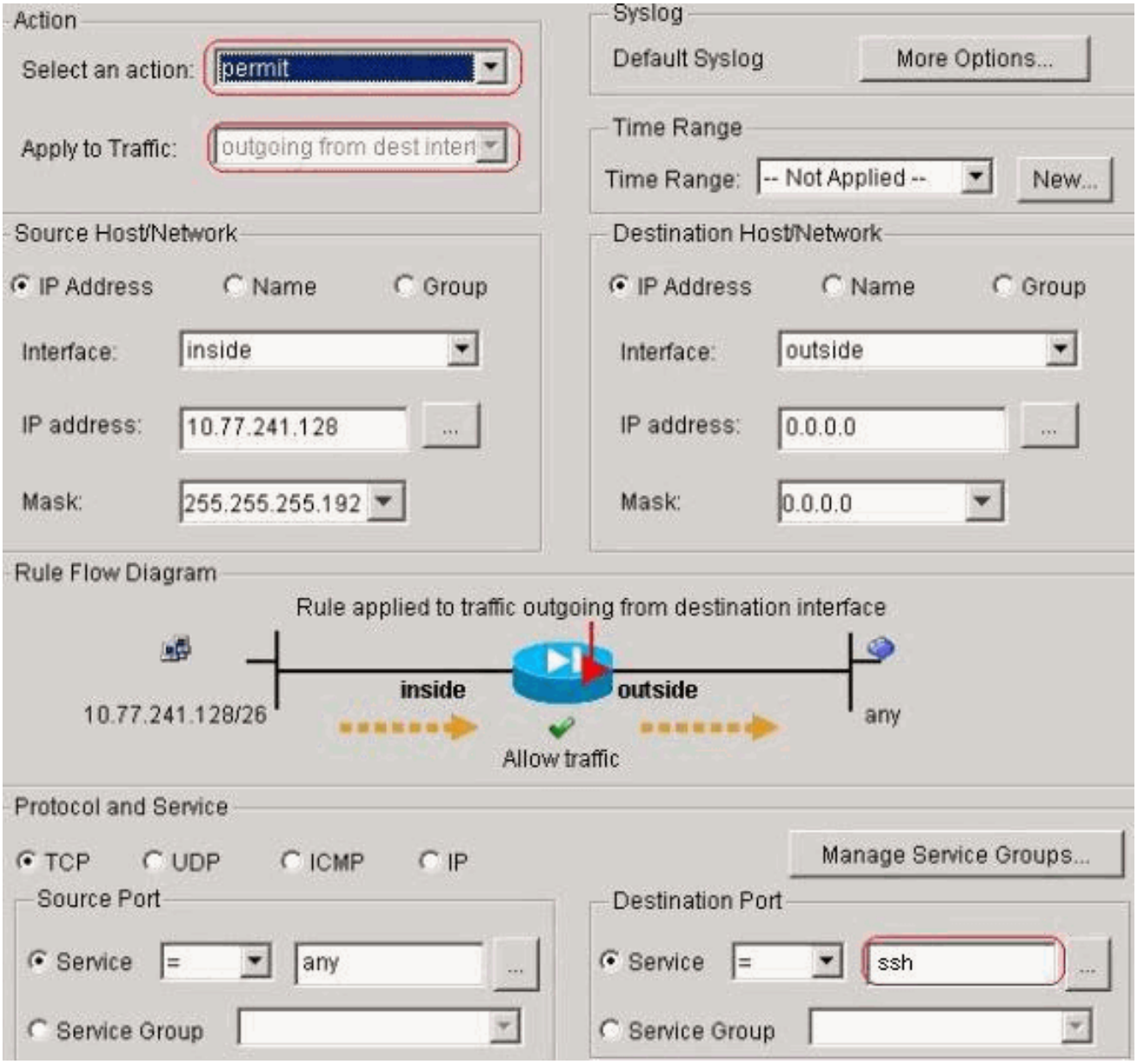
等效的CLI配置，如下所示：

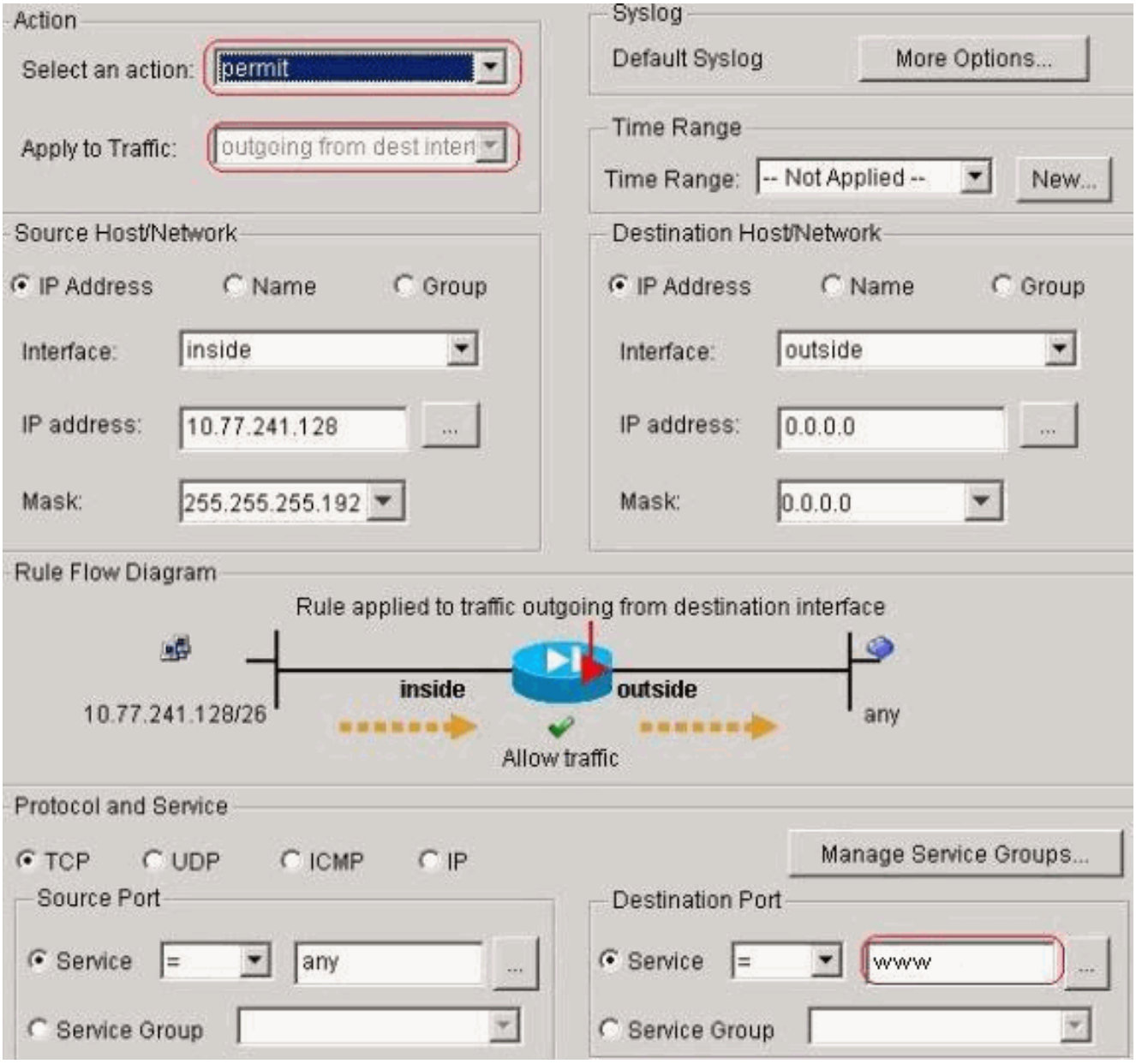
```
access-list inside_nat0_outbound extended permit ip 10.77.241.128 255.255.255.192 any
nat (inside) 0 access-list inside_nat0_outbound
```

3. **配置ACL**依序選擇「**Configuration > Security Policy > Access Rules**」，以設定ACL，如下所示。按一下**Add**以設定允許從網路10.77.241.128/26產生的Telnet流量傳送到任何目的地網路的ACL 101，並將其套用到外部介面上的傳出流量。



按一下「**OK**」（確定）。類似於ssh和http流量
：

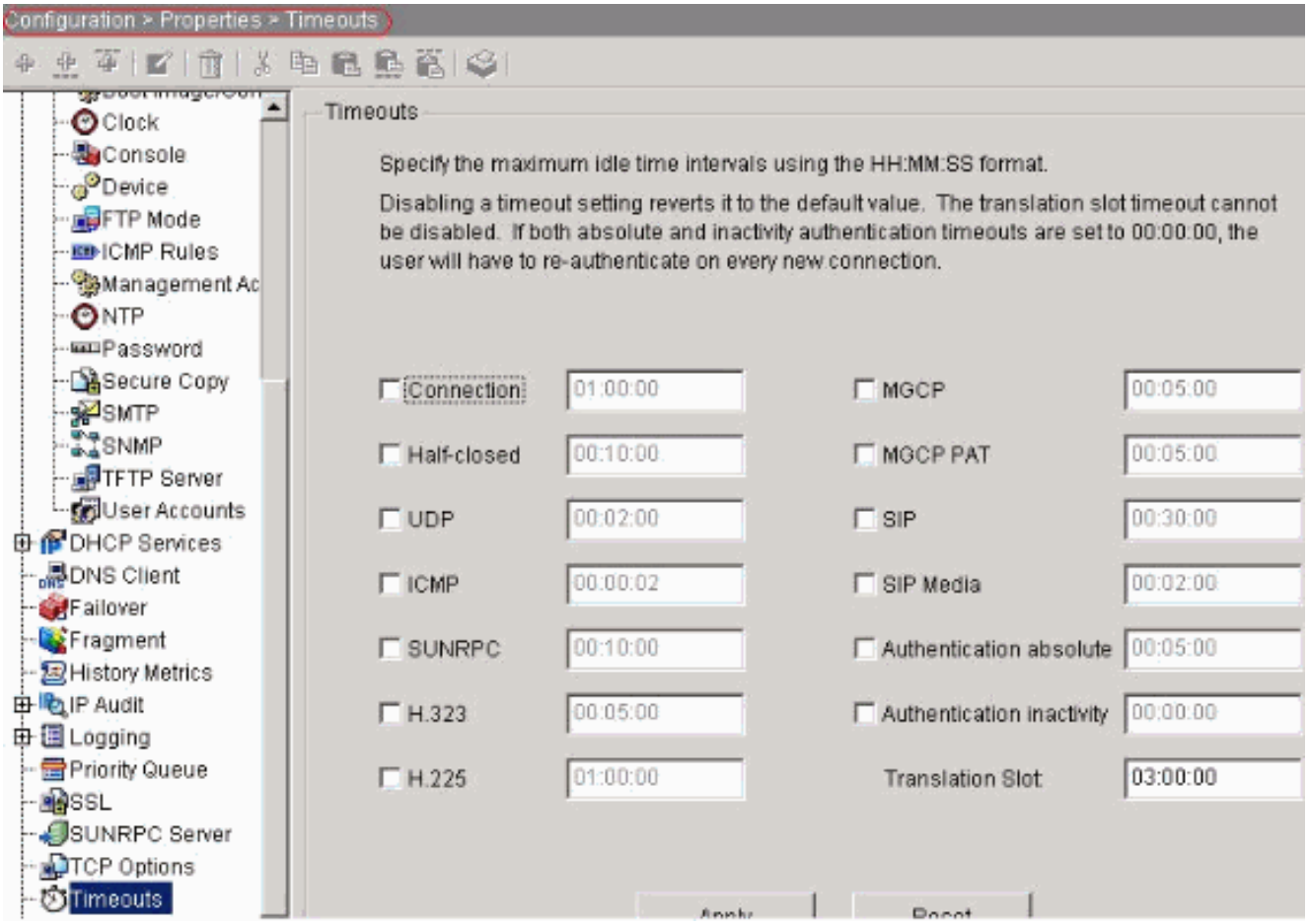

Action
Select an action:
permit
Apply to Traffic:
outgoing from dest inter
Syslog
Default Syslog
More Options...
Time Range
Time Range:
-- Not Applied --
New...
Source Host/Network
IP Address
Name
Group
Interface:
inside
IP address:
10.77.241.128
Mask:
255.255.255.192
Destination Host/Network
IP Address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



等效的CLI配置，如下所示：

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

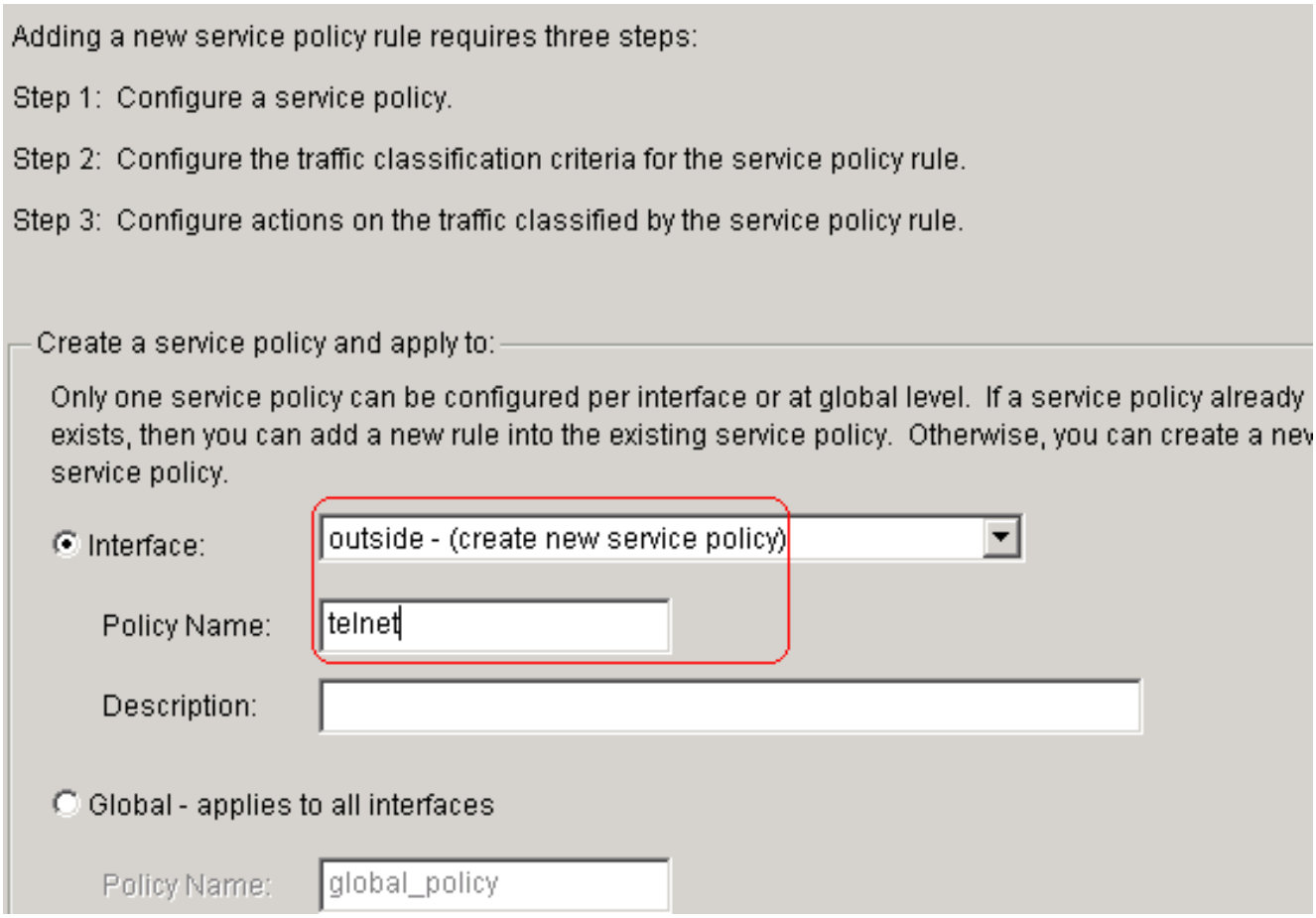
4. **配置超時**選擇**Configuration > Properties > Timeouts**以配置各種超時。在此情況中，保留所有超時的預設值。



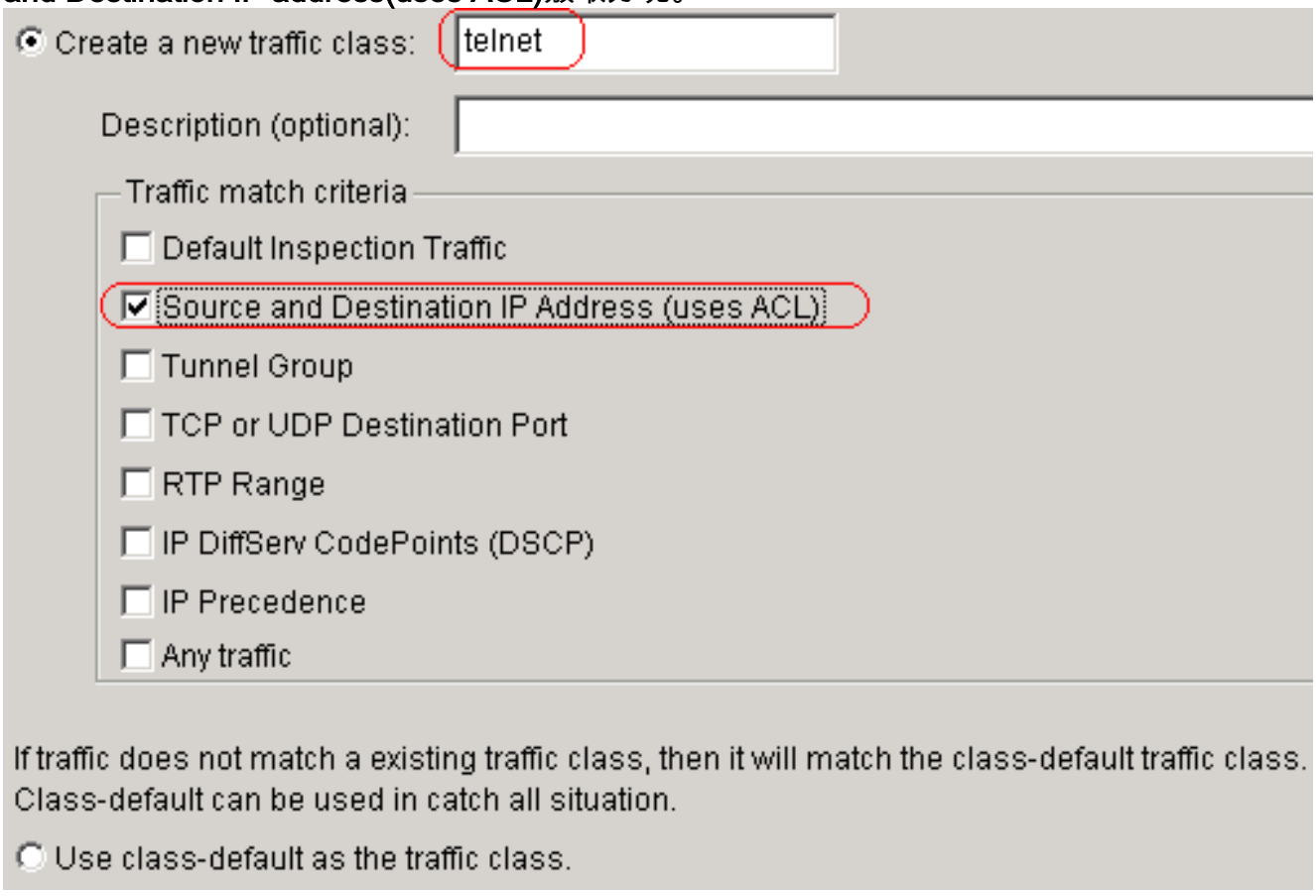
等效的CLI配置，如下所示：

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

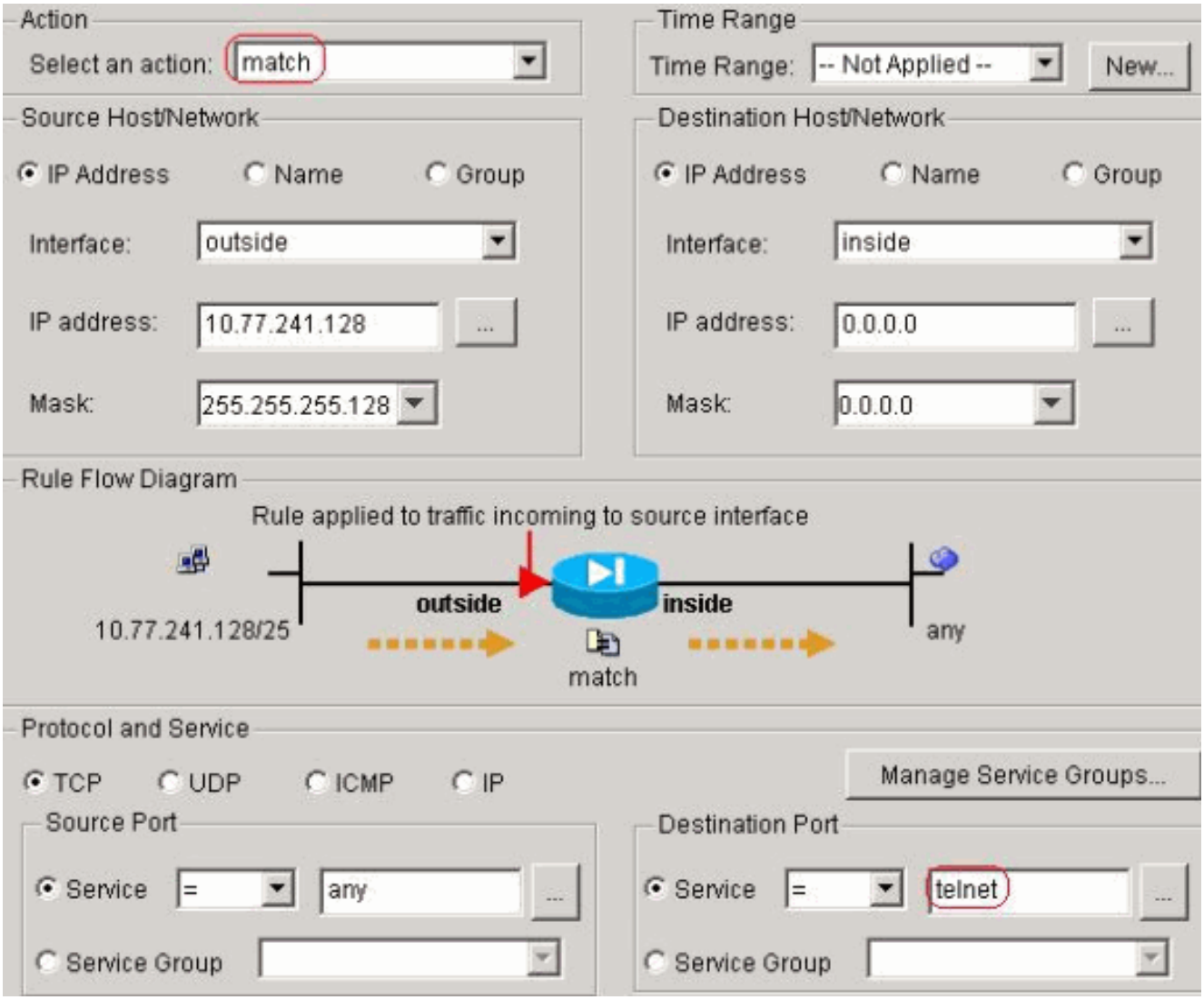
5. 配置**服務策略規則**。選擇**Configuration > Security Policy > Service Policy Rules > Add**以配置類對映、將TCP連線超時設定為10分鐘的策略對映，並在外部介面上應用服務策略，如下所示。選擇**Interface**單選按鈕以選擇**outside — （建立新服務策略）**（將建立該策略），並指定**telnet**作為策略名稱。



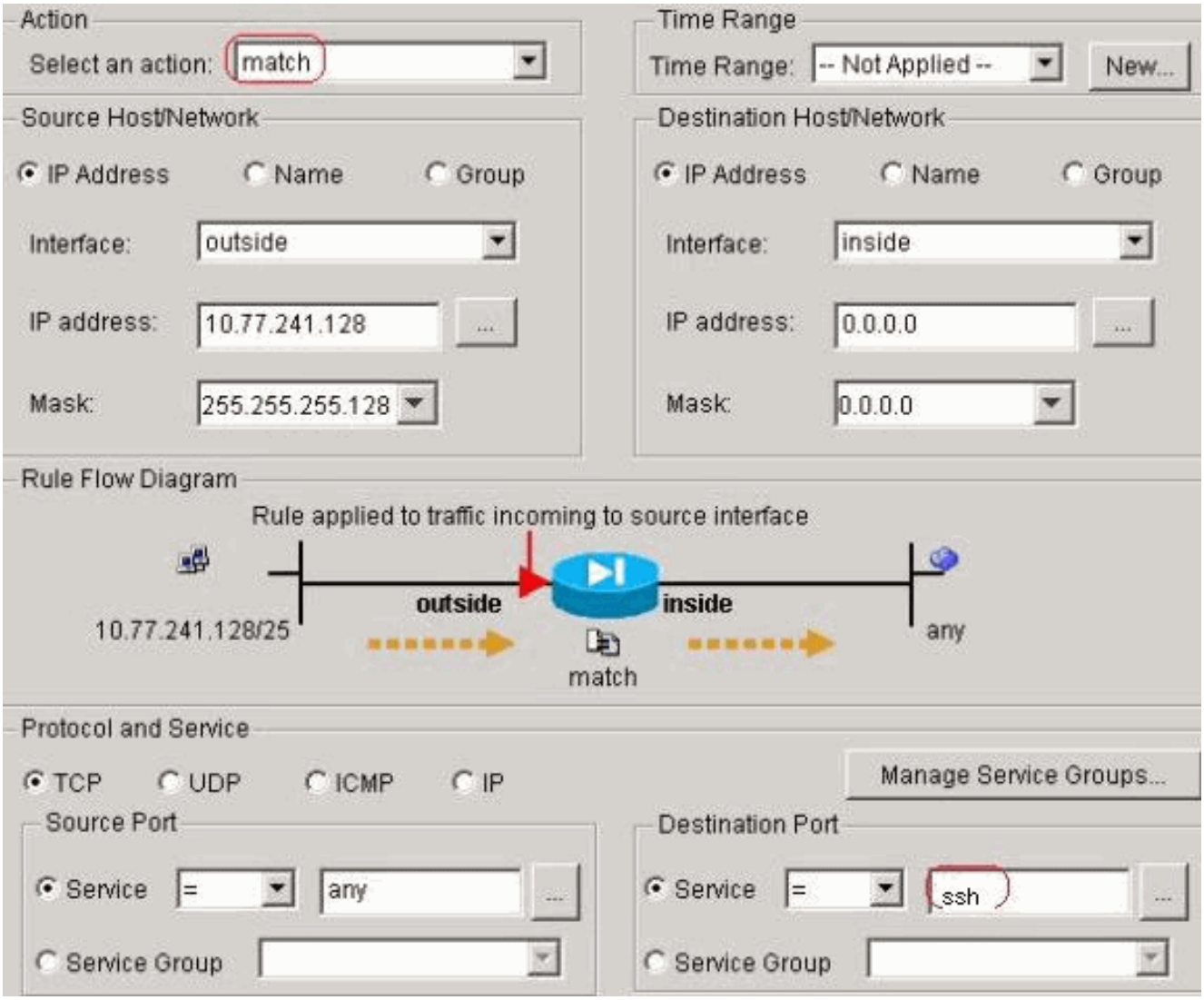
按「**Next**」（下一步）。建立一個類對映名稱telnet，然後在Traffic match條件中選擇**Source and Destination IP address(uses ACL)**覈取方塊。

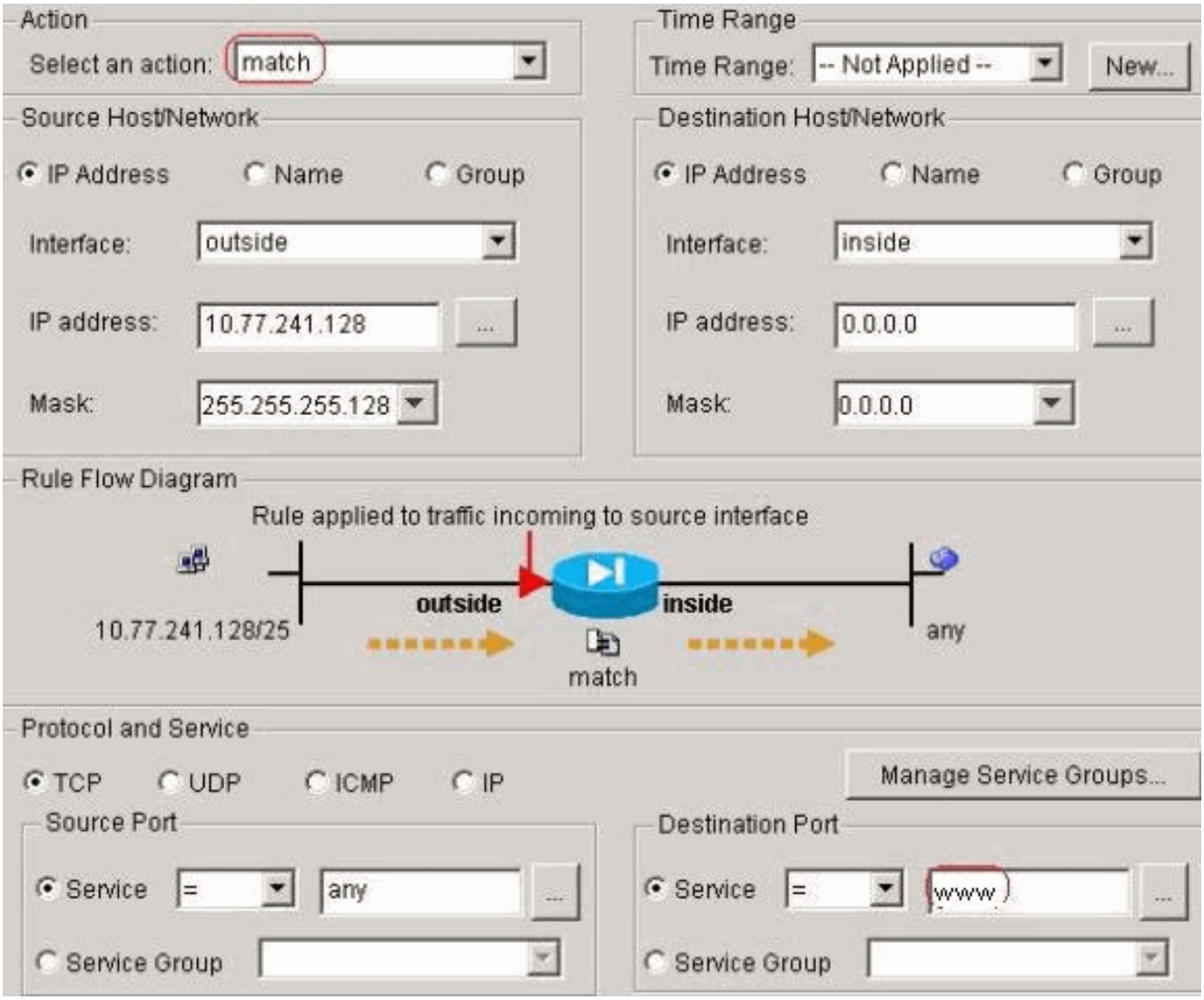


按「**Next**」（下一步）。建立ACL以匹配從網路10.77.241.128/26發往任何目標網路的Telnet流量，並將其應用到telnet類。

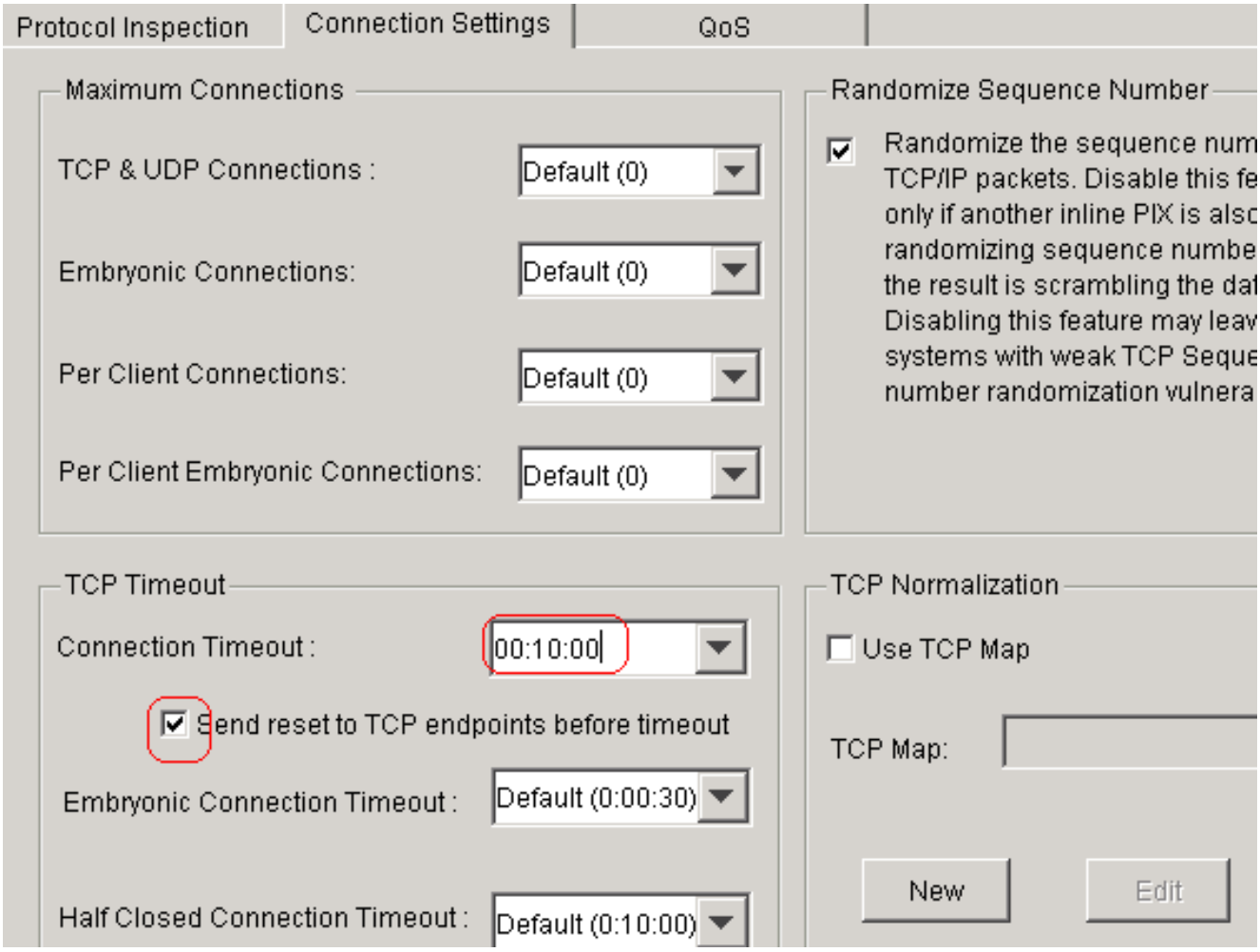


按「**Next**」（下一步）。類似於ssh和http流量：

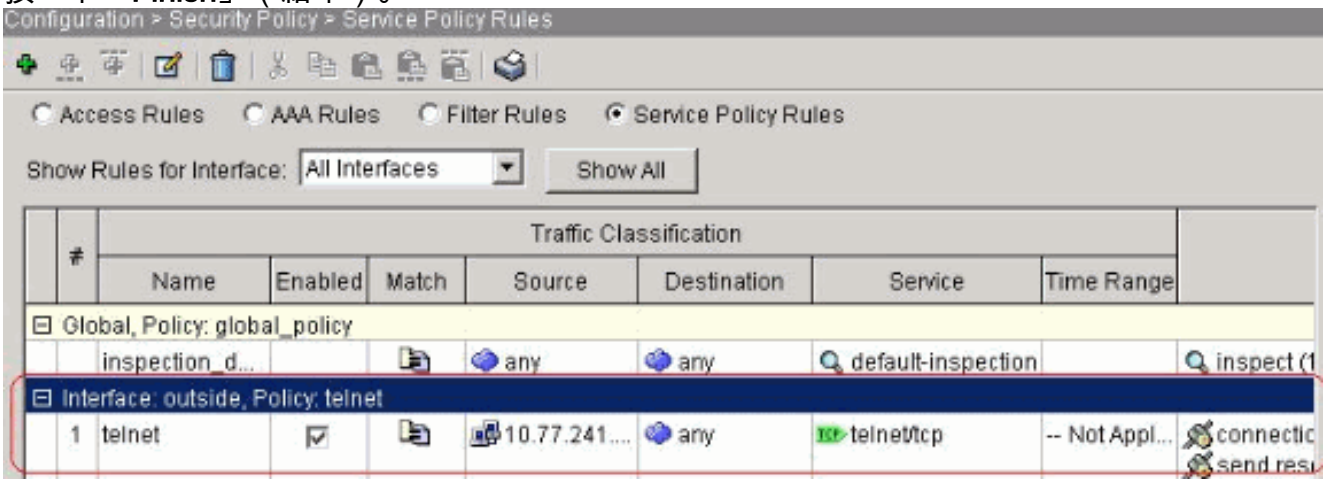

Action
Select an action: match
Time Range
Time Range: -- Not Applied --
New...
Source Host/Network
IP Address
Name
Group
Interface: outside
IP address: 10.77.241.128
Mask: 255.255.255.128
Destination Host/Network
IP Address
Name
Group
Interface: inside
IP address: 0.0.0.0
Mask: 0.0.0.0
Rule Flow Diagram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



選擇**Connection Settings**以將TCP連線超時設定為10分鐘，同時選擇**Send reset to TCP endpoints before timeout**覈取方塊。



按一下「**Finish**」（結束）。



等效的CLI配置，如下所示：

```
access-list outside_mpc_in extended permit tcp host 10.77.241.129  any eq telnet
access-list outside_mpc_in extended permit tcp host 10.77.241.129 any eq ssh
access-list outside_mpc_in extended permit tcp host 10.77.241.129 any eq www

class-map telnet
 description telnet
  match access-list outside_mpc_in

policy-map telnet
class telnet
  set connection timeout tcp 00:10:00 reset
service-policy telnet interface outside
```

Ebryonic超時

早期連線是半開連線，或者例如尚未完成三次握手。定義為ASA上的SYN超時；預設情況下，ASA上的SYN超時為30秒。以下是設定Embryonic Timeout的方式：

```
access-list emb_map extended permit tcp any any

class-map emb_map
match access-list emb_map

policy-map global_policy
class emb_map
set connection timeout embryonic 0:02:00

service-policy global_policy global
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**指令輸出的分析。

發出**show service-policy interface outside**命令以驗證您的設定。

```
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
```

發出show service-policy flow 命令，以驗證特定流量是否與服務原則設定相符。

此命令輸出顯示一個示例：

```
PIX#show service-policy flow tcp host 10.77.241.129 host 10.1.1.2 eq 23

   Global policy:
  Service-policy: global_policy

Interface outside:
  Service-policy: telnet
    Class-map: telnet
      Match: access-list 101
        Access rule: permit tcp 10.77.241.128 255.255.255.192 any eq telnet
      Action:
        Input flow:  set connection timeout tcp 0:10:00 reset
```

疑難排解

如果您發現連線超時無法與模組化策略框架(MPF)配合使用，請檢查TCP啟動連線。問題可能是源和目標IP地址顛倒，或者訪問清單中配置的IP地址在MPF中不匹配，以設定新的超時值或更改應用

程式的預設超時。根據連線發起建立訪問清單條目（源和目標），以便使用MPF設定連線超時。

相關資訊

- Cisco PIX 500系列安全裝置
- Cisco ASA 5500系列調適型安全裝置
- Cisco PIX防火牆軟體
- Cisco Secure PIX防火牆命令參考
- 安全產品現場通知（包括PIX）
- 要求建議 (RFC)