PIX/ASA 7.x及更高版本：使用Internet連線多個內部網路的配置示例

目錄

簡介

本文檔提供了使用命令列介面(CLI)或自適應安全裝置管理器(ASDM)5.x及更高版本連線到網際網路（或外部網路）的多個內部網路的PIX/ASA安全裝置7.x及更高版本的配置示例。

有關如何通過PIX/ASA建立和排除連線故障的資訊，請參閱通過思科安全裝置建立連線並排除連線故障。

有關常見PIX命令的資訊，請參閱在PIX上使用nat、global、static、conduit和access-list命令和埠重定向（轉發）。

注意：其他ASDM版本中的某些選項可能與ASDM 5.1中的選項不同。有關詳細資訊，請參閱ASDM文檔。

必要條件

需求

在PIX防火牆後面新增多個內部網路時，請記住以下幾點：

- PIX不支援輔助定址。
- 必須在PIX後面使用路由器，才能在現有網路和新新增的網路之間實現路由。
- 所有主機的預設網關都需要指向內部路由器。
- 在指向PIX的內部路由器上新增預設路由。
- 清除內部路由器上的地址解析協定(ARP)快取。

請參閱允許ASDM進行HTTPS訪問，以允許由ASDM配置裝置。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- PIX安全裝置515E，軟體版本7.1
- ASDM 5.1
- 採用Cisco IOS®軟體版本12.3(7)T的Cisco路由器

註：本文檔已通過PIX/ASA軟體版本8.x和Cisco IOS軟體版本12.4重新認證。

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。

相關產品

此配置還可以與Cisco ASA安全裝置7.x版及更高版本配合使用。

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(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

此配置中使用的IP編址方案在Internet上不能合法路由。這些地址是在實驗室環境中使用的RFC 1918地址。

背景資訊

在此場景中，有三個內部網路(10.1.1.0/24、10.2.1.0/24和10.3.1.0/24)通過PIX連線到Internet（或外部網路）。內部網路連線到PIX的內部介面。Internet連線是通過連線到PIX外部介面的路由器進行的。PIX的IP地址為172.16.1.1/24。

靜態路由用於將資料包從內部網路路由到Internet，反之亦然。除了使用靜態路由，您還可以使用動態路由協定，如路由資訊協定(RIP)或開放最短路徑優先(OSPF)。

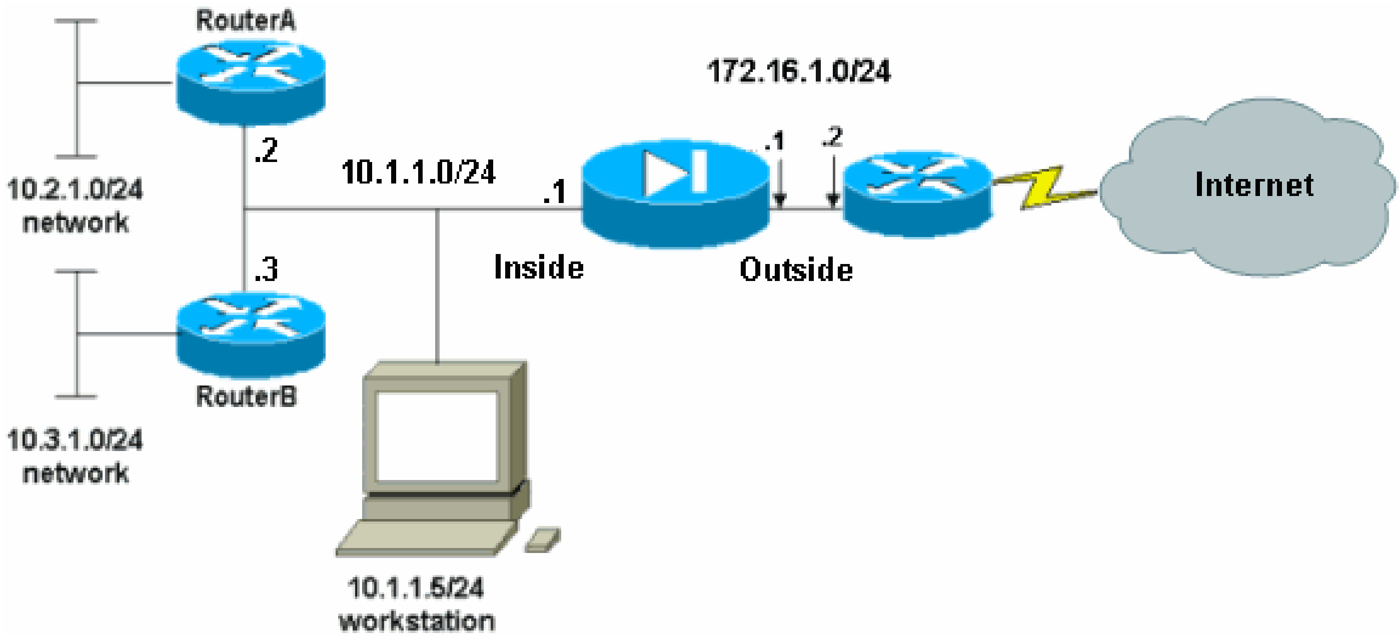
內部主機使用動態NAT（IP地址池 — 172.16.1.5到172.16.1.10）將PIX上的內部網路轉換為網際網路進行通訊。 如果IP地址池耗盡，PIX將PAT（使用IP地址172.16.1.4）內部主機訪問Internet。

有關NAT/PAT的詳細資訊，請參閱PIX/ASA 7.x NAT和PAT語句。

注意：如果靜態NAT使用外部IP(global_IP)地址進行轉換，則可能導致轉換。因此，在靜態轉換中使用關鍵字interface而不是IP地址。

網路圖表

本檔案會使用以下網路設定：



10.1.1.0網路中主機的預設網關指向RouterA。在RouterB上新增了一條指向RouterA的預設路由。RouterA具有指向PIX內部介面的預設路由。

組態

本檔案會使用以下設定：

- 路由器A配置
- RouterB組態
- PIX安全裝置7.1配置使用ASDM配置PIXPIX安全裝置CLI配置

路由器A配置
```
RouterA#show running-config
Building configuration...

Current configuration : 1151 bytes
!
version 12.4
service config
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
```

```
interface Ethernet2/0
 ip address 10.2.1.1 255.255.255.0
 half-duplex
!

interface Ethernet2/1
 ip address 10.1.1.2 255.255.255.0
 half-duplex
!
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
!
!
line con 0
line aux 0
line vty 0 4
!
end
RouterA#
```

RouterB組態

```

RouterB#show running-config
Building configuration...
Current configuration : 1132 bytes
!
version 12.4
service config
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterB
!

interface FastEthernet0/0
 ip address 10.1.1.3 255.255.255.0
 speed auto
!

interface Ethernet1/0
 ip address 10.3.1.1 255.255.255.0
 half-duplex
!
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
end
RouterB#
```

如果要使用ASDM配置PIX安全裝置，但尚未引導裝置，請完成以下步驟：

1. 通過控制檯連線到PIX。
2. 在已清除的配置中，使用互動式提示來啟用ASDM以便從工作站10.1.1.5管理PIX。

PIX安全裝置7.1配置

```
Pre-configure Firewall now through interactive prompts
[yes]? yes
Firewall Mode [Routed]:
Enable password [<use current password>]: cisco
Allow password recovery [yes]?
Clock (UTC):
  Year [2005]:
  Month [Mar]:
  Day [15]:
  Time [05:40:35]: 14:45:00
Inside IP address: 10.1.1.1
Inside network mask: 255.255.255.0
Host name: OZ-PIX
Domain name: cisco.com
IP address of host running Device Manager: 10.1.1.5

The following configuration will be used:
         Enable password: cisco
         Allow password recovery: yes
         Clock (UTC): 14:45:00 Mar 15 2005
         Firewall Mode: Routed
         Inside IP address: 10.1.1.1
         Inside network mask: 255.255.255.0
         Host name: OZ-PIX
         Domain name: cisco.com
         IP address of host running Device Manager:
10.1.1.5

Use this configuration and write to flash? yes
         INFO: Security level for "inside" set to 100 by
default.
         Cryptochecksum: a0bff9bb aa3d815f c9fd269a
3f67fef5

965 bytes copied in 0.880 secs
         INFO: converting 'fixup protocol dns maximum-
length 512' to MPF commands
         INFO: converting 'fixup protocol ftp 21' to MPF
commands
         INFO: converting 'fixup protocol h323_h225
1720' to MPF commands
         INFO: converting 'fixup protocol h323_ras 1718-
1719' to MPF commands
         INFO: converting 'fixup protocol netbios 137-
138' to MPF commands
         INFO: converting 'fixup protocol rsh 514' to
MPF commands
         INFO: converting 'fixup protocol rtsp 554' to
MPF commands
         INFO: converting 'fixup protocol sip 5060' to
MPF commands
         INFO: converting 'fixup protocol skinny 2000'
to MPF commands
         INFO: converting 'fixup protocol smtp 25' to
MPF commands
         INFO: converting 'fixup protocol sqlnet 1521'
to MPF commands
```

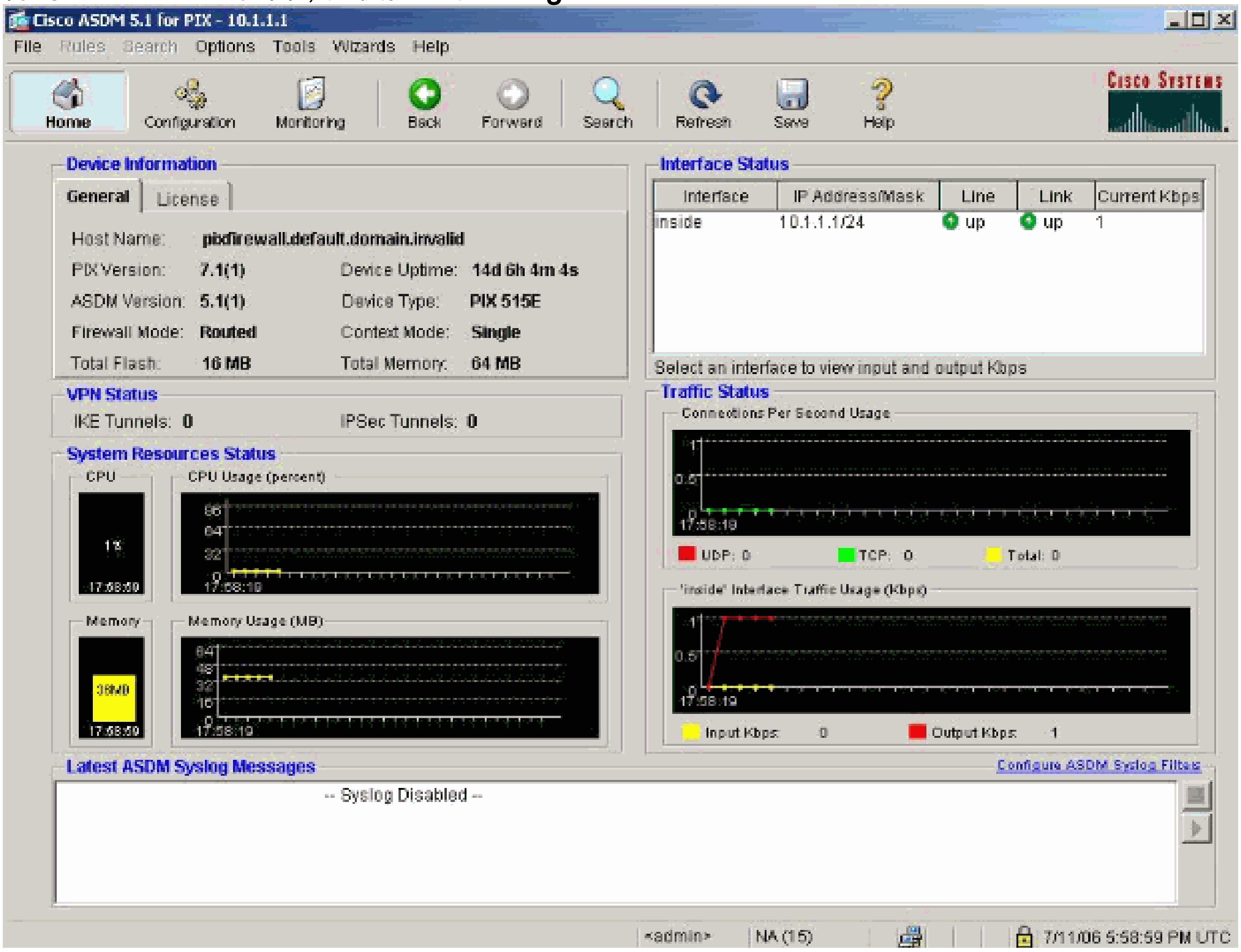
```
         INFO: converting 'fixup protocol sunrpc_udp
111' to MPF commands
         INFO: converting 'fixup protocol tftp 69' to
MPF commands
         INFO: converting 'fixup protocol sip udp 5060'
to MPF commands
         INFO: converting 'fixup protocol xdmcp 177' to
MPF commands

Type help or '?' for a list of available commands.
         OZ-PIX>
```

使用ASDM配置PIX

完成以下步驟，以便通過ASDM GUI進行配置：

1. 從工作站10.1.1.5開啟Web瀏覽器以使用ADSM(在本例中為https://10.1.1.1)。
2. 在憑證提示中按一下**yes**。
3. 使用先前配置的啟用密碼登入。
4. 如果這是第一次在PC上運行ASDM，系統將提示您使用ASDM啟動程式或ASDM作為Java應用。在此示例中，選擇並安裝了ASDM啟動器。
5. 轉到ASDM Home視窗，然後按一下**Configuration**。



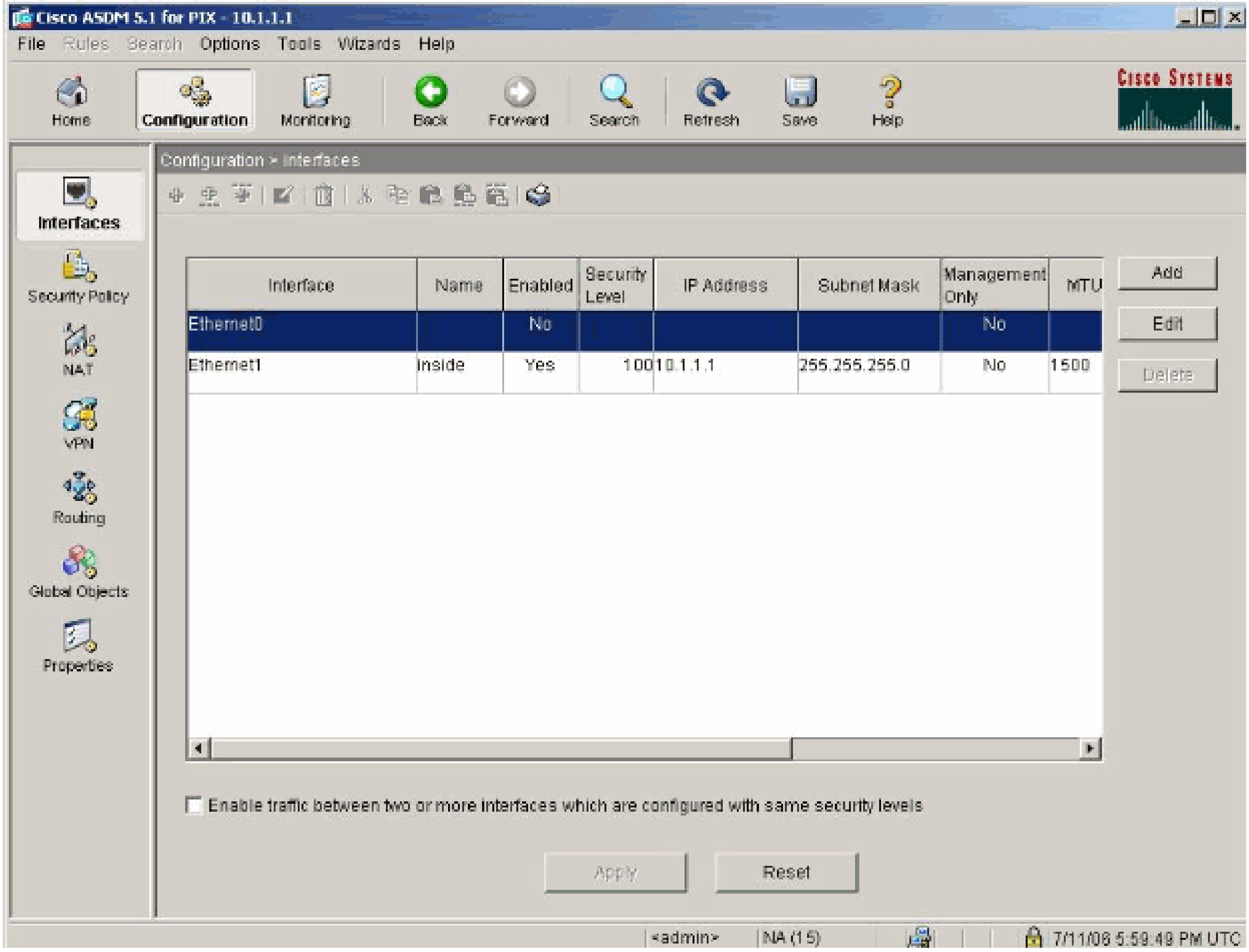
Host Name: pixfirewall.default.domain.invalid
PIX Version: 7.1(1)   Device Uptime: 14d 6h 4m 4s
ASDM Version: 5.1(1)   Device Type: PIX 515E
Firewall Mode: Routed   Context Mode: Single
Total Flash: 16 MB   Total Memory: 64 MB

IKE Tunnels: 0   IPSec Tunnels: 0

Interface	IP Address/Mask	Line	Link	Current Kbps
inside	10.1.1.1/24	up	up	1

Select an interface to view input and output Kbps

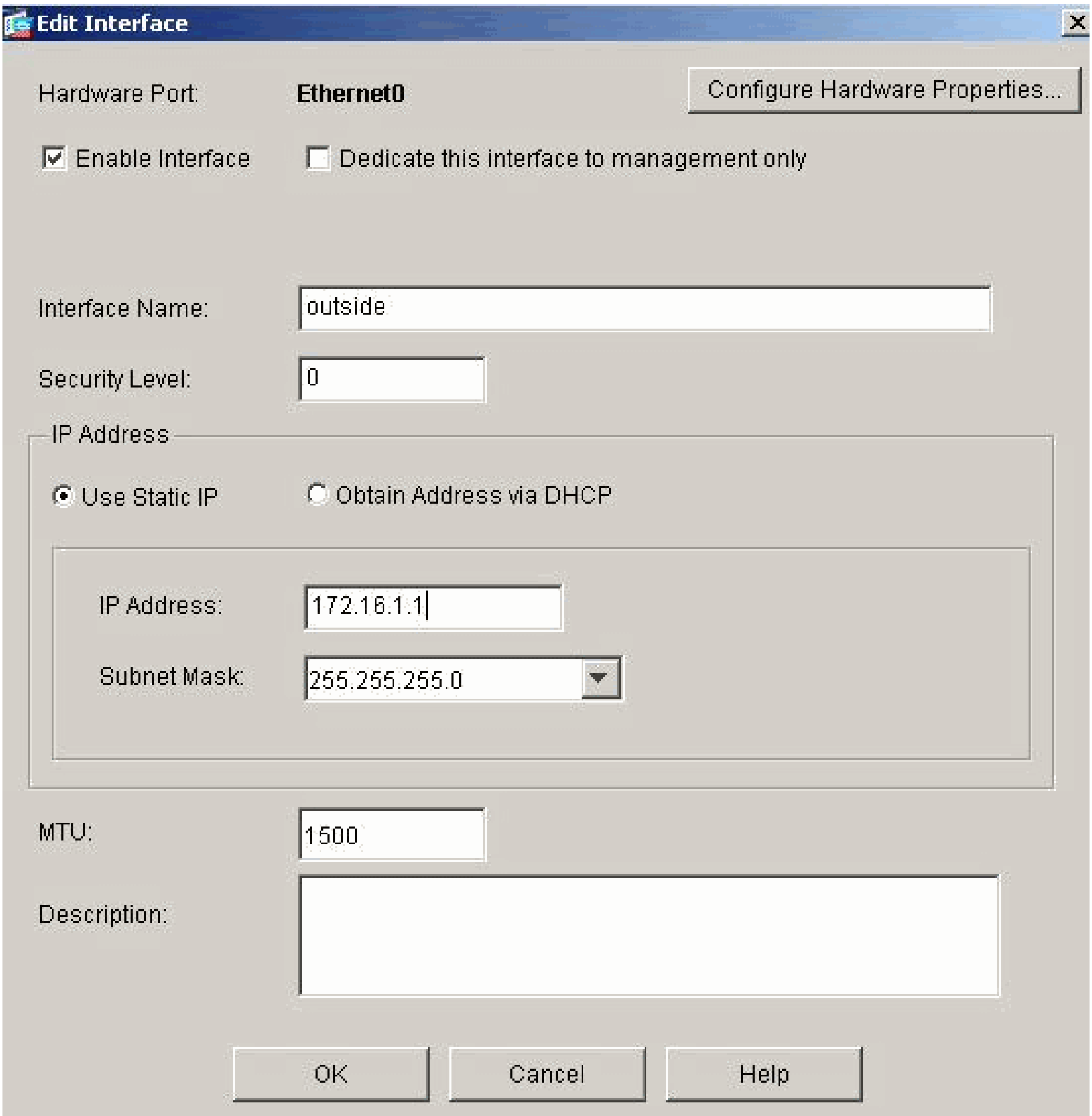
6. 選擇**Interface > Edit**以配置外部介面。



Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU
Ethernet0		No				No	
Ethernet1	inside	Yes	100	10.1.1.1	255.255.255.0	No	1500

☐ Enable traffic between two or more interfaces which are configured with same security levels

7. 輸入介面詳細資訊，完成後按一下**OK**。



Edit Interface

Hardware Port: Ethernet0

Configure Hardware Properties...

☑ 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: 172.16.1.1

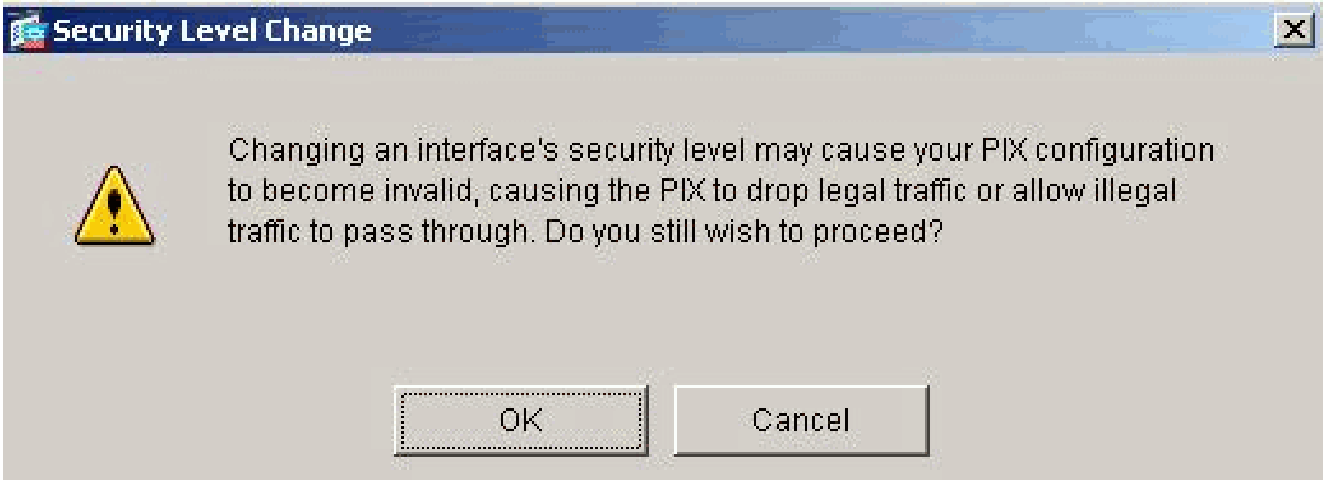
Subnet Mask: 255.255.255.0

MTU: 1500

Description:

OK Cancel Help

8. 在Security Level Change對話方塊中按一下**OK**。

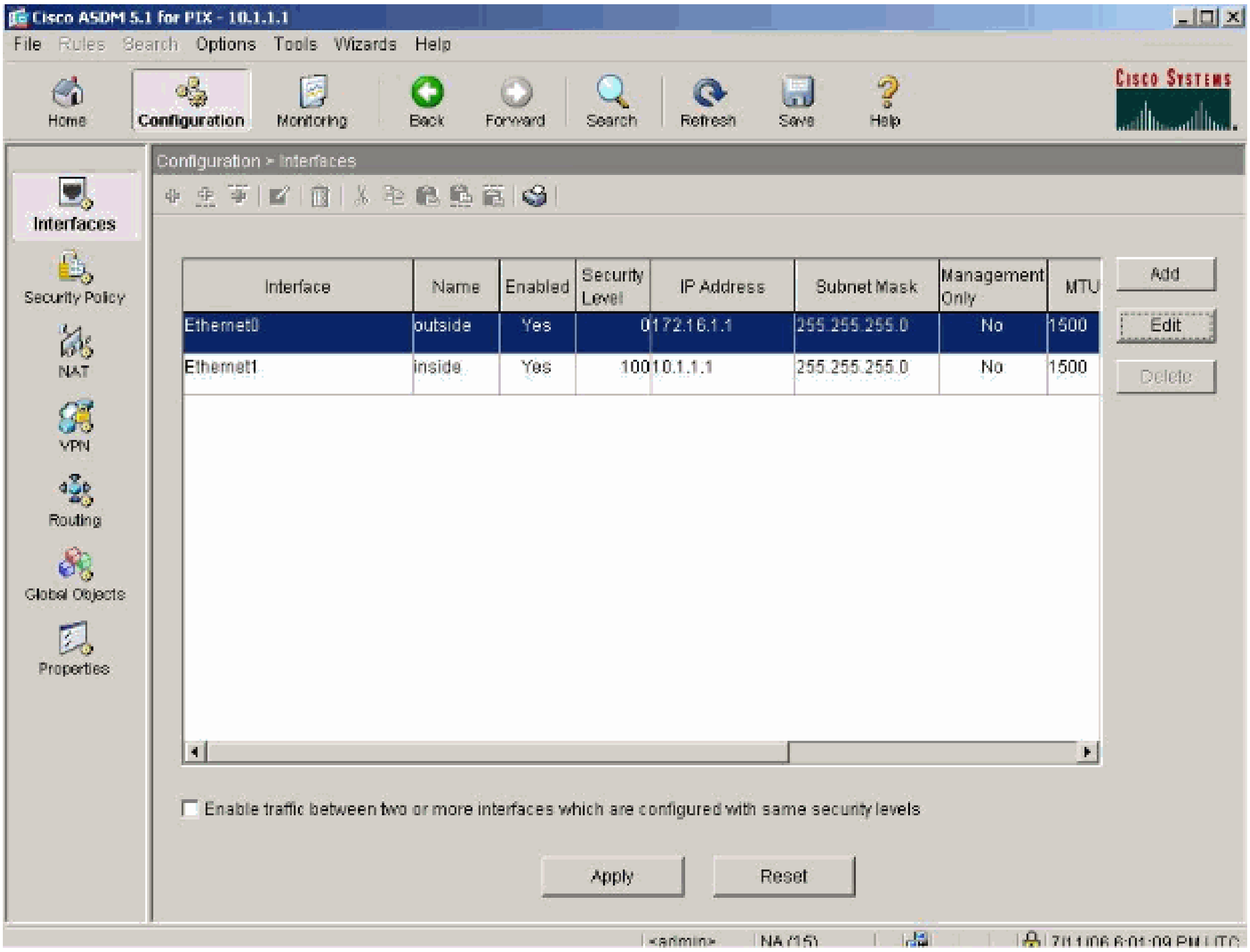


Security Level Change

Changing an interface's security level may cause your PIX configuration to become invalid, causing the PIX to drop legal traffic or allow illegal traffic to pass through. Do you still wish to proceed?

OK Cancel

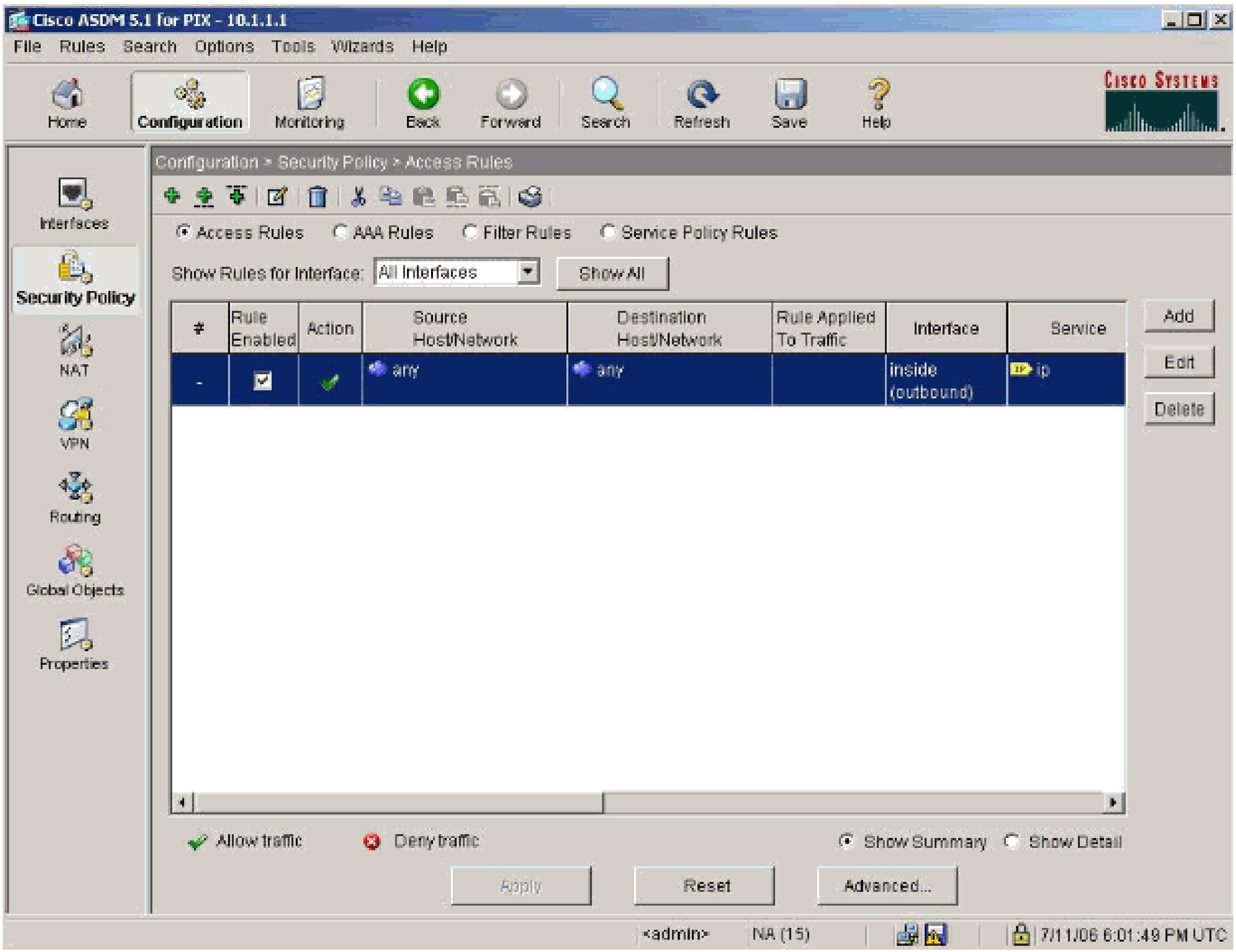
9. 按一下「**Apply**」以接受介面組態。該配置也將推到PIX上。



Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU
Ethernet0	outside	Yes	0	172.16.1.1	255.255.255.0	No	1500
Ethernet1	inside	Yes	100	10.1.1.1	255.255.255.0	No	1500

□ Enable traffic between two or more interfaces which are configured with same security levels

10. 在Features（功能）頁籤上選擇**Security Policy**（安全策略），以複查使用的安全策略規則。在本示例中，使用預設內部規則。



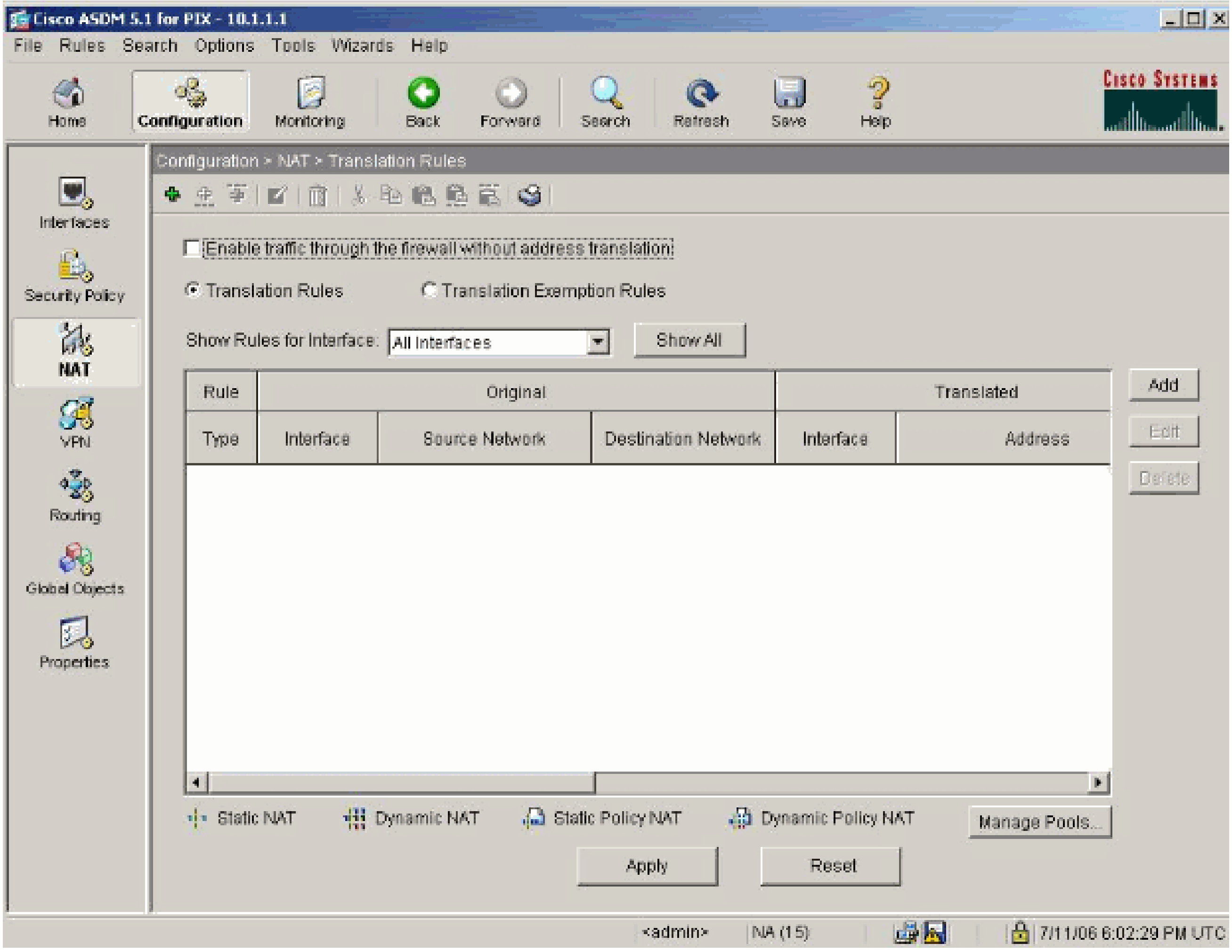
● Access Rules ○ AAA Rules ○ Filter Rules ○ Service Policy Rules

Show Rules for Interface: All Interfaces

#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Rule Applied To Traffic	Interface	Service
-	☑	✓	any	any		inside (outbound)	ip

● Show Summary ○ Show Detail

11. 本示例使用NAT。取消選中**Enable traffic through the firewall without address translation**覈取方塊，然後按一下**Add**以配置NAT規則。



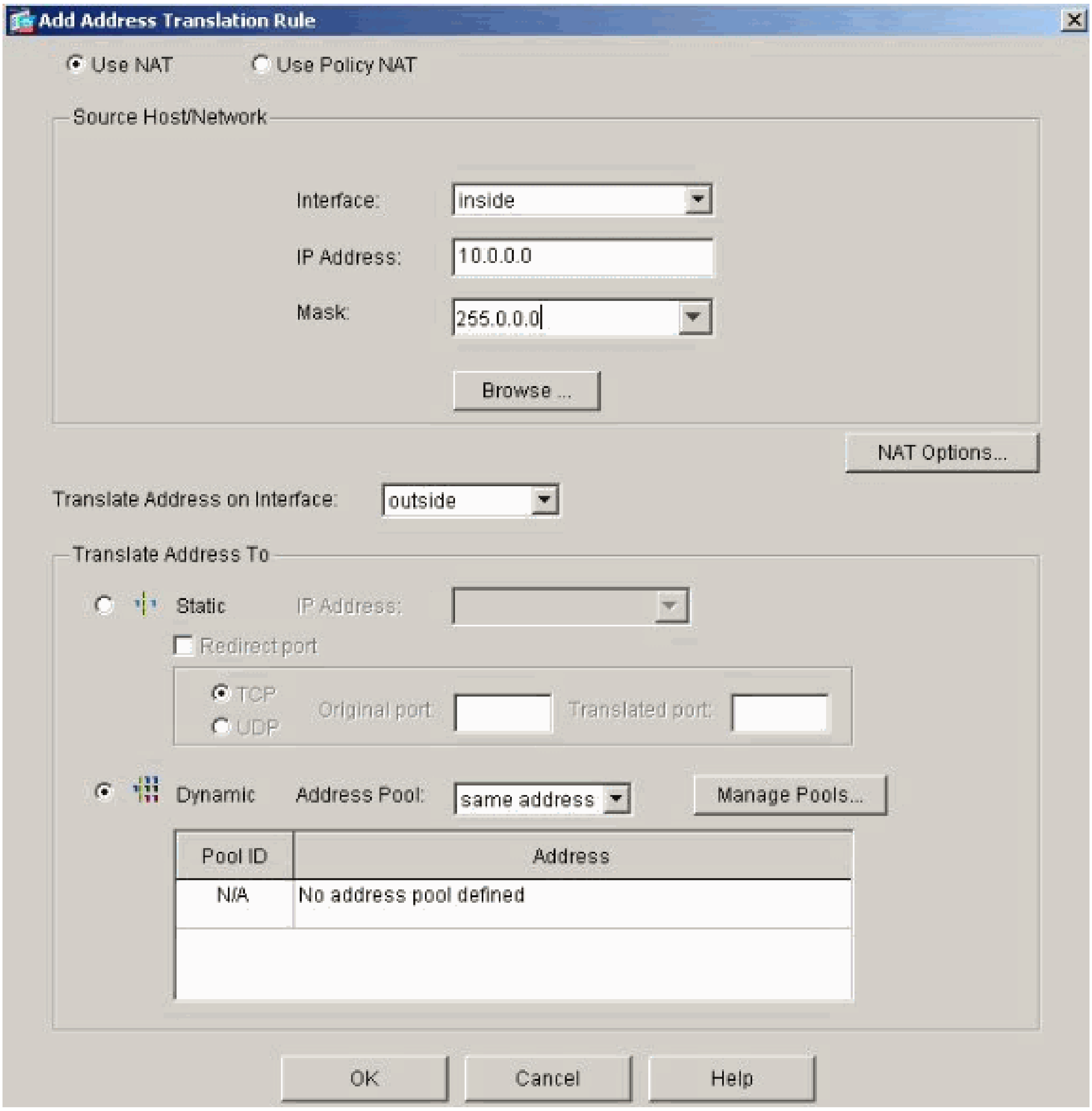
□ Enable traffic through the firewall without address translation

● Translation Rules ○ Translation Exemption Rules

Show Rules for Interface: All Interfaces Show All

Rule	Original			Translated	
Type	Interface	Source Network	Destination Network	Interface	Address

12. 配置源網路。在本示例中，10.0.0.0用於IP地址，255.0.0.0用於掩碼。按一下**Manage Pools**以定義NAT池地址。



Add Address Translation Rule

● Use NAT ○ Use Policy NAT

Source Host/Network

Interface: inside

IP Address: 10.0.0.0

Mask: 255.0.0.0

Translate Address on Interface: outside

Translate Address To

○ Static IP Address:

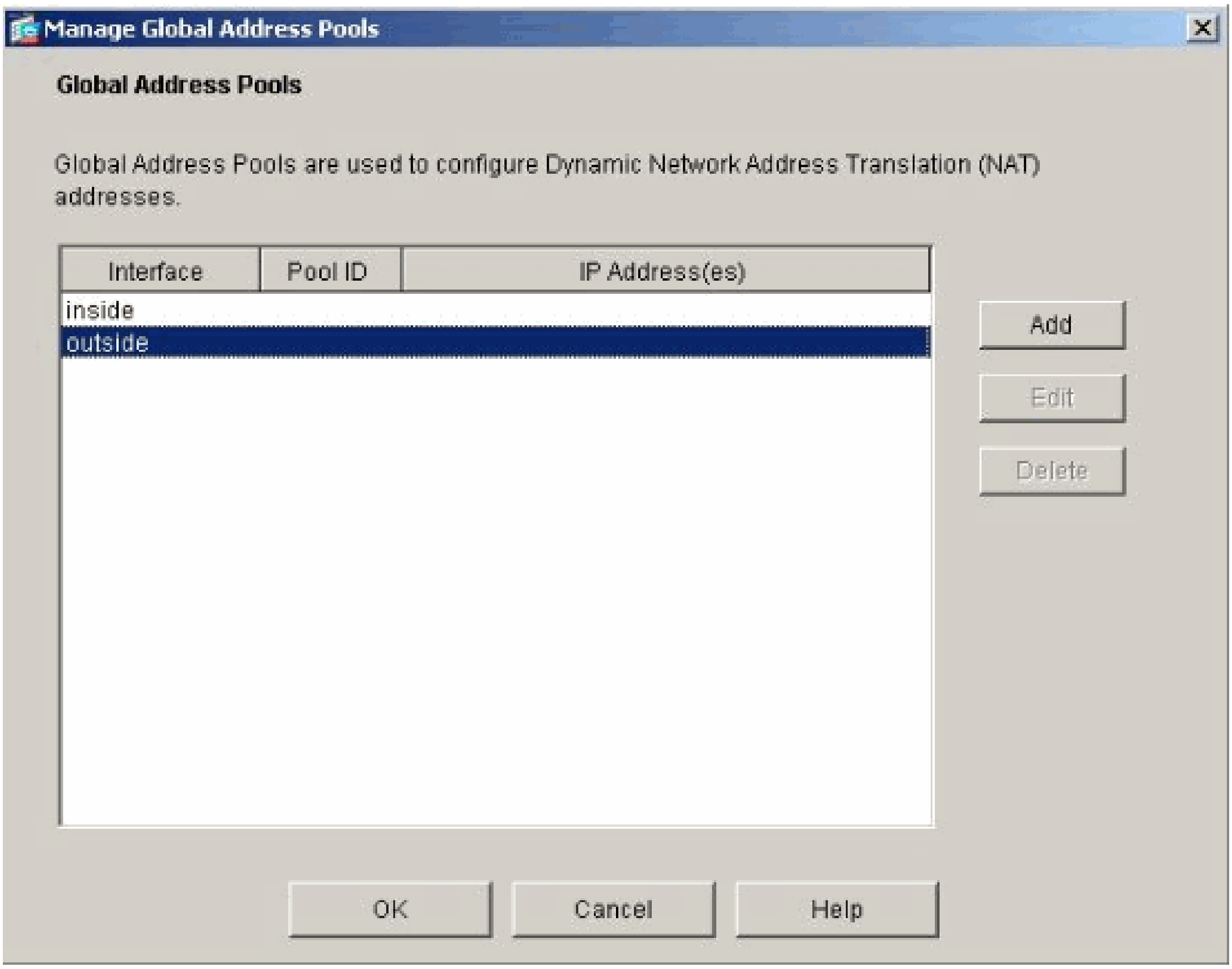
□ Redirect port

● TCP ○ UDP Original port: Translated port:

● Dynamic Address Pool: same address

Pool ID	Address
N/A	No address pool defined

13. 選擇外部介面，然後按一下**Add**。



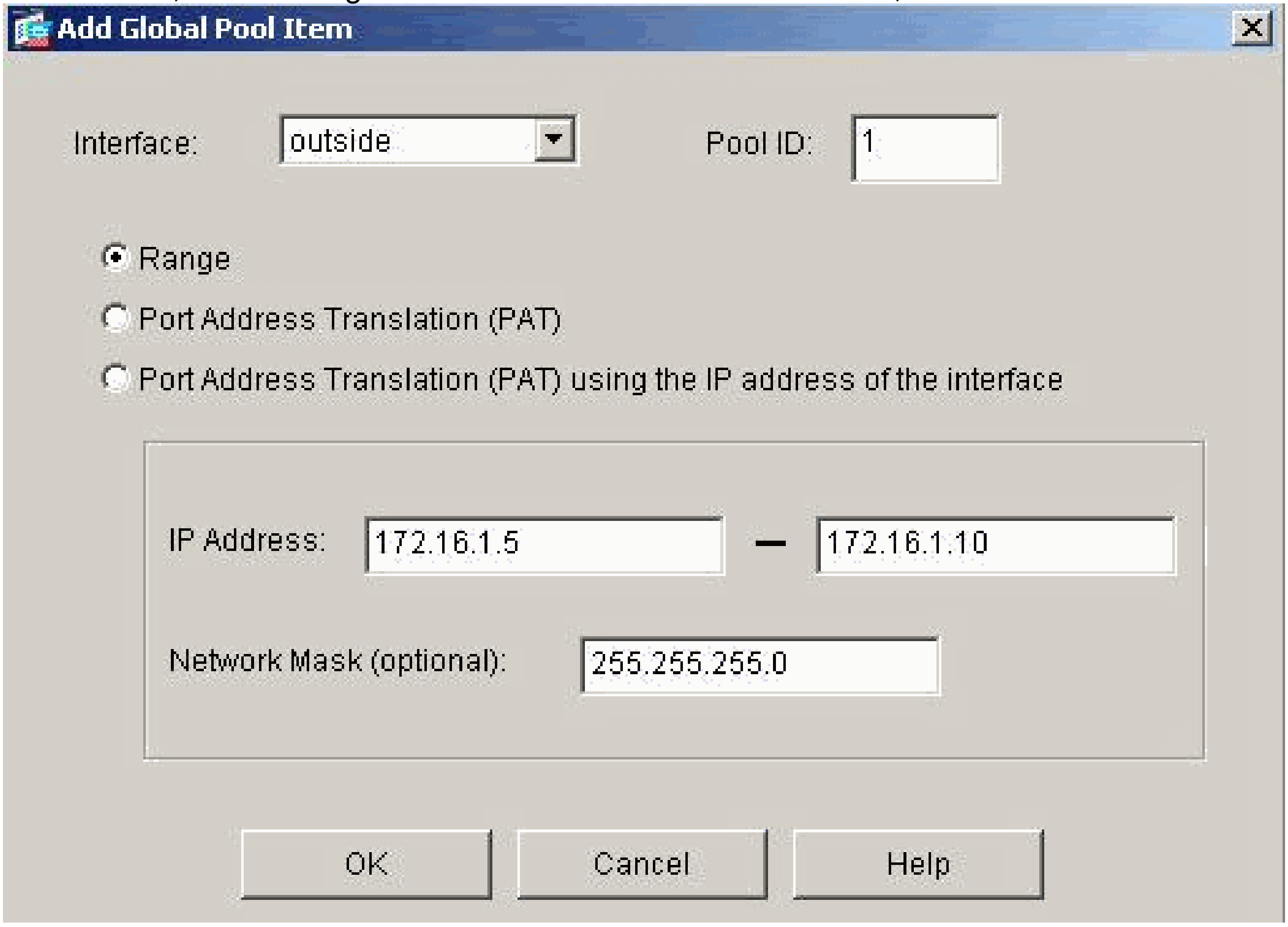
Manage Global Address Pools

Global Address Pools

Global Address Pools are used to configure Dynamic Network Address Translation (NAT) addresses.

Interface	Pool ID	IP Address(es)
inside		
outside		

14. 在此示例中，配置了Range和PAT地址池。配置範圍NAT池地址，然後按一下**OK**。



Add Global Pool Item

Interface: outside

Pool ID: 1

● Range

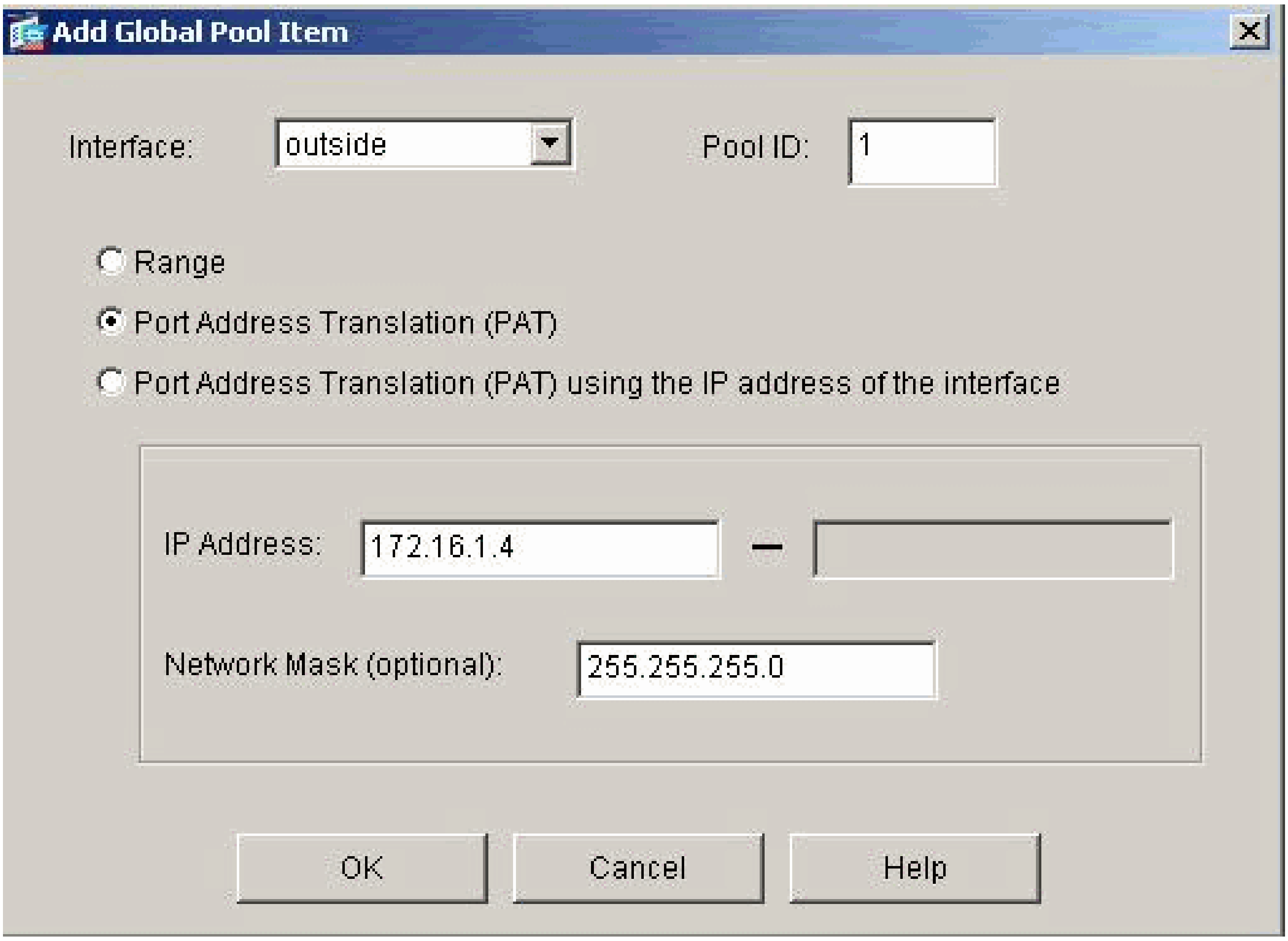
○ Port Address Translation (PAT)

○ Port Address Translation (PAT) using the IP address of the interface

IP Address: 172.16.1.5 – 172.16.1.10

Network Mask (optional): 255.255.255.0

15. 在步驟13中選擇外部介面以配置PAT地址。按一下「**OK**」



Add Global Pool Item

Interface: outside

Pool ID: 1

○ Range

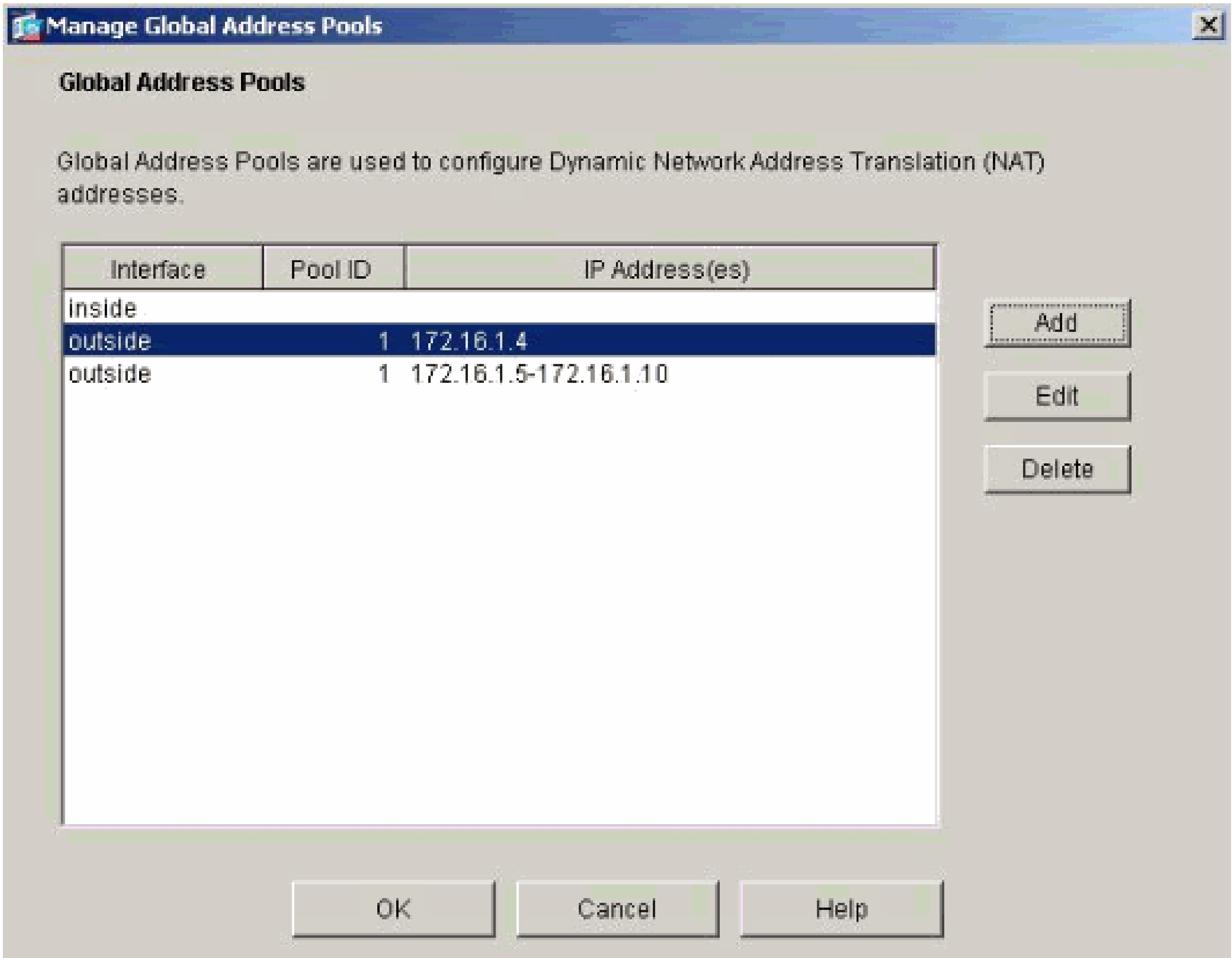
● Port Address Translation (PAT)

○ Port Address Translation (PAT) using the IP address of the interface

IP Address: 172.16.1.4 –

Network Mask (optional): 255.255.255.0

按一下「**OK**」以繼續。



Manage Global Address Pools

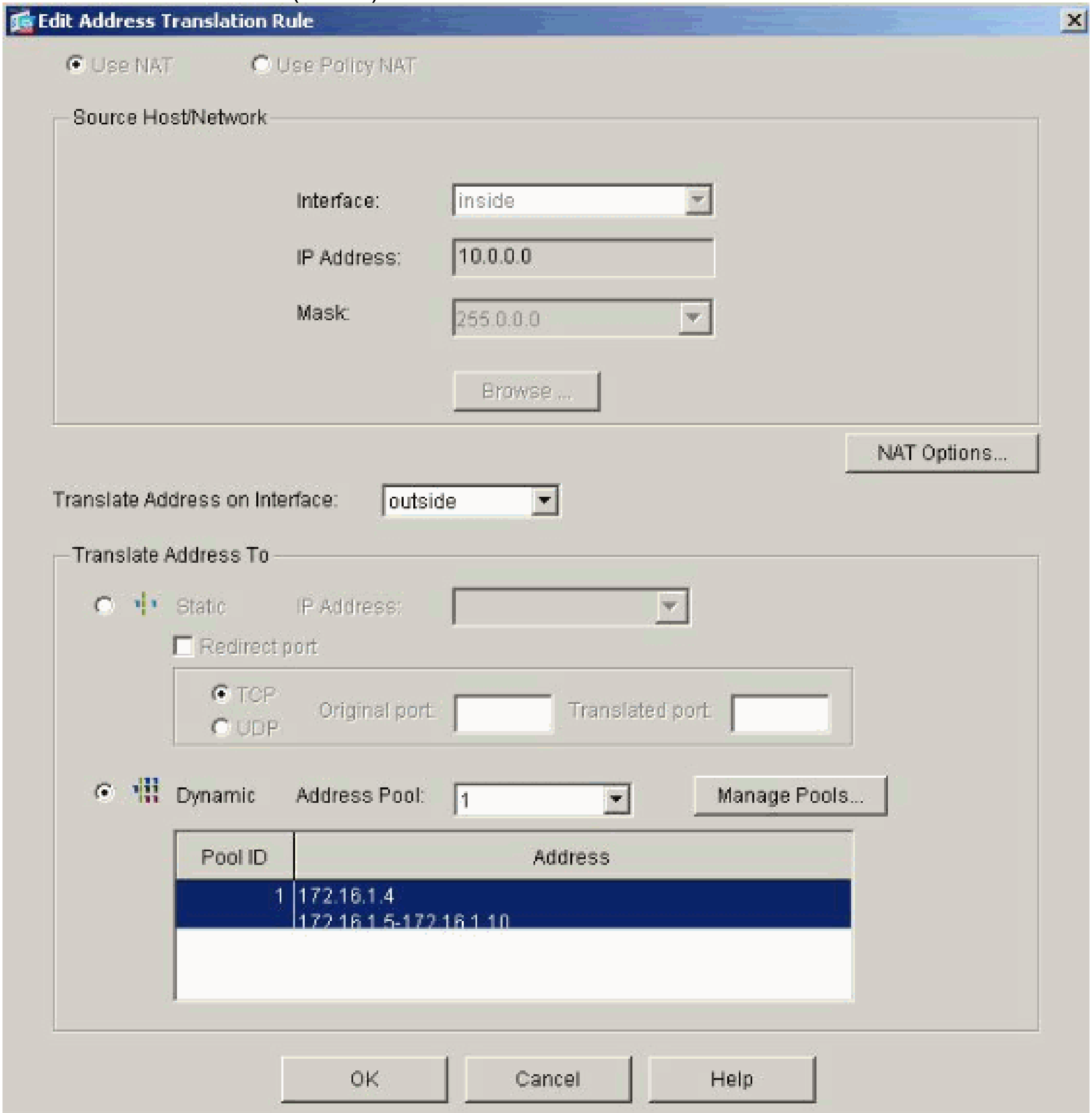
Global Address Pools

Global Address Pools are used to configure Dynamic Network Address Translation (NAT) addresses.

Interface	Pool ID	IP Address(es)
inside		
outside	1	172.16.1.4
outside	1	172.16.1.5-172.16.1.10

16. 在Edit Address Translation Rule（編輯地址轉換規則）視窗中，選擇要由配置的源網路使用

的池ID。按一下「OK」（確定）。



● Use NAT ○ Use Policy NAT

Source Host/Network

Interface: inside

IP Address: 10.0.0.0

Mask: 255.0.0.0

Translate Address on Interface: outside

Translate Address To

○ Static IP Address:

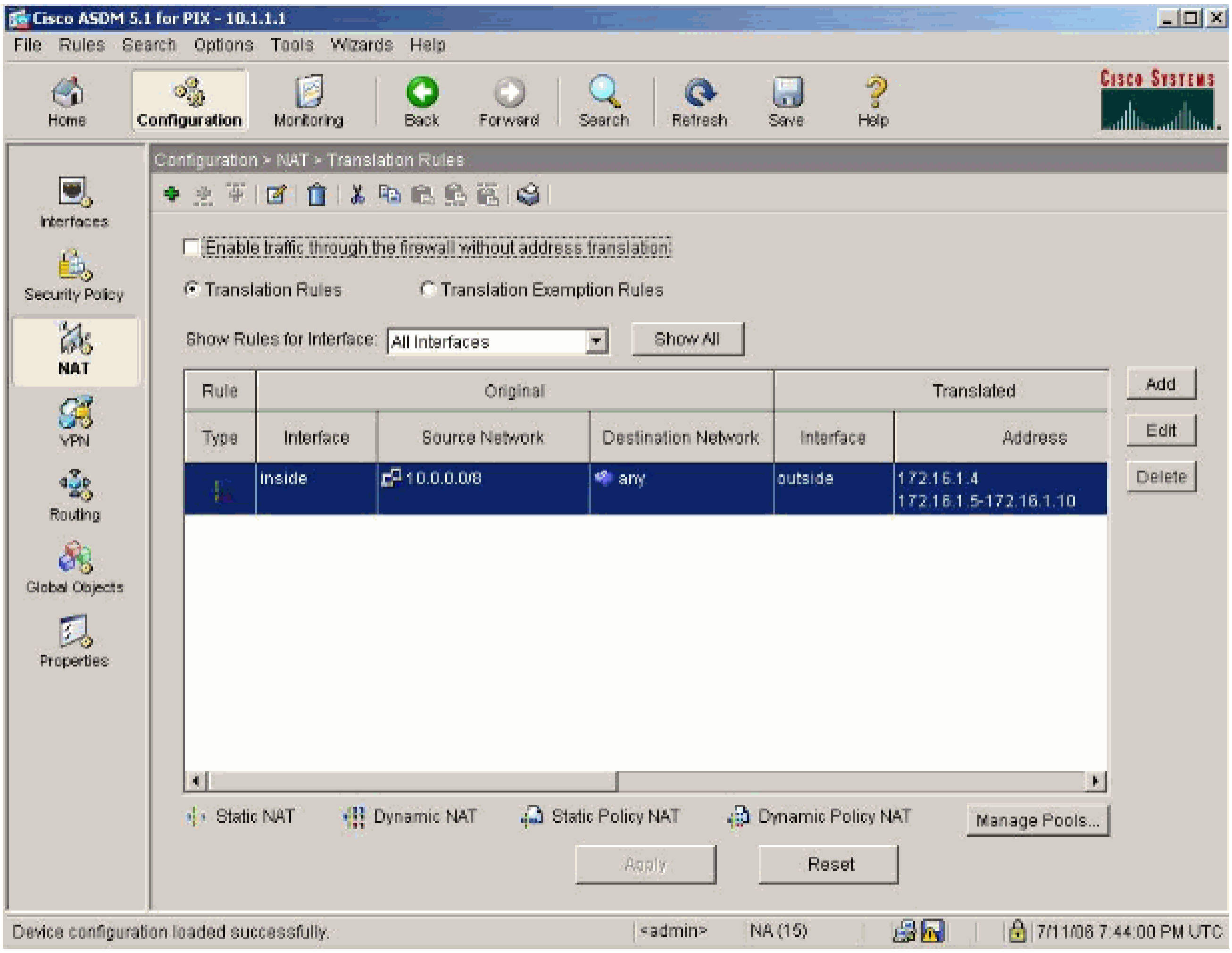
□ Redirect port

● TCP ○ UDP Original port: Translated port:

● Dynamic Address Pool: 1

Pool ID	Address
1	172.16.1.4 172.16.1.5-172.16.1.10

17. 按一下**Apply**以將配置的NAT規則推送到PIX。



Configuration > NAT > Translation Rules

□ Enable traffic through the firewall without address translation

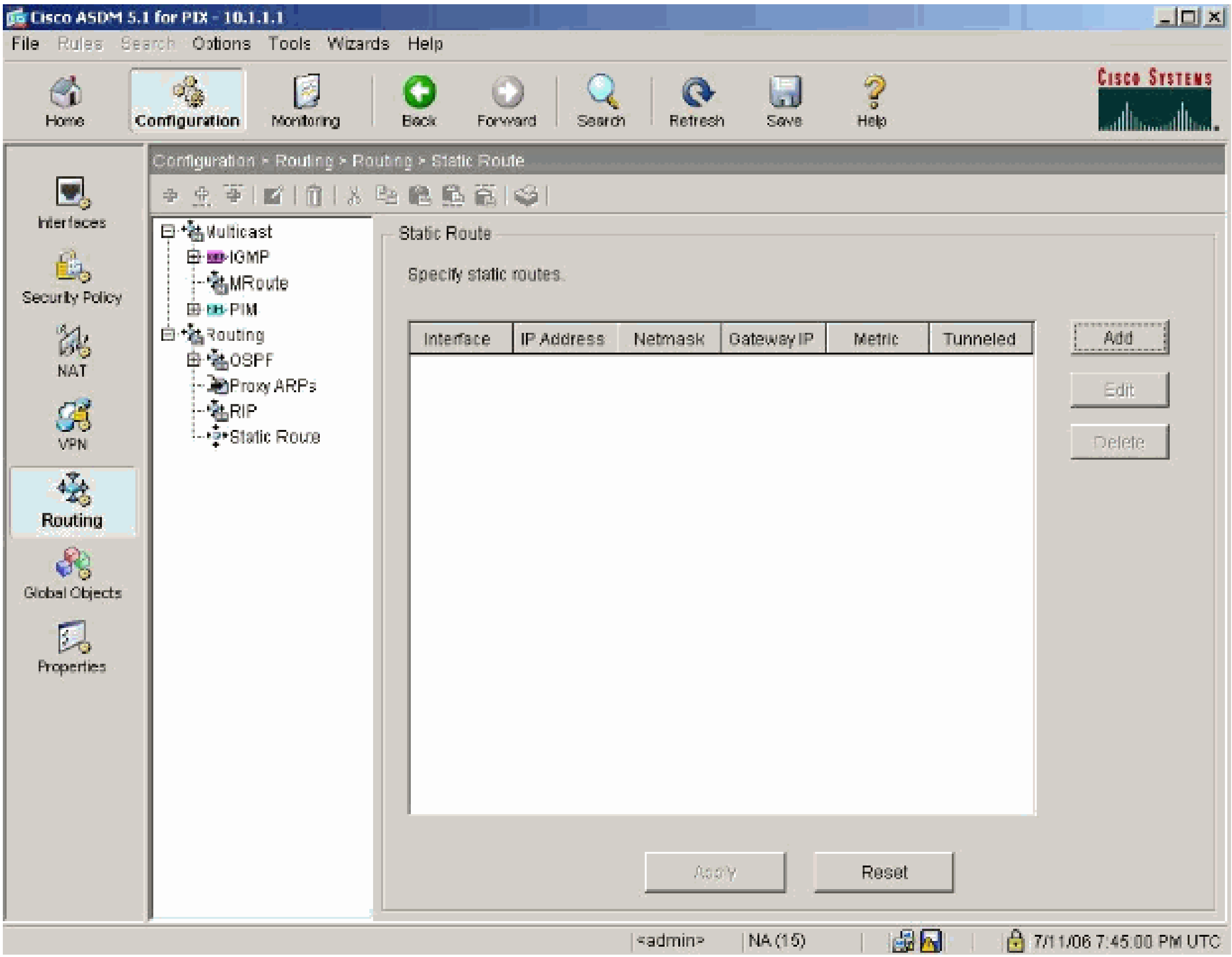
● Translation Rules ○ Translation Exemption Rules

Show Rules for Interface: All Interfaces

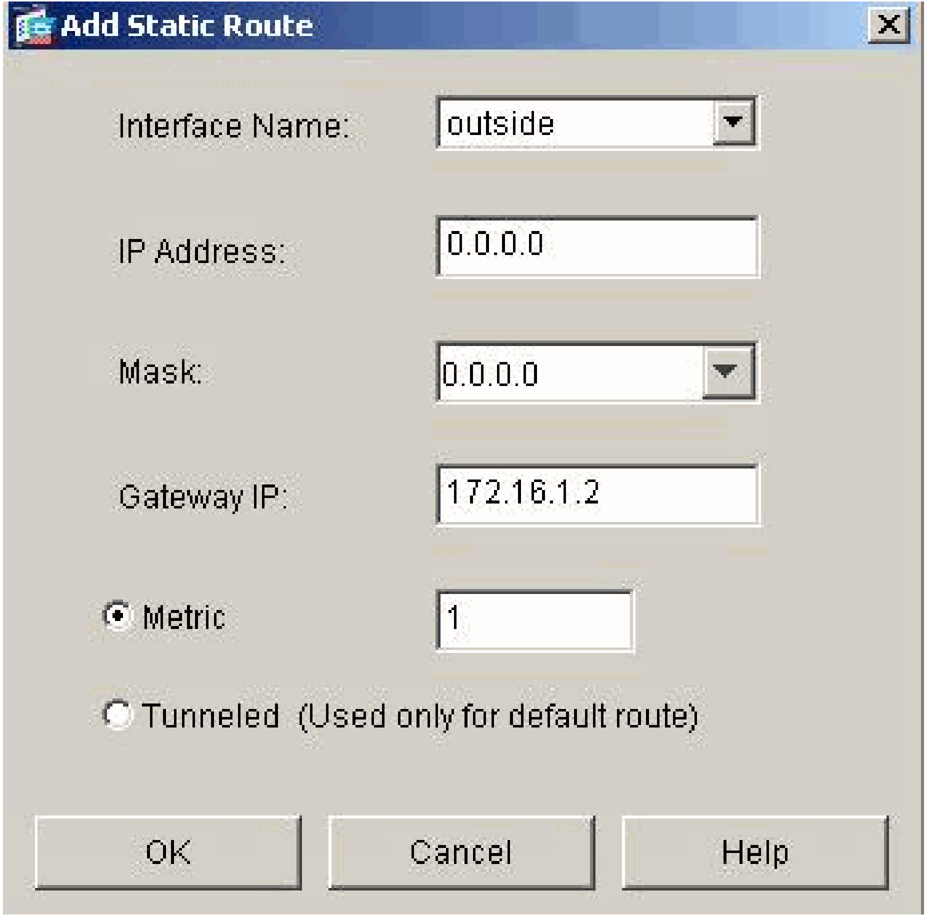
Rule	Original			Translated	
Type	Interface	Source Network	Destination Network	Interface	Address
	inside	10.0.0.0/8	any	outside	172.16.1.4 172.16.1.5-172.16.1.10

Device configuration loaded successfully. <admin> NA (15) 7/11/08 7:44:00 PM UTC

18. 在此示例中，使用了靜態路由。按一下「Routing」，選擇「Static Route」，然後按一下「Add」。



19. 設定預設閘道，然後按一下**OK**。



Interface Name: outside

IP Address: 0.0.0.0

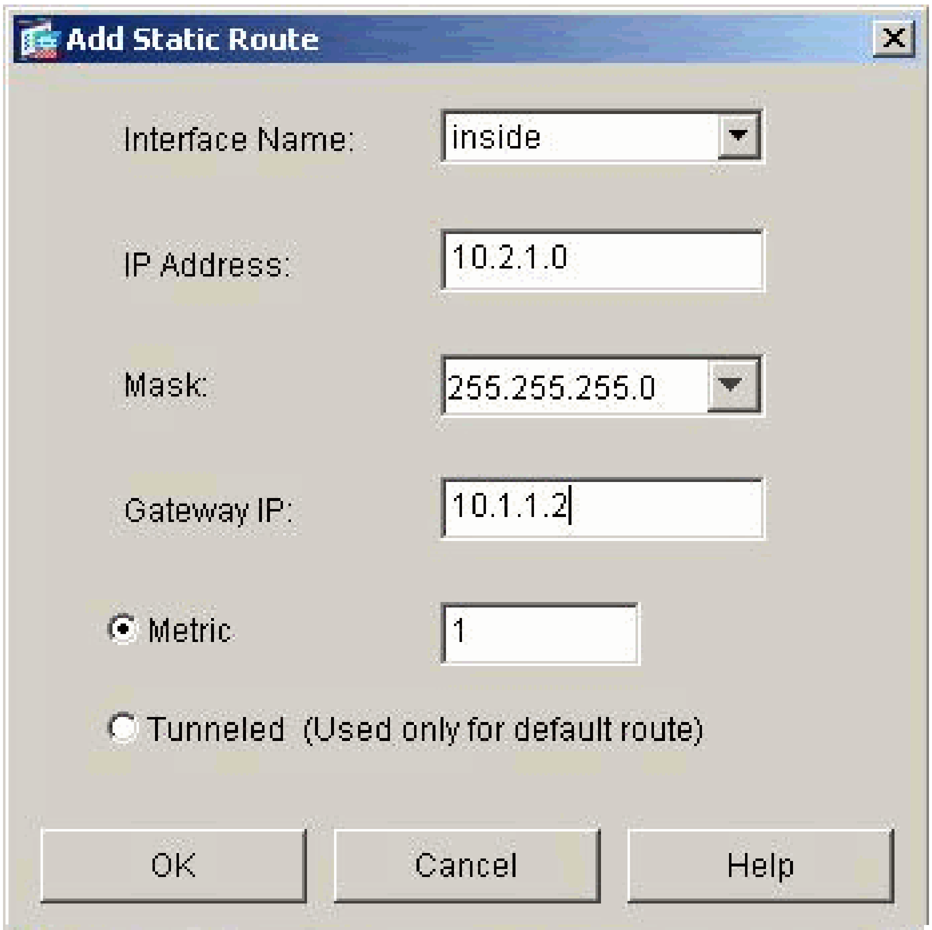
Mask: 0.0.0.0

Gateway IP: 172.16.1.2

● Metric 1

○ Tunneled (Used only for default route)

20. 按一下**Add**，將路由新增到內部網路。



Add Static Route

Interface Name: inside

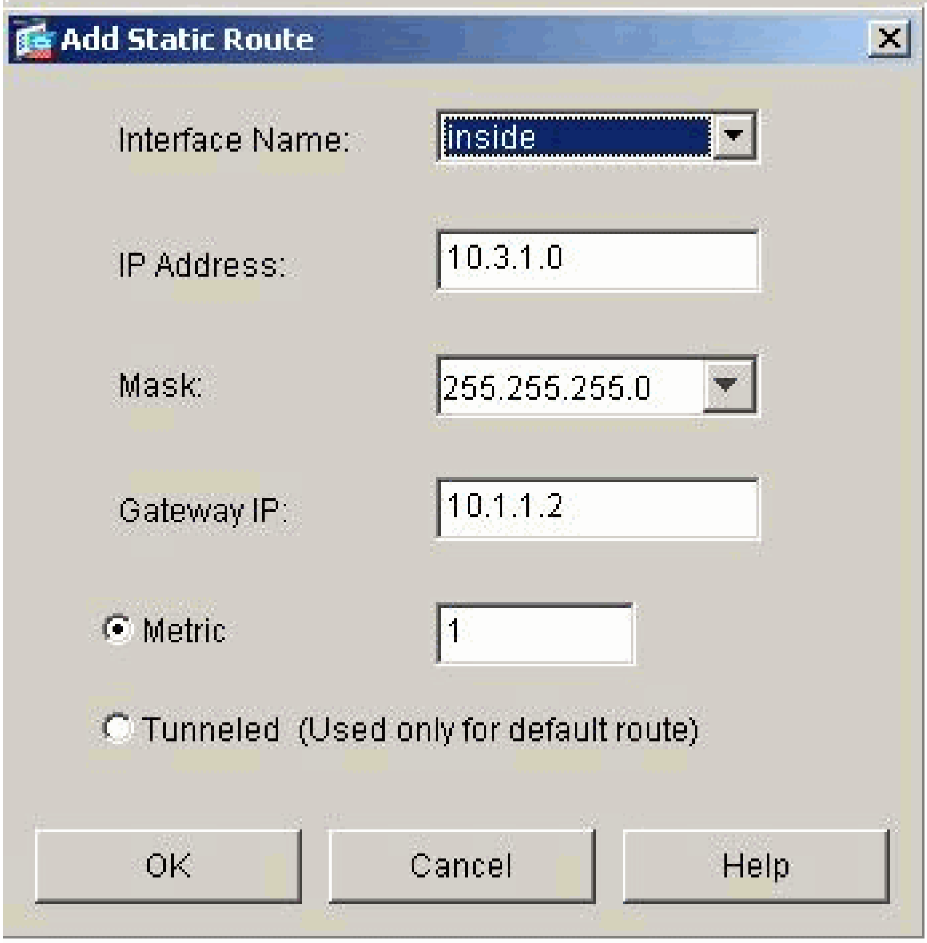
IP Address: 10.2.1.0

Mask: 255.255.255.0

Gateway IP: 10.1.1.2

● Metric 1

○ Tunneled (Used only for default route)



Add Static Route

Interface Name: inside

IP Address: 10.3.1.0

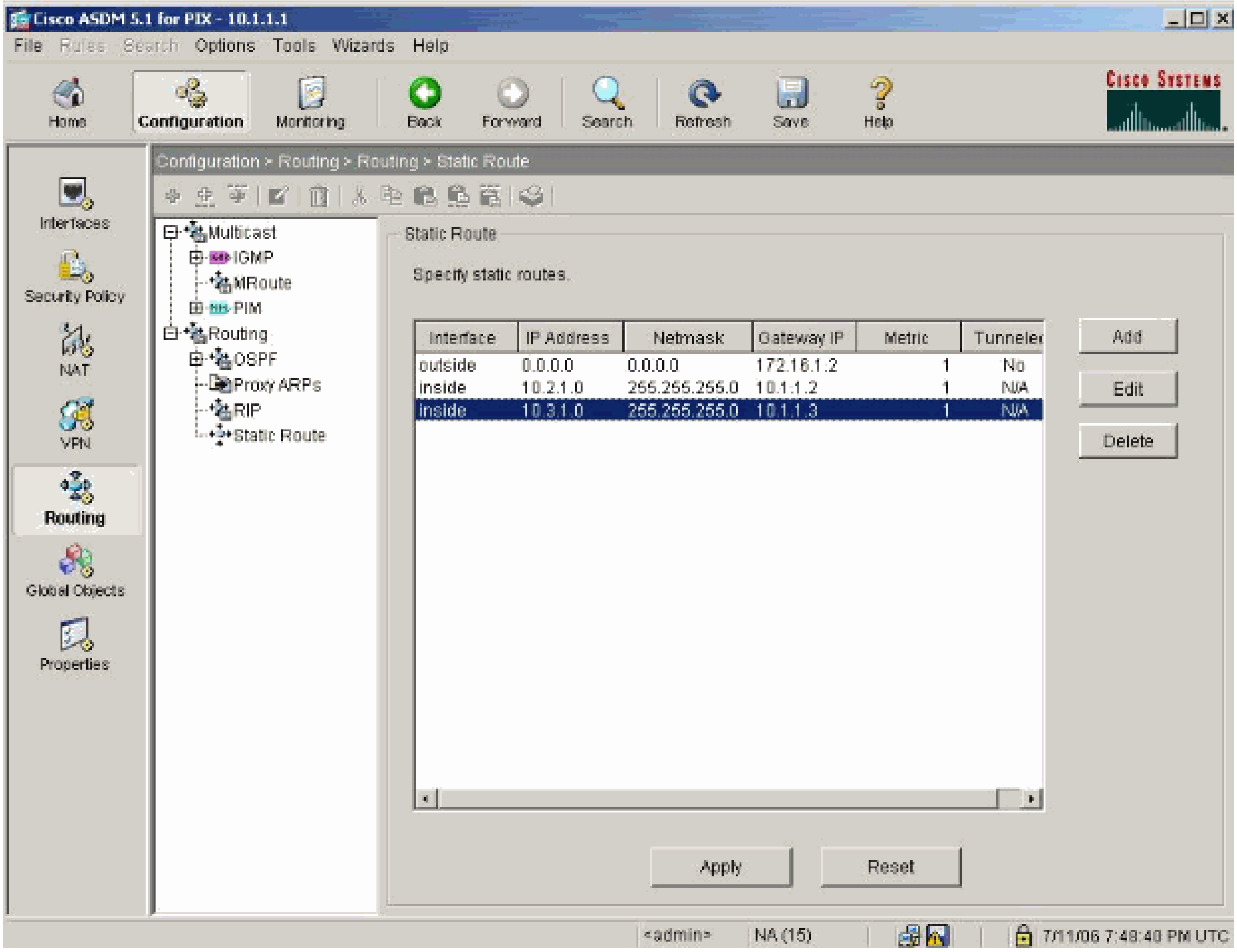
Mask: 255.255.255.0

Gateway IP: 10.1.1.2

● Metric 1

○ Tunneled (Used only for default route)

21. 確認配置了正確的路由，然後按一下**Apply**。



Static Route

Specify static routes.

Interface	IP Address	Netmask	Gateway IP	Metric	Tunneled
outside	0.0.0.0	0.0.0.0	172.16.1.2	1	No
inside	10.2.1.0	255.255.255.0	10.1.1.2	1	N/A
inside	10.3.1.0	255.255.255.0	10.1.1.3	1	N/A

使用CLI配置PIX

通過ASDM GUI的配置現已完成。

您可透過CLI看到此組態：

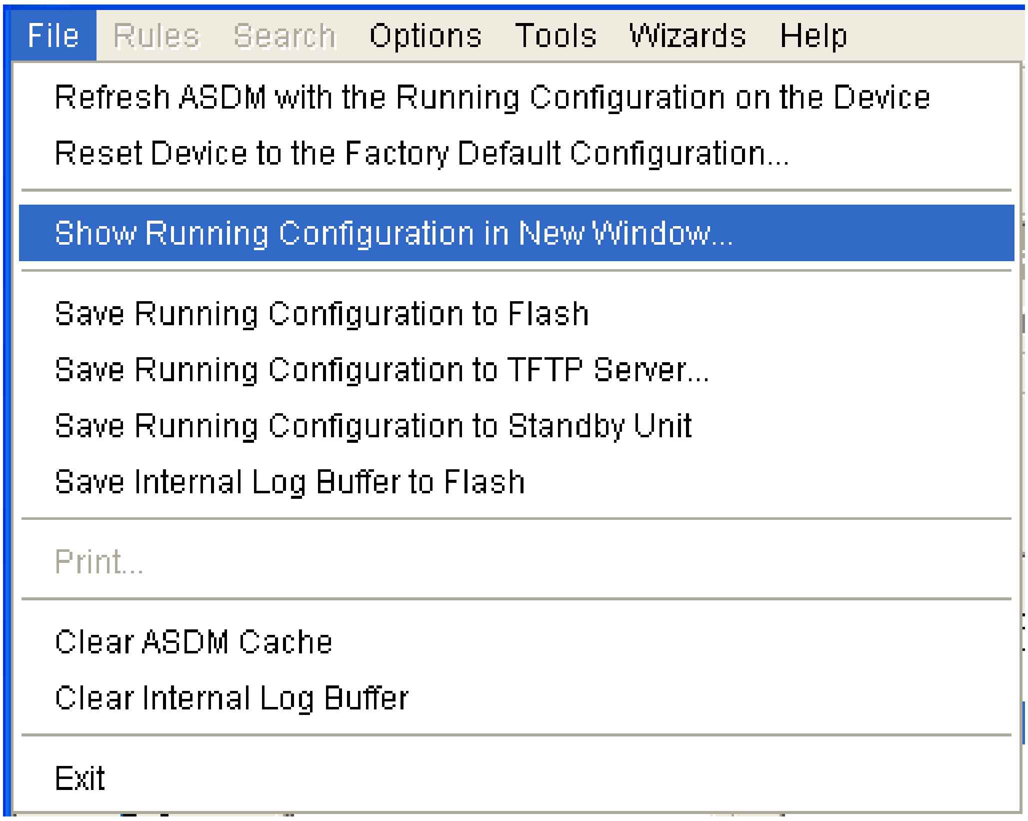
PIX安全裝置CLI

```
pixfirewall(config)#write terminal
PIX Version 7.0(0)102
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!

interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!--- Assign name and IP address to the interfaces enable
password 2KFQnbNIdI.2KYOU encrypted passwd
2KFQnbNIdI.2KYOU encrypted asdm image
flash:/asdmfile.50073 no asdm history enable arp timeout
14400 nat-control
!--- Enforce a strict NAT for all the traffic through
the Security appliance global (outside) 1 172.16.1.5-
```

```
172.16.1.10 netmask 255.255.255.0
!--- Define a pool of global addresses 172.16.1.5 to
172.16.1.10 with !--- NAT ID 1 to be used for NAT global
(outside) 1 172.16.1.4 netmask 255.255.255.0
!--- Define a single IP address 172.16.1.4 with NAT ID 1
to be used for PAT nat (inside) 1 10.0.0.0 255.0.0.0
!--- Define the inside networks with same NAT ID 1 used
in the global command for NAT route inside 10.3.1.0
255.255.255.0 10.1.1.3 1
route inside 10.2.1.0 255.255.255.0 10.1.1.2 1
!--- Configure static routes for routing the packets
towards the internal network route outside 0.0.0.0
0.0.0.0 172.16.1.2 1
!--- Configure static route for routing the packets
towards the Internet (or External network) timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00
sip_media 0:02:00 timeout uauth 0:05:00 absolute http
server enable
!--- Enable the HTTP server on PIX for ASDM access http
10.1.1.5 255.255.255.255 inside
!--- Enable HTTP access from host 10.1.1.5 to configure
PIX using ASDM (GUI) ! !--- Output suppressed ! !
Cryptochecksum:a0bff9bbaa3d815fc9fd269a3f67fef5 : end
```

選擇**File > Show Running Configuration in New Window**以檢視ASDM中的CLI配置。


File
Rules
Search
Options
Tools
Wizards
Help
Refresh ASDM with the Running Configuration on the Device
Reset Device to the Factory Default Configuration...
Show Running Configuration in New Window...
Save Running Configuration to Flash
Save Running Configuration to TFTP Server...
Save Running Configuration to Standby Unit
Save Internal Log Buffer to Flash
Print...
Clear ASDM Cache
Clear Internal Log Buffer
Exit

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

疑難排解指令

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**命令輸出的分析。

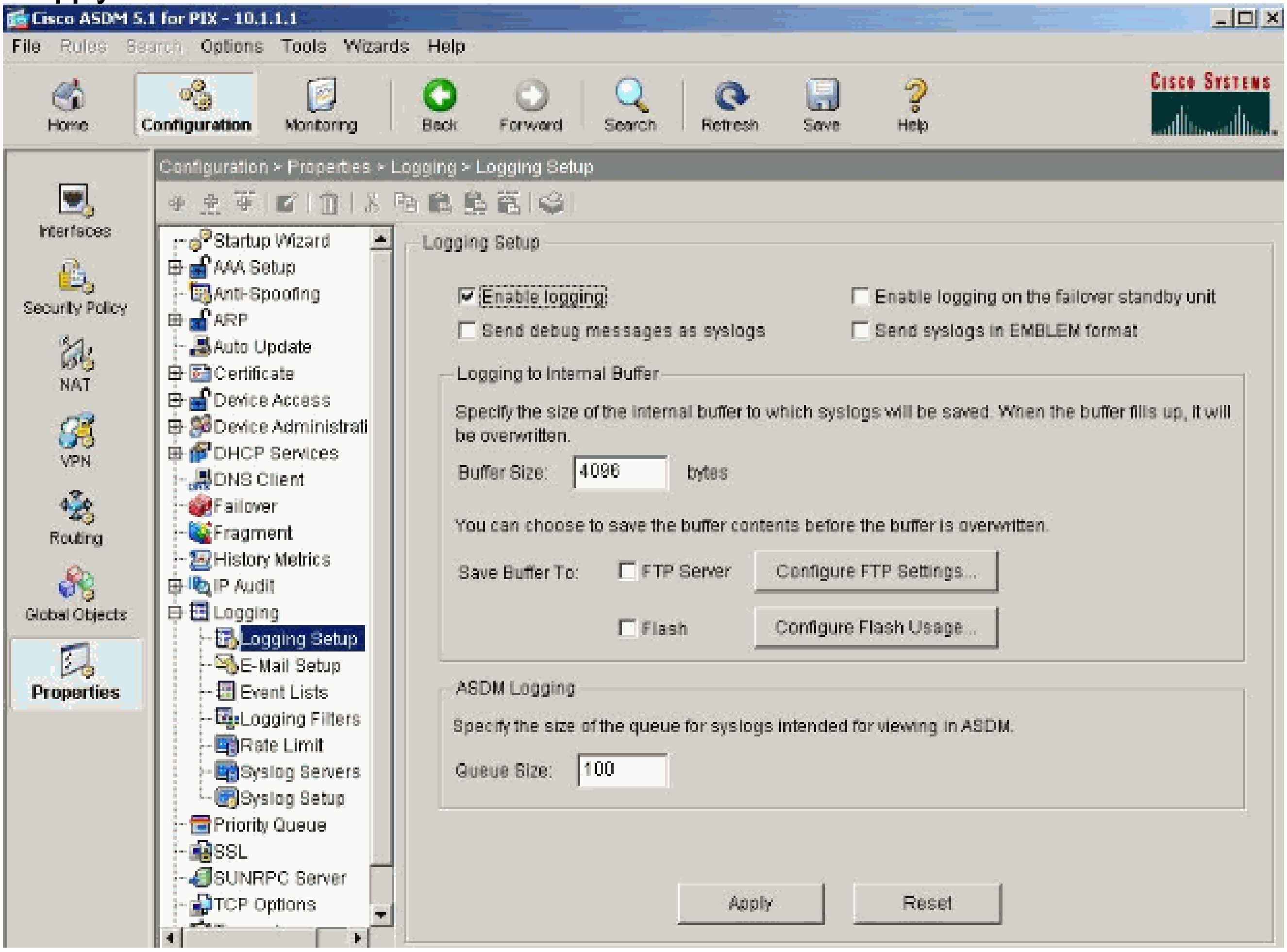
附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- **debug icmp trace** — 顯示來自主機的ICMP請求是否到達PIX。若要執行此偵錯，需要新增**access-list**指令來允許組態中的ICMP。
- **logging buffer debugging** — 顯示已建立和拒絕到通過PIX的主機的連線。該資訊儲存在PIX日誌緩衝區中，可以使用**show log**命令檢視輸出。

疑難排解程序

ASDM可用於啟用日誌記錄以及檢視日誌：

1. 選擇**Configuration > Properties > Logging > Logging Setup**，選中**Enable Logging**，然後按一下**Apply**。



Logging Setup

☑ Enable logging

□ Enable logging on the failover standby unit

□ Send debug messages as syslogs

□ Send syslogs in EMBLEM format

Logging to Internal Buffer

Specify the size of the internal buffer to which syslogs will be saved. When the buffer fills up, it will be overwritten.

Buffer Size: 4096 bytes

You can choose to save the buffer contents before the buffer is overwritten.

Save Buffer To: □ FTP Server Configure FTP Settings...

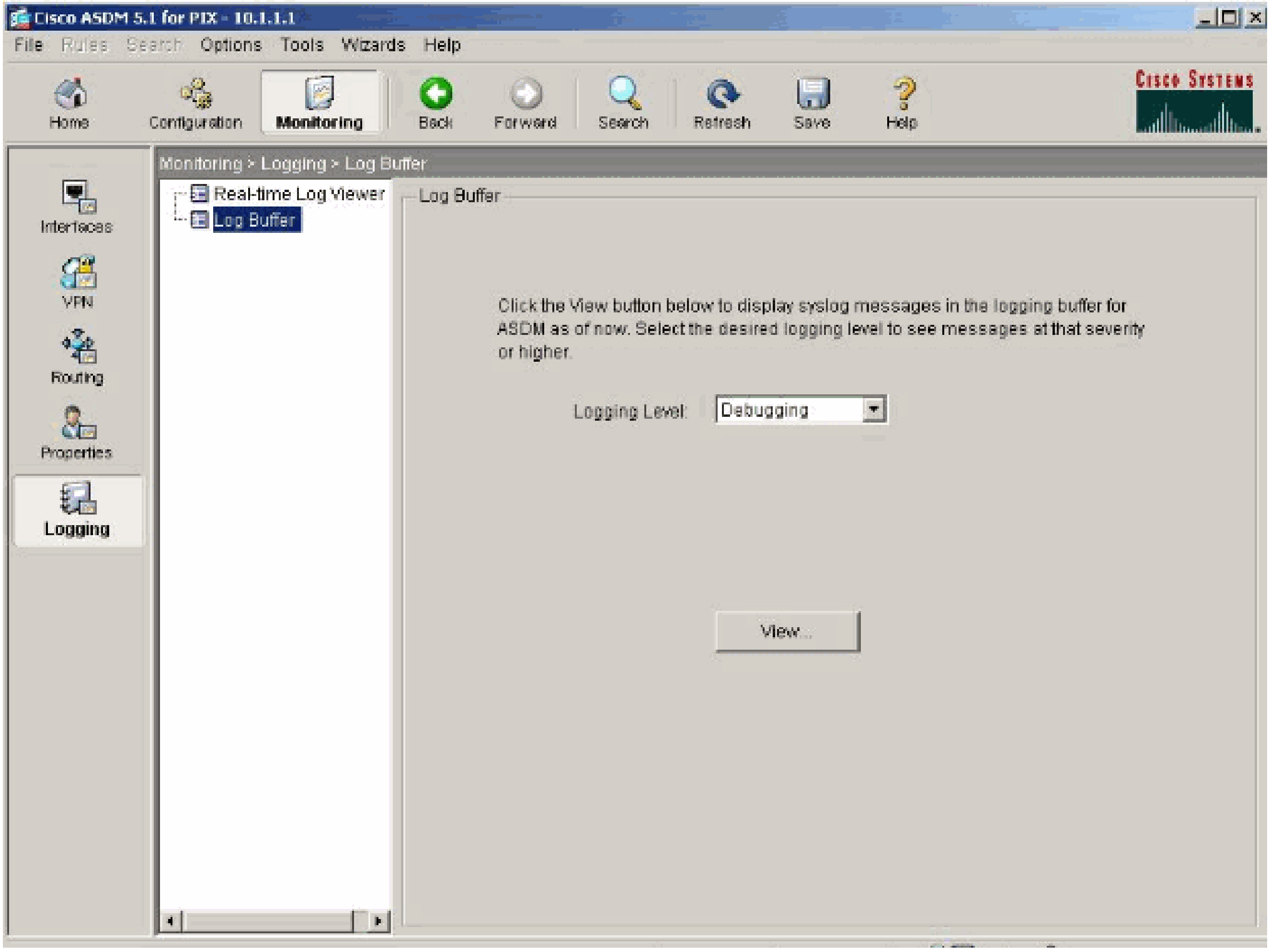
□ Flash Configure Flash Usage...

ASDM Logging

Specify the size of the queue for syslogs intended for viewing in ASDM.

Queue Size: 100

2. 選擇**Monitoring > Logging > Log Buffer > Logging Level**，然後從下拉選單中選擇**Logging Buffer**。按一下「**View**」。

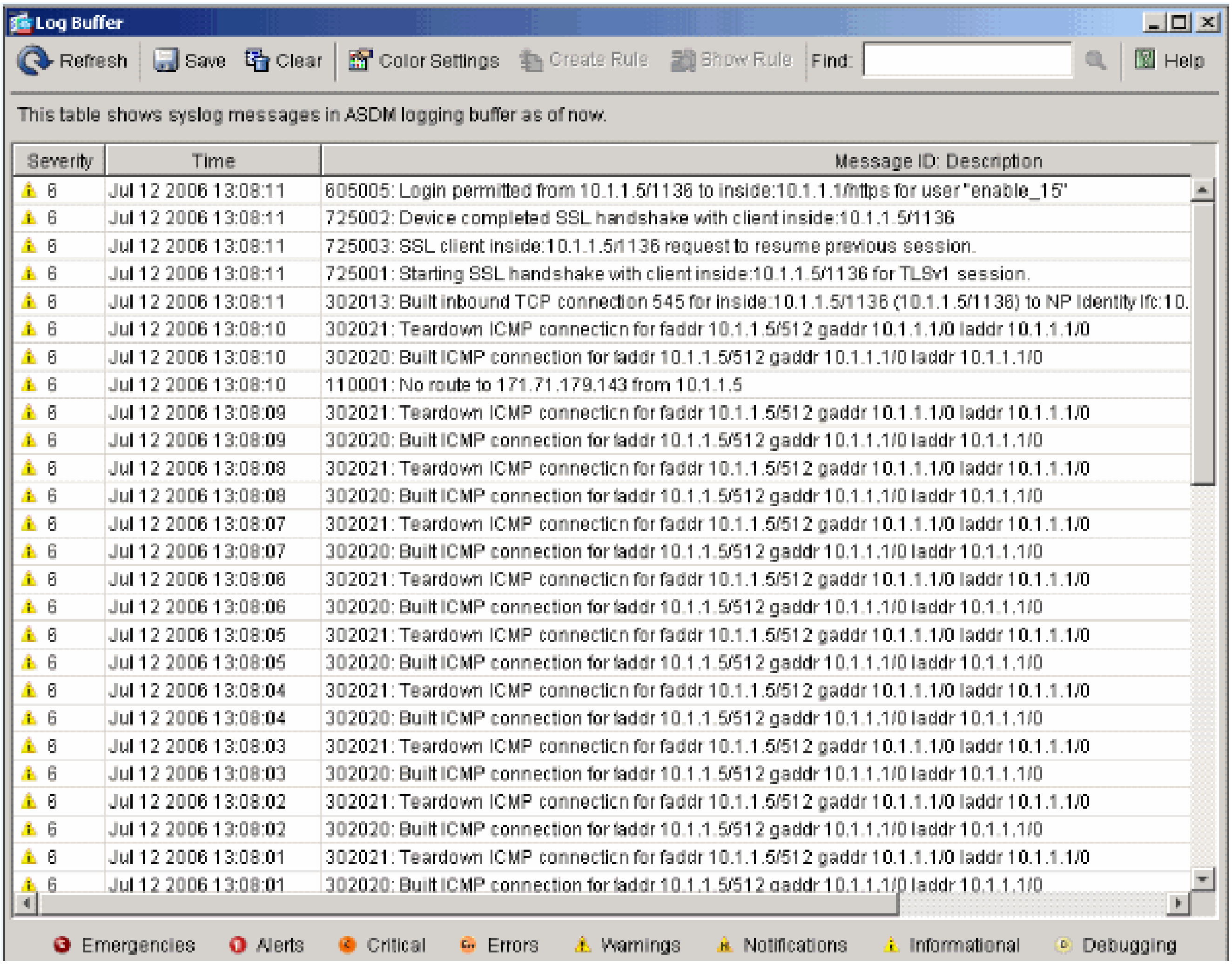

Cisco ASDM 5.1 for PIX - 10.1.1.1
File Rules Search Options Tools Wizards Help
Home Configuration Monitoring Back Forward Search Refresh Save Help
Cisco Systems
Interfaces
VPN
Routing
Properties
Logging
Monitoring > Logging > Log Buffer
Real-time Log Viewer
Log Buffer
Log Buffer
View...

Click the View button below to display syslog messages in the logging buffer for ASDM as of now. Select the desired logging level to see messages at that severity or higher.

Logging Level: Debugging

3. 以下是日誌緩衝區的示例

：



This table shows syslog messages in ASDM logging buffer as of now.

Severity	Time	Message ID: Description
6	Jul 12 2006 13:08:11	605005: Login permitted from 10.1.1.5/1136 to inside:10.1.1.1/https for user "enable_15"
6	Jul 12 2006 13:08:11	725002: Device completed SSL handshake with client inside:10.1.1.5/1136
6	Jul 12 2006 13:08:11	725003: SSL client inside:10.1.1.5/1136 request to resume previous session.
6	Jul 12 2006 13:08:11	725001: Starting SSL handshake with client inside:10.1.1.5/1136 for TLSv1 session.
6	Jul 12 2006 13:08:11	302013: Built inbound TCP connection 545 for inside:10.1.1.5/1136 (10.1.1.5/1136) to NP Identity Ifc:10.
6	Jul 12 2006 13:08:10	302021: Teardown ICMP connecticn for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:10	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:10	110001: No route to 171.71.179.143 from 10.1.1.5
6	Jul 12 2006 13:08:09	302021: Teardown ICMP connecticn for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:09	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:08	302021: Teardown ICMP connecticn for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:08	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:07	302021: Teardown ICMP connecticn for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:07	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:06	302021: Teardown ICMP connecticn for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:06	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:05	302021: Teardown ICMP connecticn for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:05	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:04	302021: Teardown ICMP connecticn for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:04	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:03	302021: Teardown ICMP connecticn for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:03	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:02	302021: Teardown ICMP connecticn for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:02	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:01	302021: Teardown ICMP connecticn for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:01	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0

無法按名稱訪問網站

在某些情況下，內部網路無法使用Web瀏覽器中的名稱（使用IP地址）訪問Internet網站。此問題很常見，通常在未定義DNS伺服器時發生，特別是在PIX/ASA是DHCP伺服器的情況下。此外，如果PIX/ASA無法推送DNS伺服器或者無法訪問DNS伺服器，也可能會發生這種情況。

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 Secure PIX防火牆命令參考
- 思科調適型資安裝置管理員
- 思科自適應安全裝置管理器(ASDM)故障排除和警報
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems