

帶網路地址轉換的PIX/ASA (版本7.x和更高版本) IPsec VPN隧道配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[相關產品](#)

[設定](#)

[網路圖表](#)

[組態](#)

[PIX安全裝置和訪問清單配置](#)

[PIX安全裝置和MPF \(模組化策略框架 \) 配置](#)

[驗證](#)

[疑難排解](#)

[路由器IPsec的故障排除命令](#)

[清除安全關聯](#)

[PIX故障排除命令](#)

[相關資訊](#)

簡介

此示例配置演示了通過執行網路地址轉換(NAT)的防火牆的IPsec VPN隧道。如果您使用早於12.2(13)T且不包括12.2(13)T的Cisco IOS®軟體版本，則此配置不適用於埠地址轉換(PAT)。此型別的配置可用於隧道IP流量。此組態不能用於加密沒有通過防火牆 (例如IPX或路由更新) 的流量。通用路由封裝(GRE)通道是更合適的選擇。在本示例中，Cisco 2621和3660路由器是加入兩個專用網路的IPsec隧道終端，其間的PIX上帶有管道或訪問控制清單(ACL)，以便允許IPsec流量。

注意：NAT是一對一地址轉換，不要與PAT混淆，後者是許多 (防火牆內部) 對一轉換。有關NAT操作和配置的詳細資訊，請參閱[驗證NAT操作和基本NAT故障排除](#)或[NAT的工作原理](#)。

注意：帶PAT的IPsec可能無法正常工作，因為外部隧道終結點裝置無法處理來自一個IP地址的多個隧道。聯絡您的供應商，以確定隧道終端裝置是否與PAT配合使用。此外，在Cisco IOS軟體版本12.2(13)T及更高版本中，NAT透明功能可用於PAT。有關詳細資訊，請參閱[IPSec NAT透明度](#)。請參閱[透過NAT的IPSec ESP支援](#)，以詳細瞭解Cisco IOS軟體版本12.2(13)T和更新版本中的這些功能。

注意：在使用Cisco技術支援開啟案例之前，請參閱[NAT常見問題](#)，該問題有許多常見問題的答案。

有關如何在PIX版本6.x及更低版本上使用NAT配置IPsec隧道穿過防火牆的詳細資訊，請參閱[使用](#)

[NAT配置IPSec隧道。](#)

[必要條件](#)

[需求](#)

本文件沒有特定需求。

[採用元件](#)

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS軟體版本12.0.7.T(最高但不包括Cisco IOS軟體版本12.2(13)T)有關最新版本，請參閱[IPSec NAT透明度](#)。
- 思科2621路由器
- 思科3660路由器
- 運行7.x及更高版本的Cisco PIX 500系列安全裝置。

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。](#)

[相關產品](#)

本檔案也適用於軟體版本7.x及更新版本的Cisco 5500系列調適型安全裝置(ASA)。

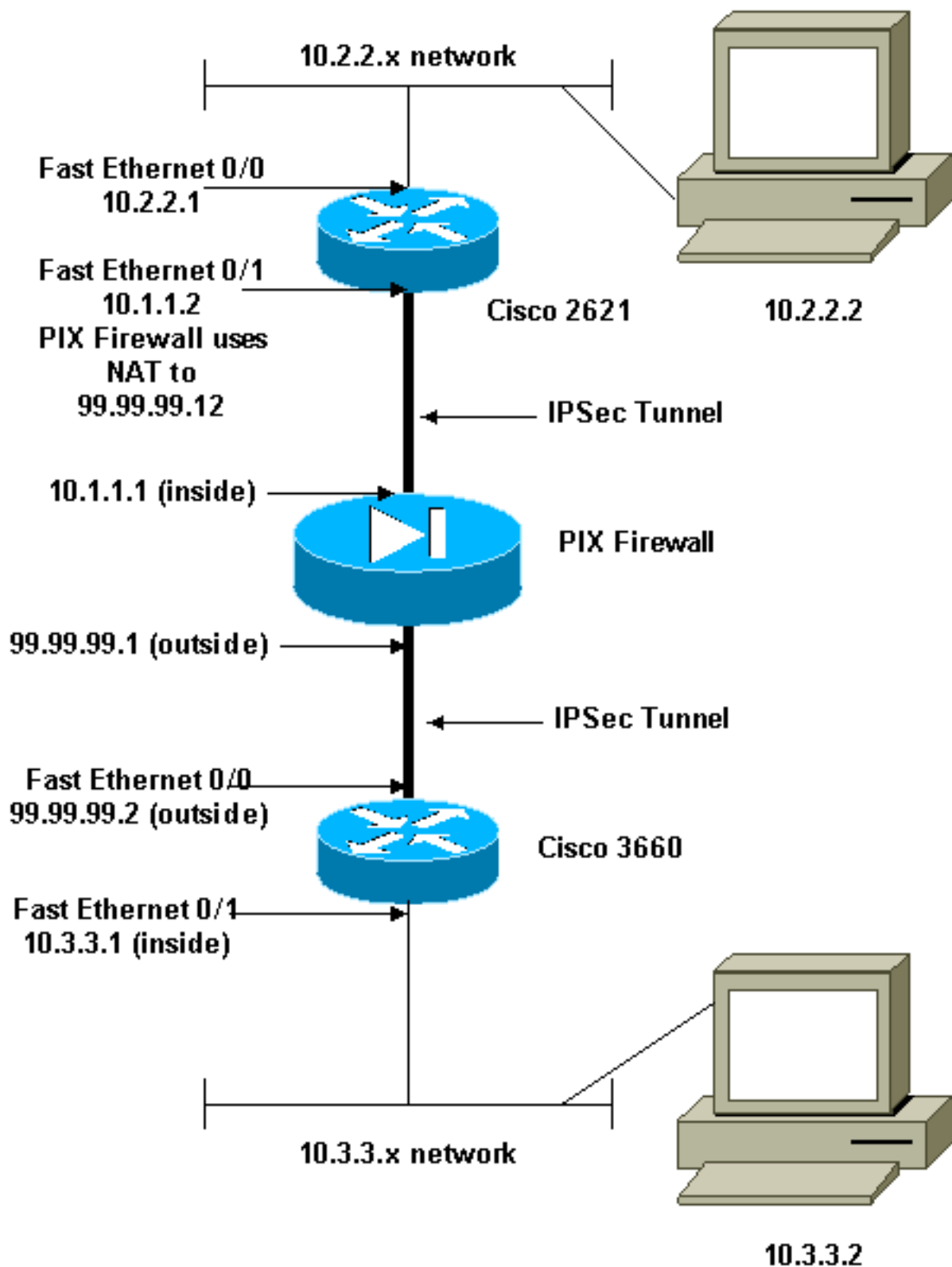
[設定](#)

本節提供可用於設定本檔案中所述功能的資訊。

注意：要查詢有關本文檔使用的命令的更多資訊，請使用[命令查詢工具](#)(僅限[註冊](#)客戶)。

[網路圖表](#)

本檔案會使用以下網路設定：



組態

本檔案會使用以下設定：

- [思科2621配置](#)
- [思科3660配置](#)
- [PIX安全裝置和訪問清單配置高級安全裝置管理器GUI\(ASDM\)配置命令列介面\(CLI\)配置](#)
- [PIX安全裝置和MPF \(模組化策略框架 \) 配置](#)

Cisco 2621

Current configuration:

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname goss-2621  
!  
ip subnet-zero  
!  
ip audit notify log  
ip audit po max-events 100  
isdn voice-call-failure 0  
cns event-service server  
!  
!--- The IKE policy. crypto isakmp policy 10  
  hash md5  
  authentication pre-share  
crypto isakmp key cisco123 address 99.99.99.2  
!  
crypto ipsec transform-set myset esp-des esp-md5-hmac  
!  
crypto map mymap local-address FastEthernet0/1  
  
!--- IPsec policy. crypto map mymap 10 ipsec-isakmp  
  set peer 99.99.99.2  
  set transform-set myset  
  
!--- Include the private-network-to-private-network  
traffic !--- in the encryption process. match address  
101  
!  
controller T1 1/0  
!  
interface FastEthernet0/0  
  ip address 10.2.2.1 255.255.255.0  
  no ip directed-broadcast  
  duplex auto  
  speed auto  
!  
interface FastEthernet0/1  
  ip address 10.1.1.2 255.255.255.0  
  no ip directed-broadcast  
  duplex auto  
  speed auto  
  
!--- Apply to the interface. crypto map mymap  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 10.1.1.1  
no ip http server  
  
!--- Include the private-network-to-private-network  
traffic !--- in the encryption process. access-list 101  
permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255  
  line con 0  
    transport input none  
  line aux 0  
  line vty 0 4  
!
```

```
no scheduler allocate
end
```

Cisco 3660

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname goss-3660
!
ip subnet-zero
!
cns event-service server
!

!--- The IKE policy. crypto isakmp policy 10
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 99.99.99.12
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/0

!--- The IPsec policy. crypto map mymap 10 ipsec-isakmp
  set peer 99.99.99.12
  set transform-set myset

  !--- Include the private-network-to-private-network
  traffic !--- in the encryption process. match address
101
!
interface FastEthernet0/0
  ip address 99.99.99.2 255.255.255.0
  no ip directed-broadcast
  ip nat outside
  duplex auto
  speed auto

!--- Apply to the interface. crypto map mymap
!
interface FastEthernet0/1
  ip address 10.3.3.1 255.255.255.0
  no ip directed-broadcast
  ip nat inside
  duplex auto
  speed auto
!
interface Ethernet3/0
  no ip address
  no ip directed-broadcast
  shutdown
!
interface Serial3/0
  no ip address
  no ip directed-broadcast
  no ip mroute-cache
  shutdown
!
interface Ethernet3/1
  no ip address
```

```

no ip directed-broadcast
interface Ethernet4/0
  no ip address
  no ip directed-broadcast
  shutdown
!
interface TokenRing4/0
  no ip address
  no ip directed-broadcast
  shutdown
  ring-speed 16
!

!--- The pool from which inside hosts translate to !---
the globally unique 99.99.99.0/24 network. ip nat pool
OUTSIDE 99.99.99.70 99.99.99.80 netmask 255.255.255.0

!--- Except the private network from the NAT process. ip
nat inside source route-map nonat pool OUTSIDE
  ip classless
  ip route 0.0.0.0 0.0.0.0 99.99.99.1
  no ip http server
!

!--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
  access-list 101 deny ip 10.3.3.0 0.0.0.255 any

!--- Except the private network from the NAT process.
access-list 110 deny ip 10.3.3.0 0.0.0.255 10.2.2.0
0.0.0.255
  access-list 110 permit ip 10.3.3.0 0.0.0.255 any
  route-map nonat permit 10
  match ip address 110
!
line con 0
  transport input none
line aux 0
line vty 0 4
!
end

```

PIX安全裝置和訪問清單配置

ASDM 5.0配置

完成以下步驟，以便使用ASDM配置PIX防火牆版本7.0。

1. 通過控制檯連線到PIX。在清除的配置中，使用互動式提示啟用高級安全裝置管理器 GUI(ASDM)，以便從工作站10.1.1.3管理PIX。
2. 在Workstation 10.1.1.3中開啟Web瀏覽器並使用ASDM(在本例中為https://10.1.1.1)。
3. 在證書提示上選擇Yes，然後使用[PIX防火牆ASDM載入程式配置中配置的啟用密碼登入](#)。
4. 如果這是第一次在PC上運行ASDM，則會提示您使用ASDM啟動程式還是將ASDM用作Java應用。在本示例中，ASDM啟動程式被選中並安裝這些提示。
5. 進入ASDM主視窗並選擇Configuration頁籤。

Cisco ASDM 5.0 for PIX - 10.1.1.1

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Back Forward Search Refresh Save Help

Device Information

General License

Host Name: **pixfirewall.cisco.com**

PIX Version: **7.0(0)102** Device Uptime: **0d 0h 3m 53s**

ASDM Version: **5.0(0)73** Device Type: **PIX 515E**

Firewall Mode: **Routed** Context Mode: **Single**

Total Flash: **16 MB** Total Memory: **64 MB**

Interface Status

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

VPN Status

IKE Tunnels: **0** IPsec Tunnels: **0**

System Resources Status

CPU CPU Usage (percent)

0% 10:20:28

Memory Memory Usage (MB)

20 MB 16:20:28

Traffic Status

Connections Per Second Usage

UDP: 0 TCP: 0 Total: 0

'inside' Interface Traffic Usage (Kbps)

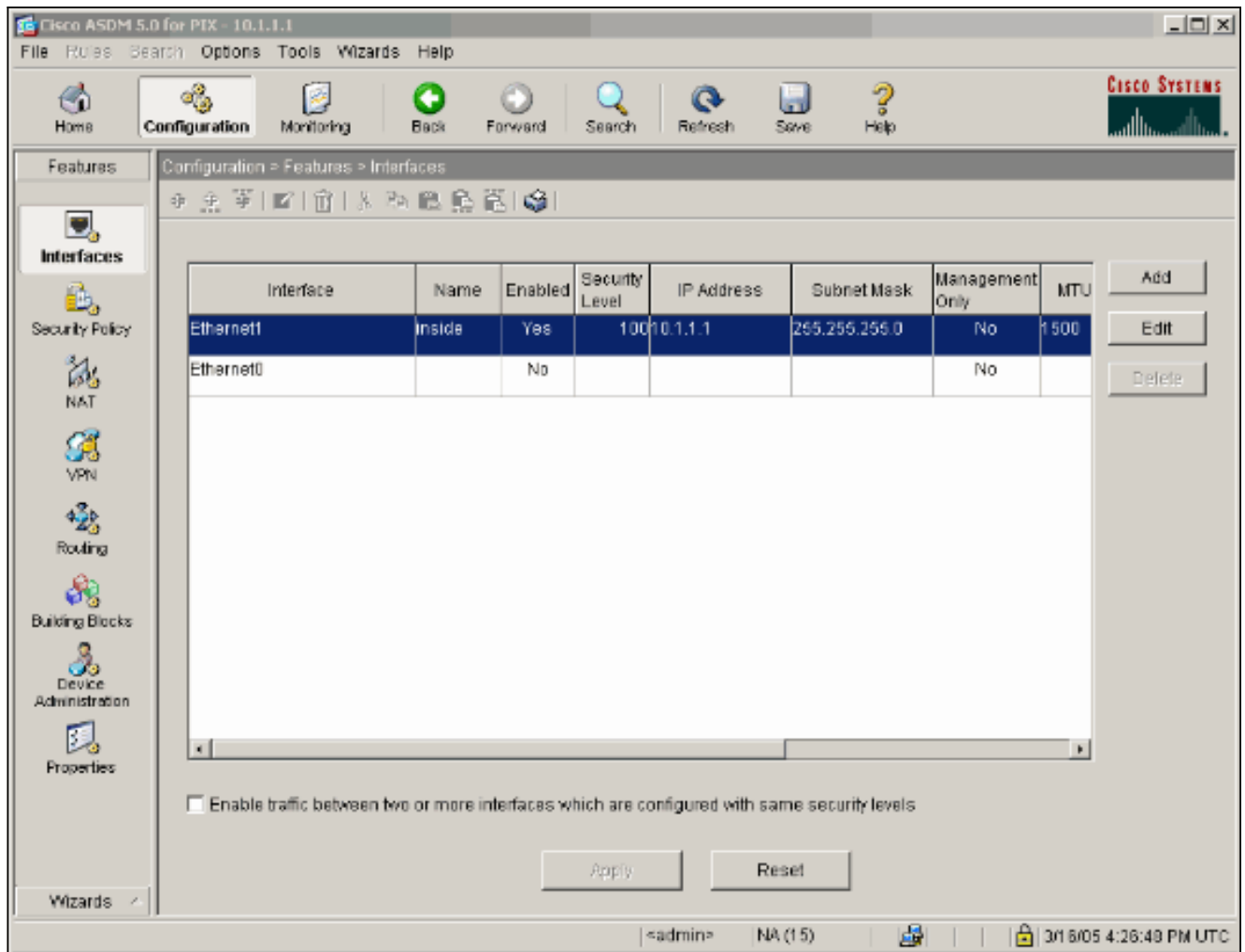
Input Kbps: 0 Output Kbps: 1

Latest ASDM Syslog Messages

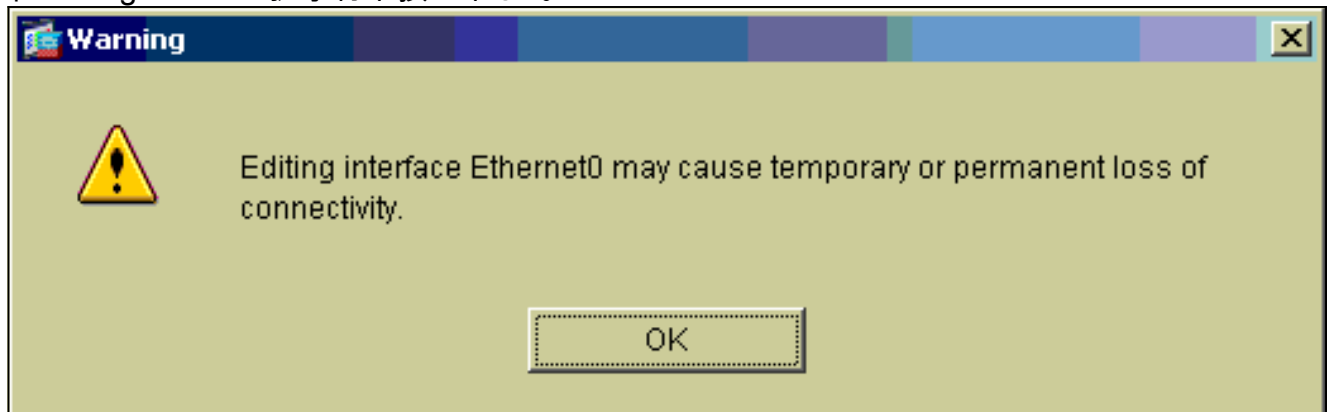
-- Syslog Disabled --

Device configuration loaded successfully. |<admin> NA (15) | 3/16/05 4:26:29 PM UTC

6. 選中Ethernet 0 Interface並按一下Edit以配置外部介面。



7. 在Editing interface提示符下按一下OK。



8. 輸入介面詳細資訊，完成後按一下OK。

Hardware Port: **Ethernet0** Configure Hardware Properties...

Enable Interface Dedicate this interface to management only

Interface Name:

Security Level:

IP Address

Use Static IP Obtain Address via DHCP

IP Address:


Subnet Mask:

MTU:

Description:

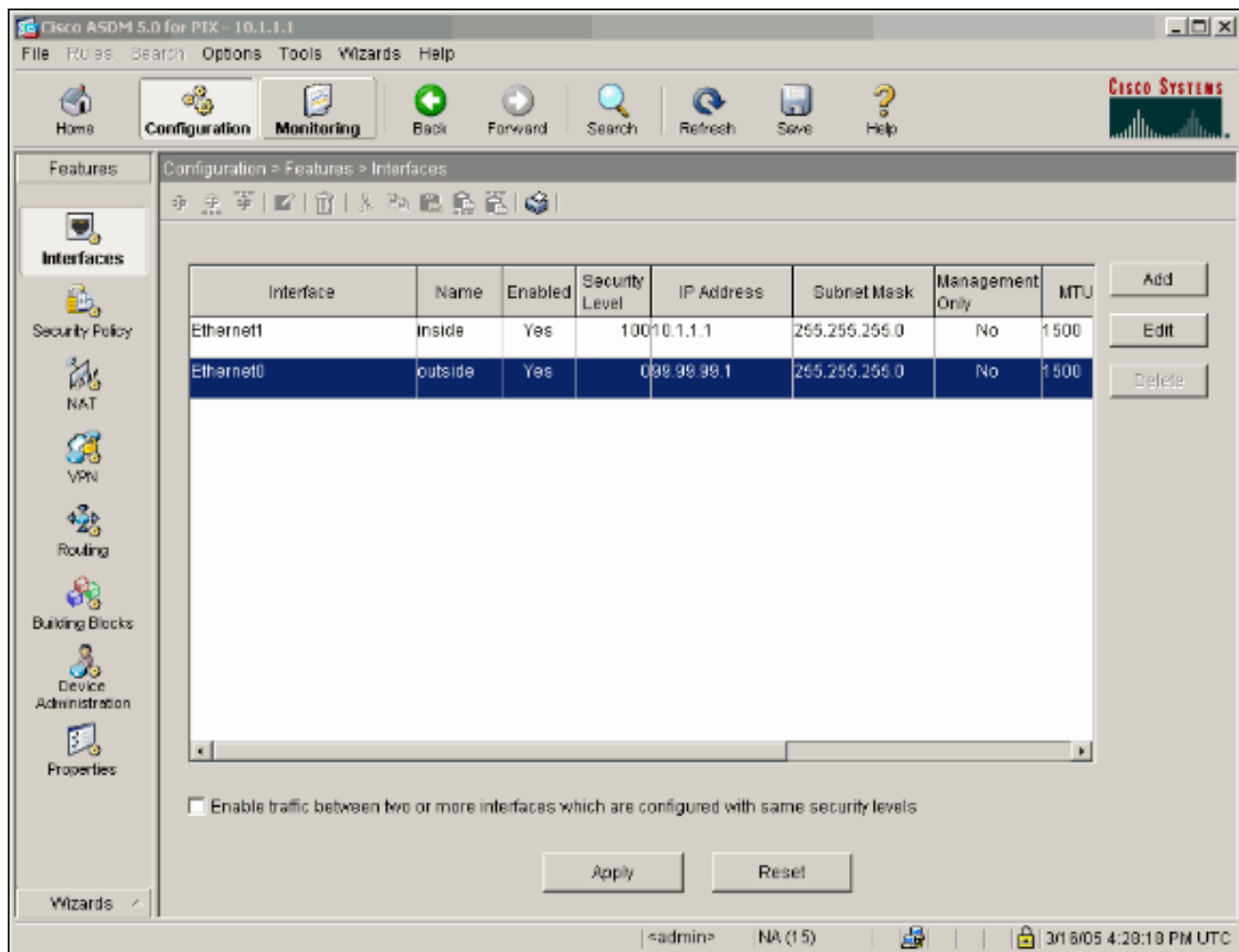
OK Cancel Help

9. 在Changing an Interface提示符下按一下OK。

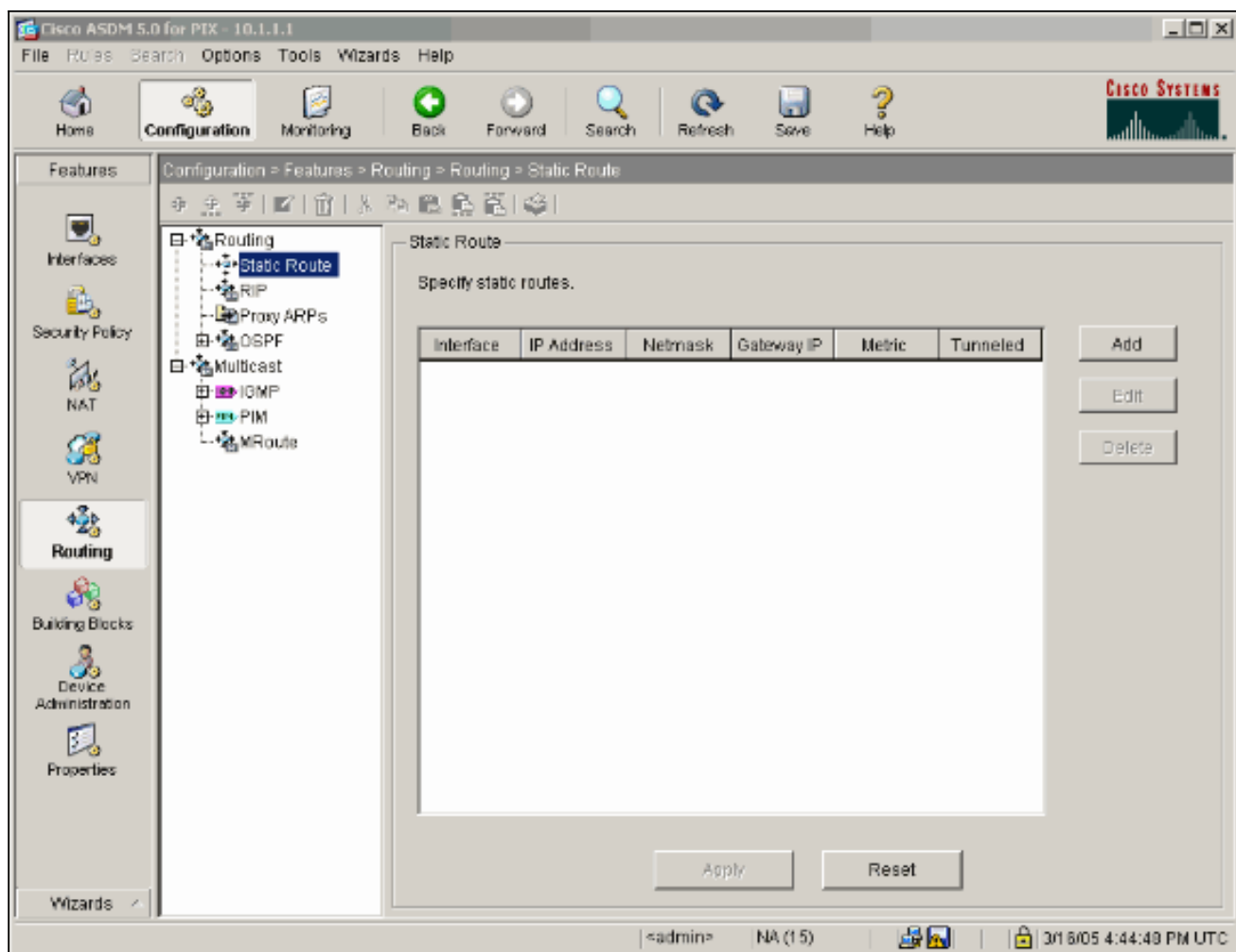
 Changing an interface's security level may cause your PIX configuration to become invalid, causing the PIX to drop legal traffic or allow illegal traffic to pass through. Do you still wish to proceed?

OK Cancel

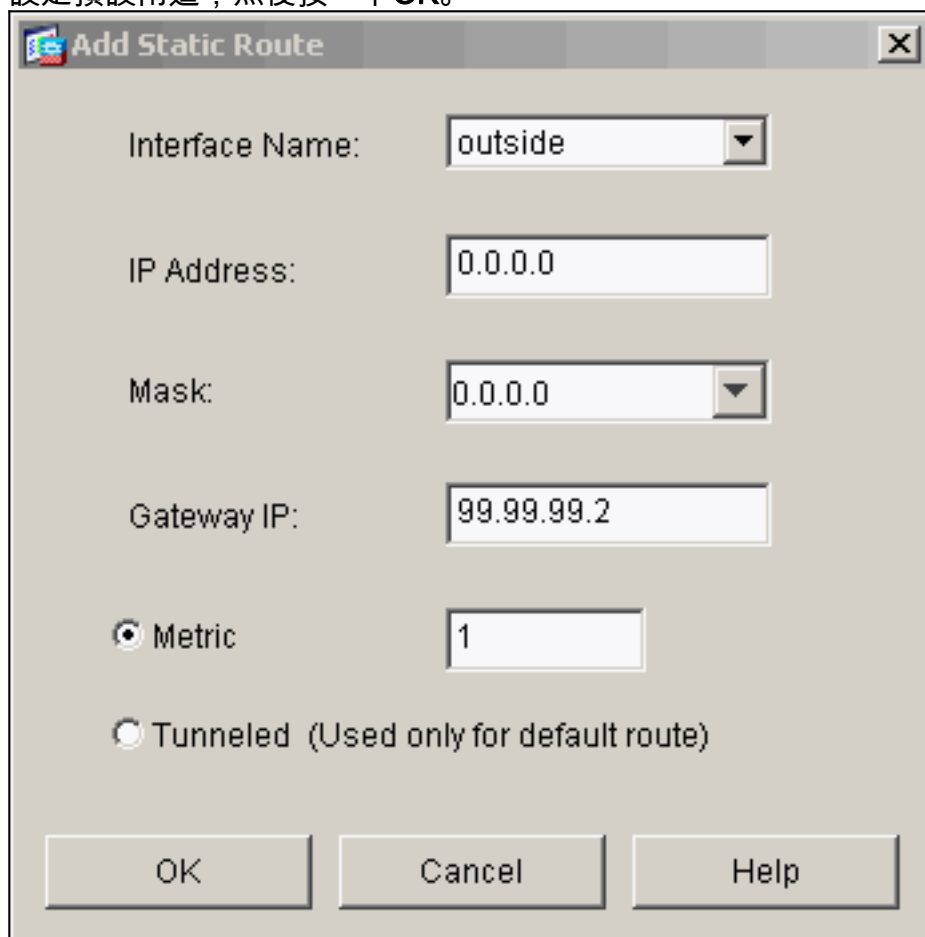
10. 按一下「Apply」以接受介面組態。該配置也將推到PIX上。此示例使用靜態路由。



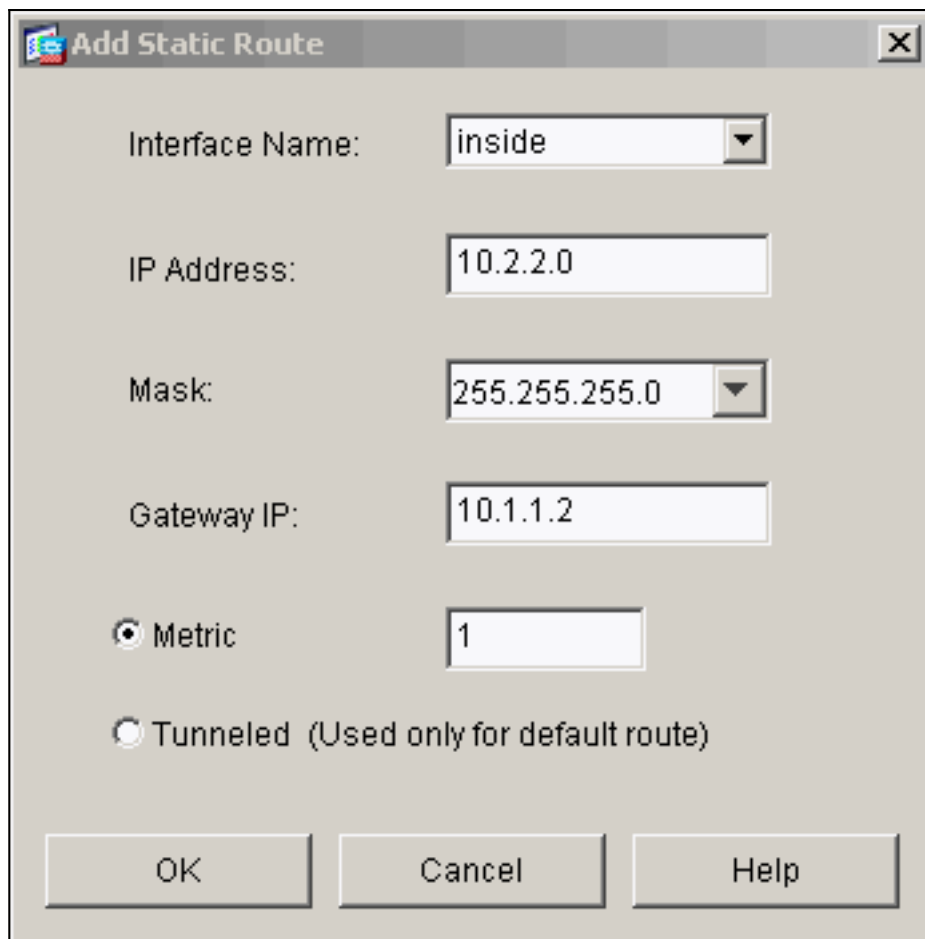
11. 在Features (功能) 頁籤下按一下Routing，選中Static Route，然後按一下Add。



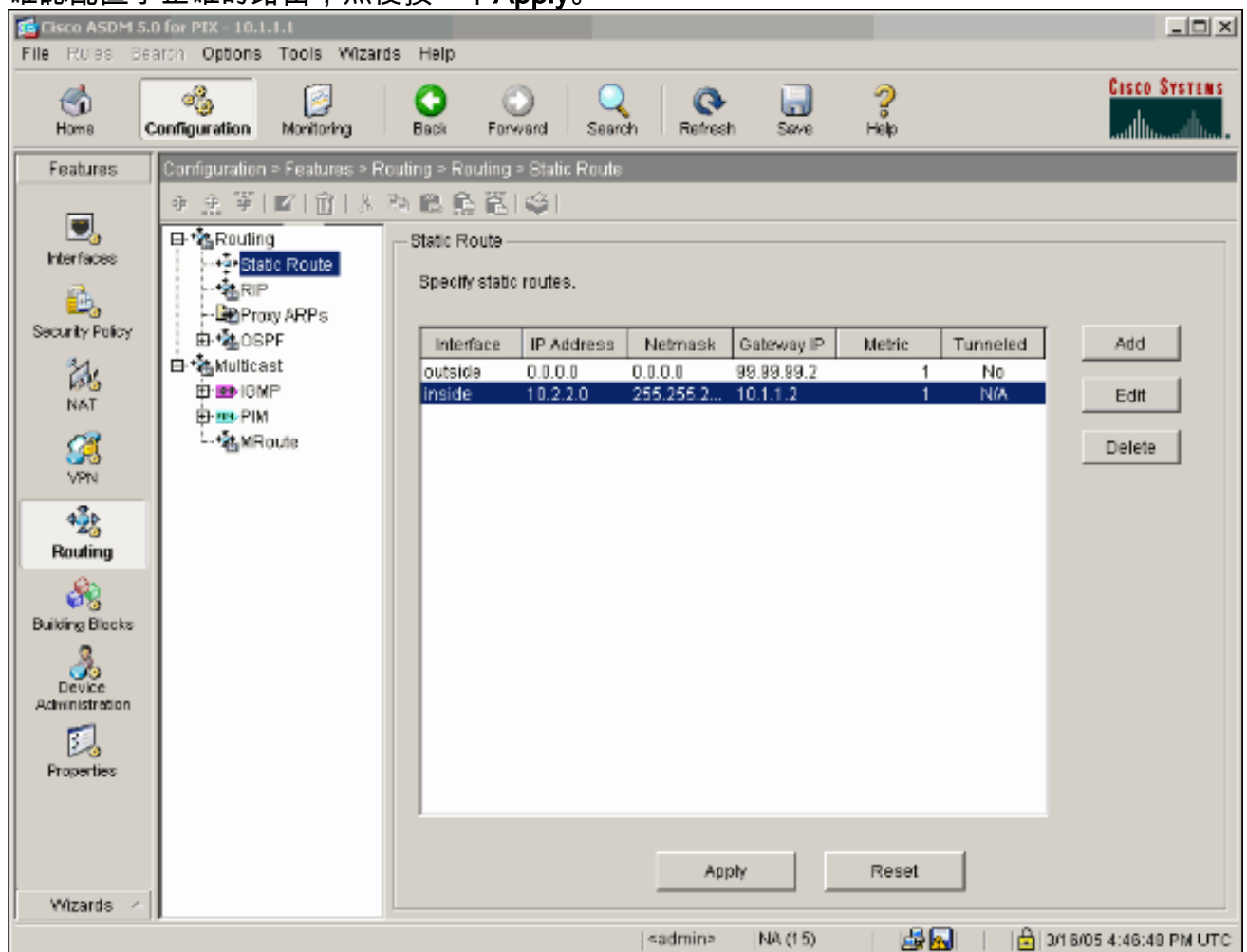
12. 設定預設閘道，然後按一下OK。



13. 按一下Add，將路由新增到內部網路。

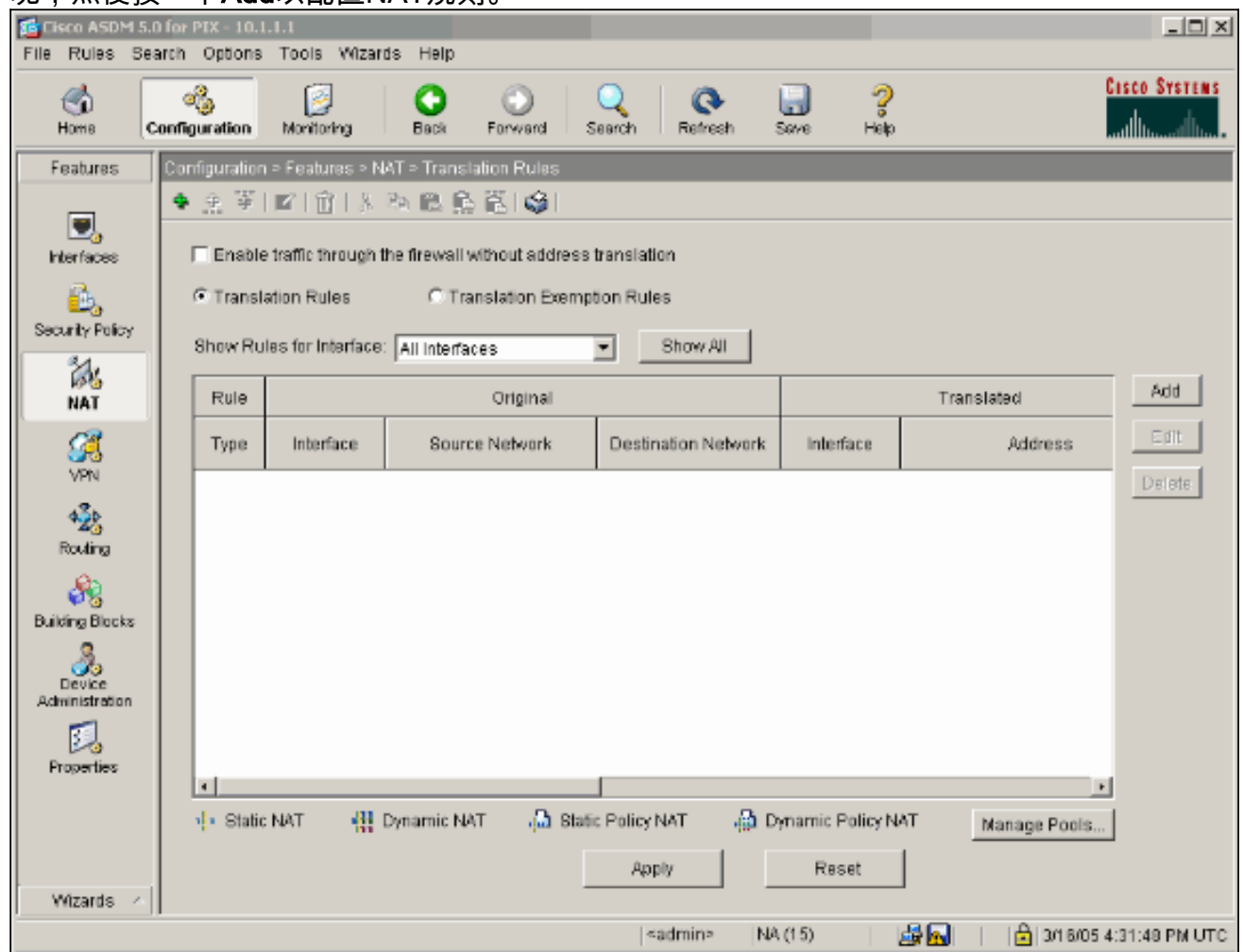


14. 確認配置了正確的路由，然後按一下Apply。



15. 本示例使用NAT。選中Enable traffic through the firewall without address translation 覆取方

塊，然後按一下Add以配置NAT規則。



16. 配置源網路 (本示例使用any)。然後按一下Manage Pools以定義PAT。

Add Address Translation Rule

Use NAT Use Policy NAT

Source Host/Network


Interface:

IP Address:

Mask:

Translate Address on Interface:


Translate Address To

 Static IP Address:

Redirect port

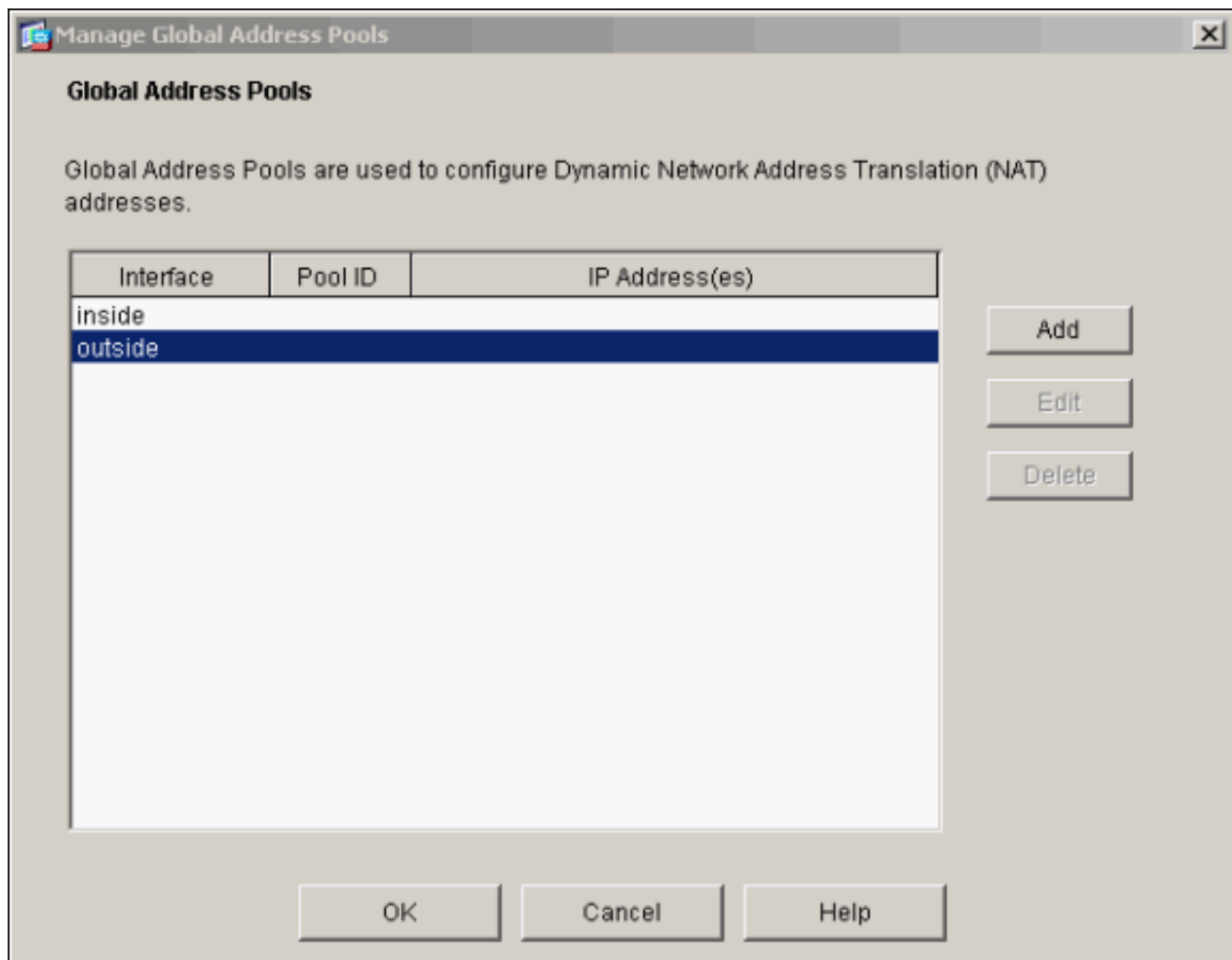
TCP Original port: Translated port:

UDP

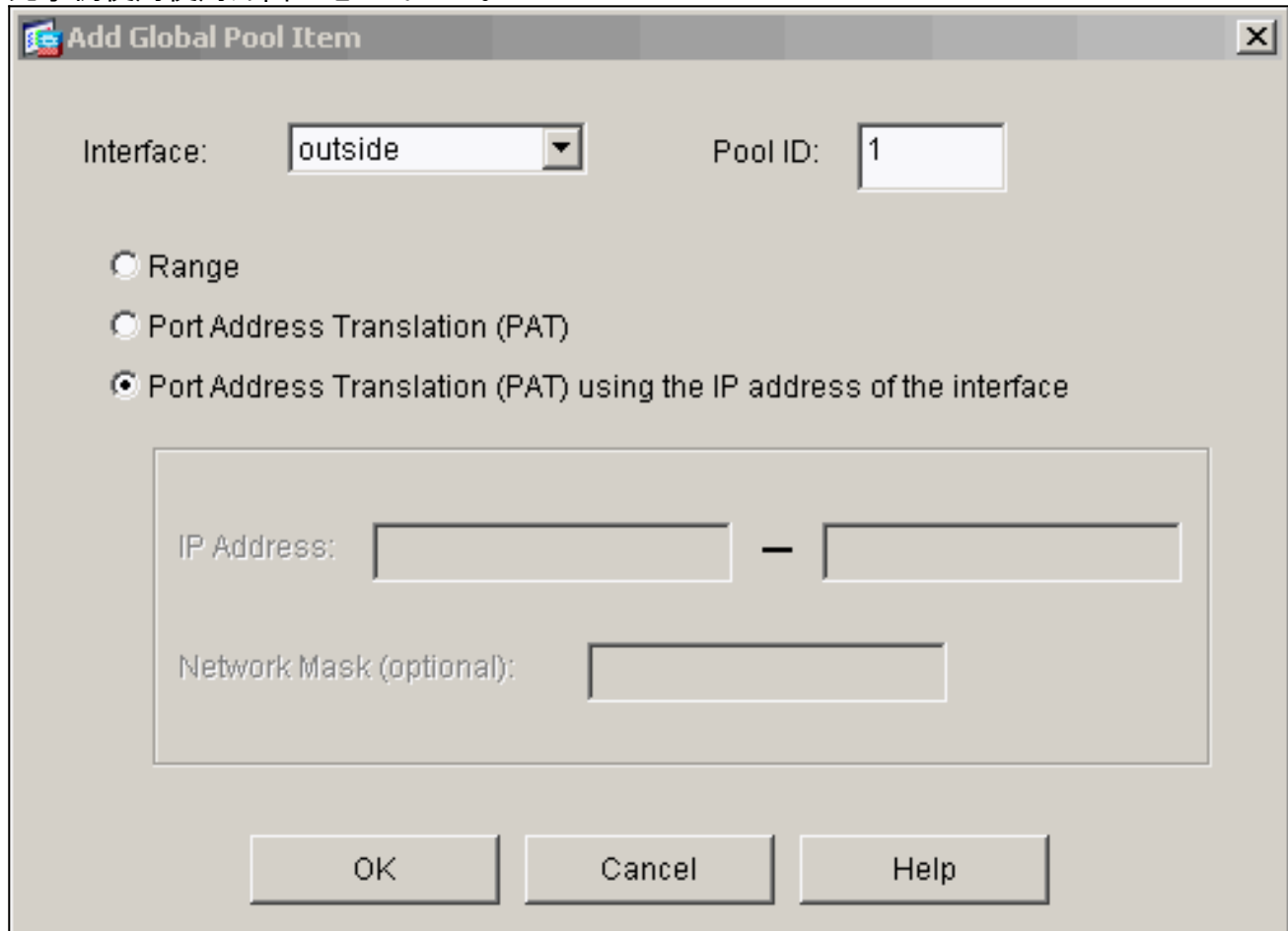
 Dynamic Address Pool:

Pool ID	Address
N/A	No address pool defined

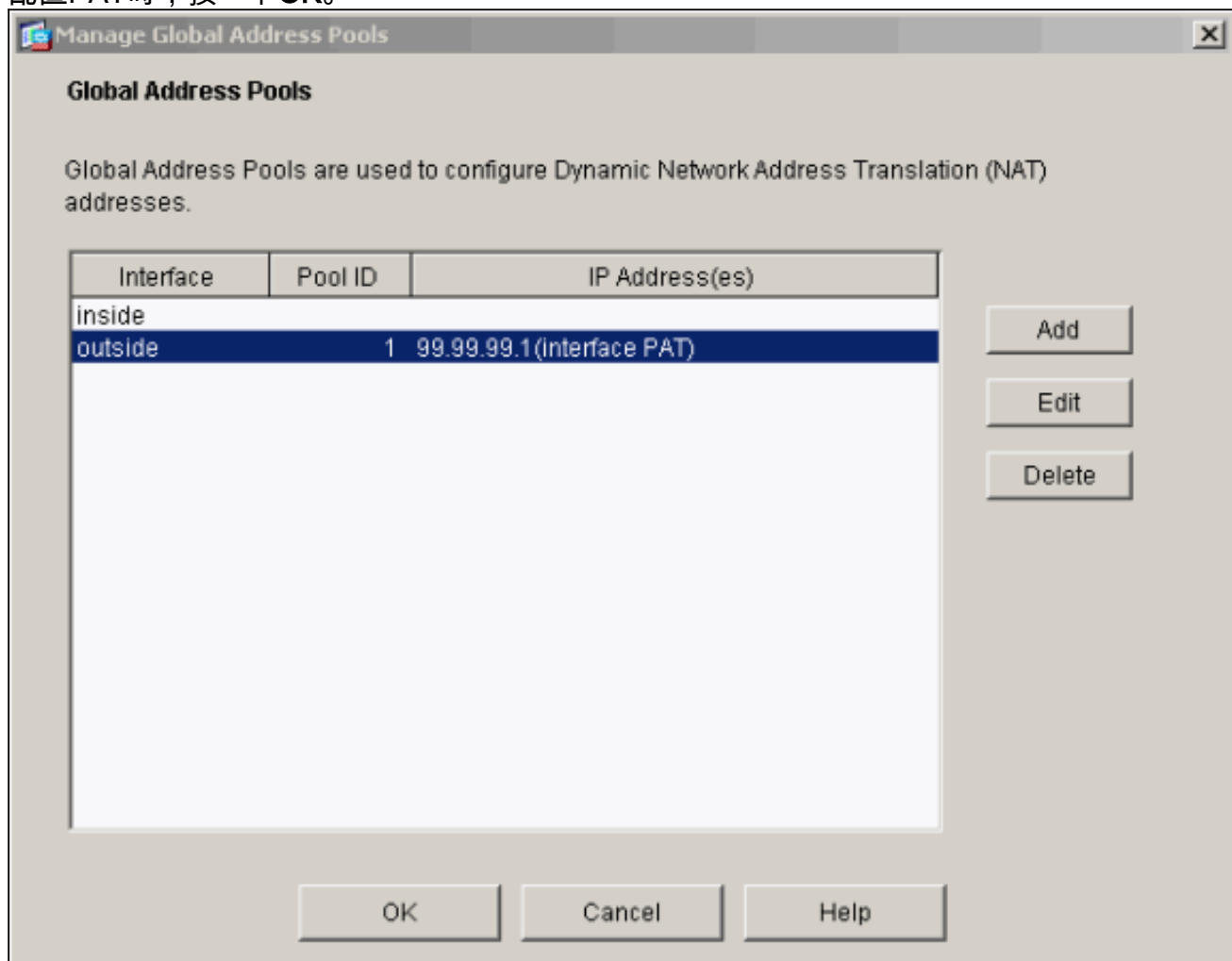
17. 選擇outside介面，然後按一下Add。



此示例使用使用介面IP地址的PAT。



18. 配置PAT時，按一下OK。



19. 按一下Add以設定靜態轉譯。

Source Host/Network

Interface: inside

IP Address: 0.0.0.0

Mask: 0.0.0.0

Browse ...

NAT Options...

Translate Address on Interface: outside

Translate Address To

Static IP Address:

Redirect port

TCP Original port: Translated port:

UDP

Dynamic Address Pool: same address Manage Pools...

Pool ID	Address
1	99.99.99.1 (interface PAT)

OK Cancel Help

20. 在Interface (介面) 下拉選單中選擇inside，然後輸入IP地址10.1.1.2，子網掩碼255.255.255.255，選擇**Static**，然後在IP Address (IP地址) 欄位中鍵入outside address 99.99.12。完成後，按一下**OK**。

Add Address Translation Rule

Use NAT Use Policy NAT

Source Host/Network


Interface:

IP Address:

Mask:

Translate Address on Interface:


Translate Address To

 Static IP Address:

Redirect port

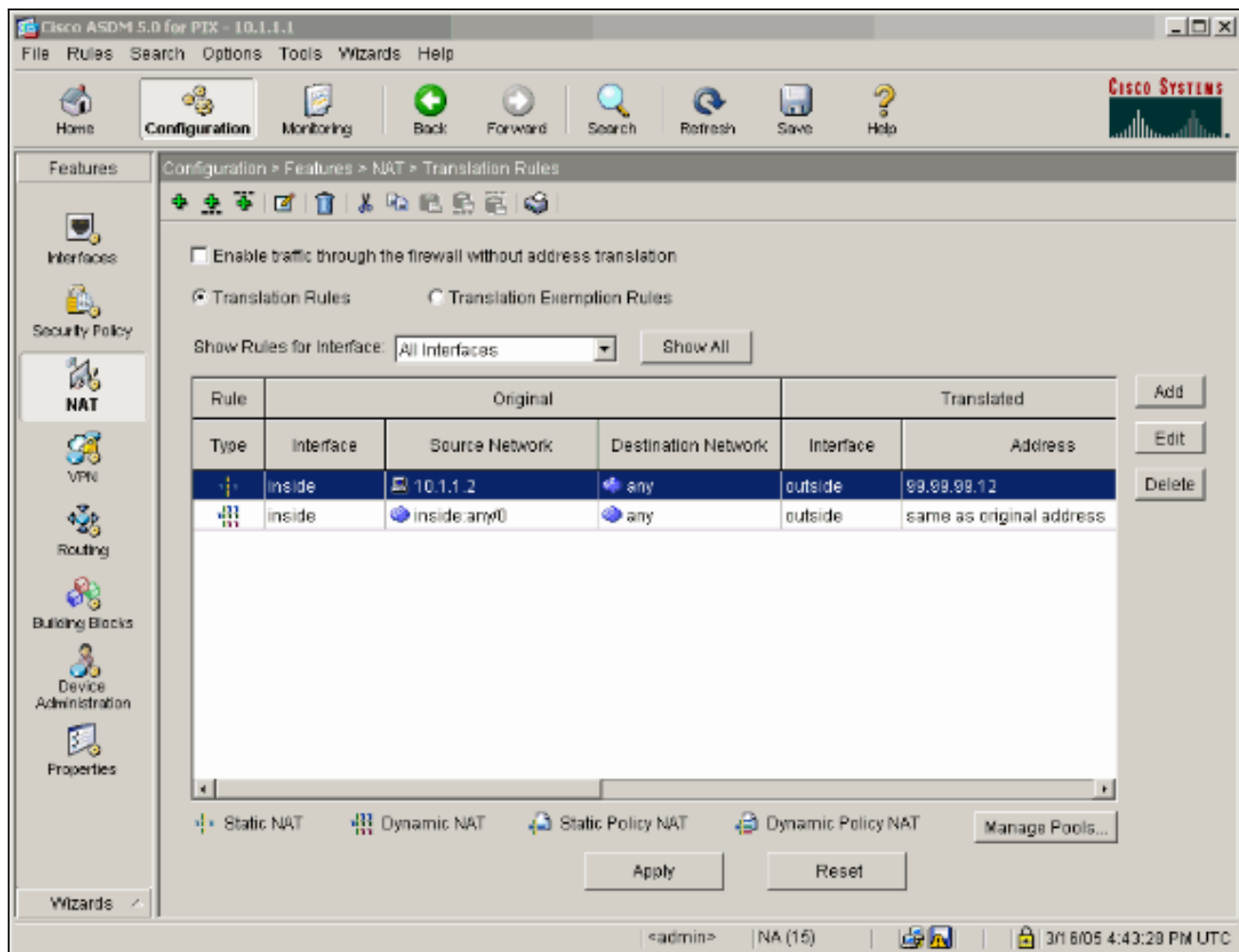
TCP Original port: Translated port:

UDP

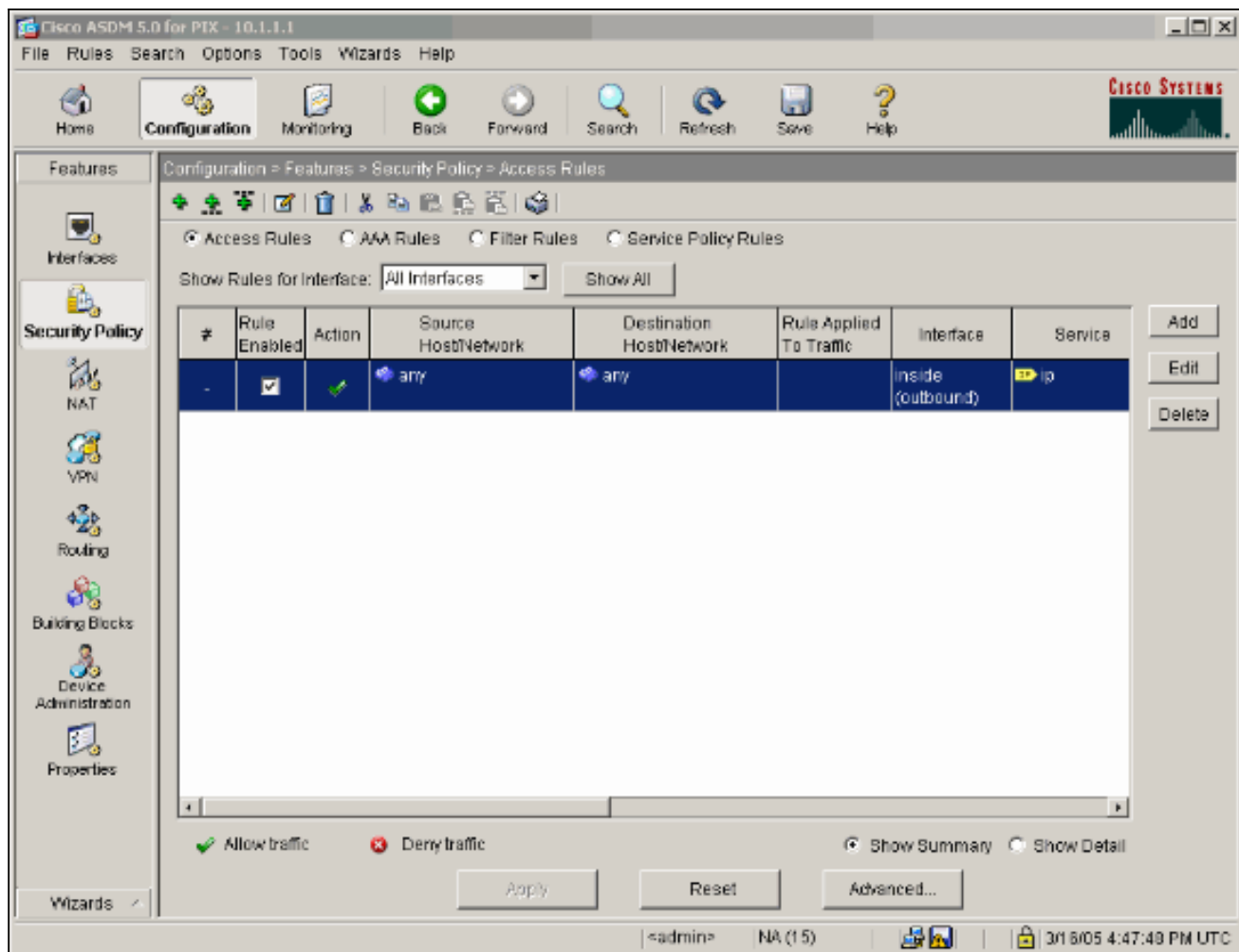
 Dynamic Address Pool:

Pool ID	Address

21. 按一下「Apply」以接受介面組態。該配置也將推到PIX上。



22. 在Features (功能) 頁籤下選擇Security Policy (安全策略) 以配置Security Policy (安全策略) 規則。



23. 按一下「Add」以允許esp流量，然後按一下「OK」以繼續。

Add Access Rule

Action
Select an action:
Apply to Traffic:

Syslog
Default Syslog

Time Range
Time Range:

Source Host/Network
 IP Address Name Group
Interface:
IP address:
Mask:

Destination Host/Network
 IP Address Name Group
Interface:
IP address:
Mask:

Rule Flow Diagram
Rule applied to traffic incoming to source interface

Protocol and Service
 TCP UDP ICMP IP
IP Protocol
IP protocol:

Please enter the description below (optional):

24. 按一下「Add」以允許ISAKMP流量，然後按一下「OK」以繼續。

Edit Access Rule

Action
 Select an action:
 Apply to Traffic:

Source Host/Network
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

Destination Host/Network
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

Rule Flow Diagram
 Rule applied to traffic incoming to source interface

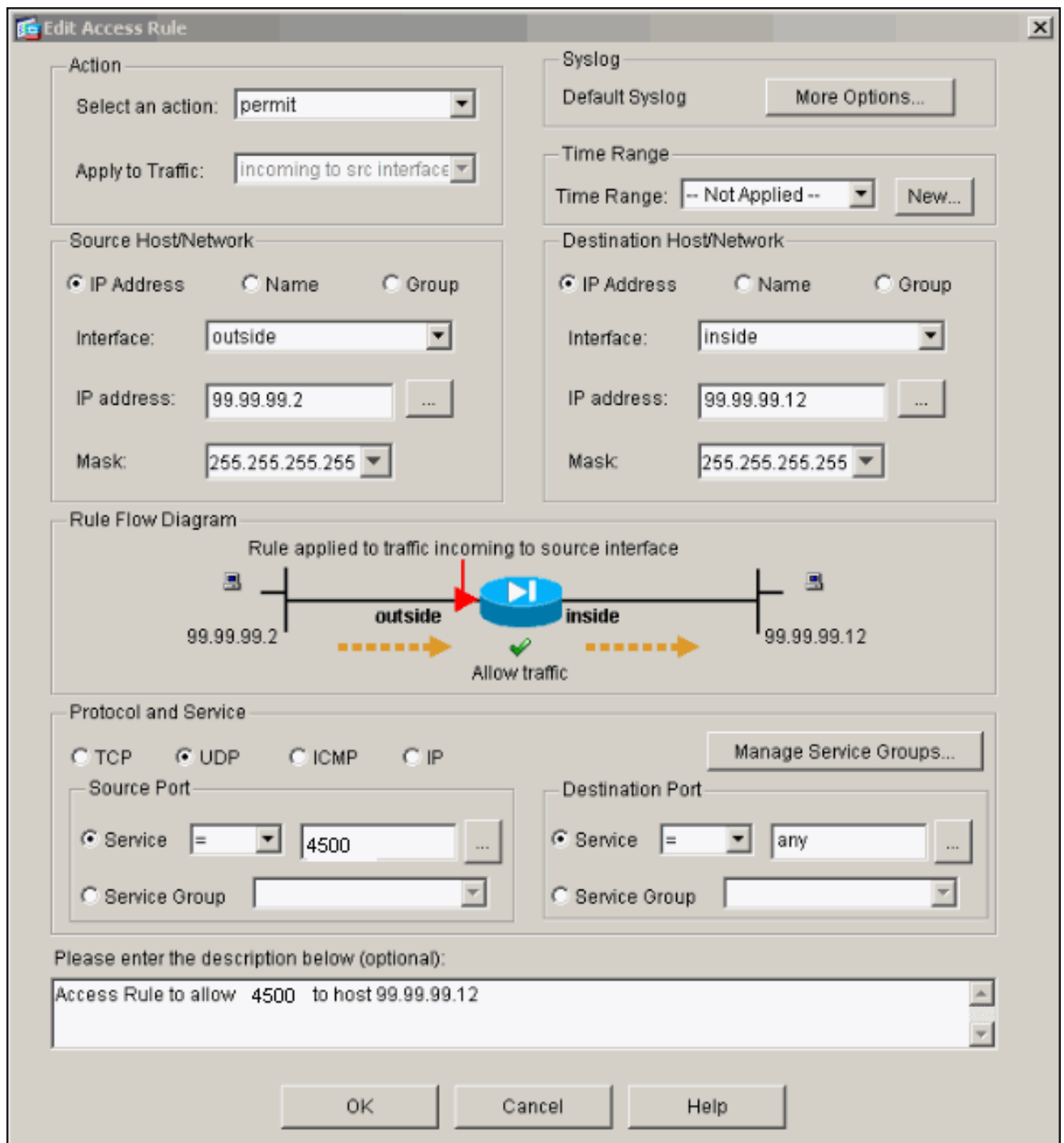
 99.99.99.2 outside inside 99.99.99.12
 Allow traffic

Protocol and Service
 TCP UDP ICMP IP Manage Service Groups...
Source Port
 Service = ...
 Service Group
Destination Port
 Service = ...
 Service Group

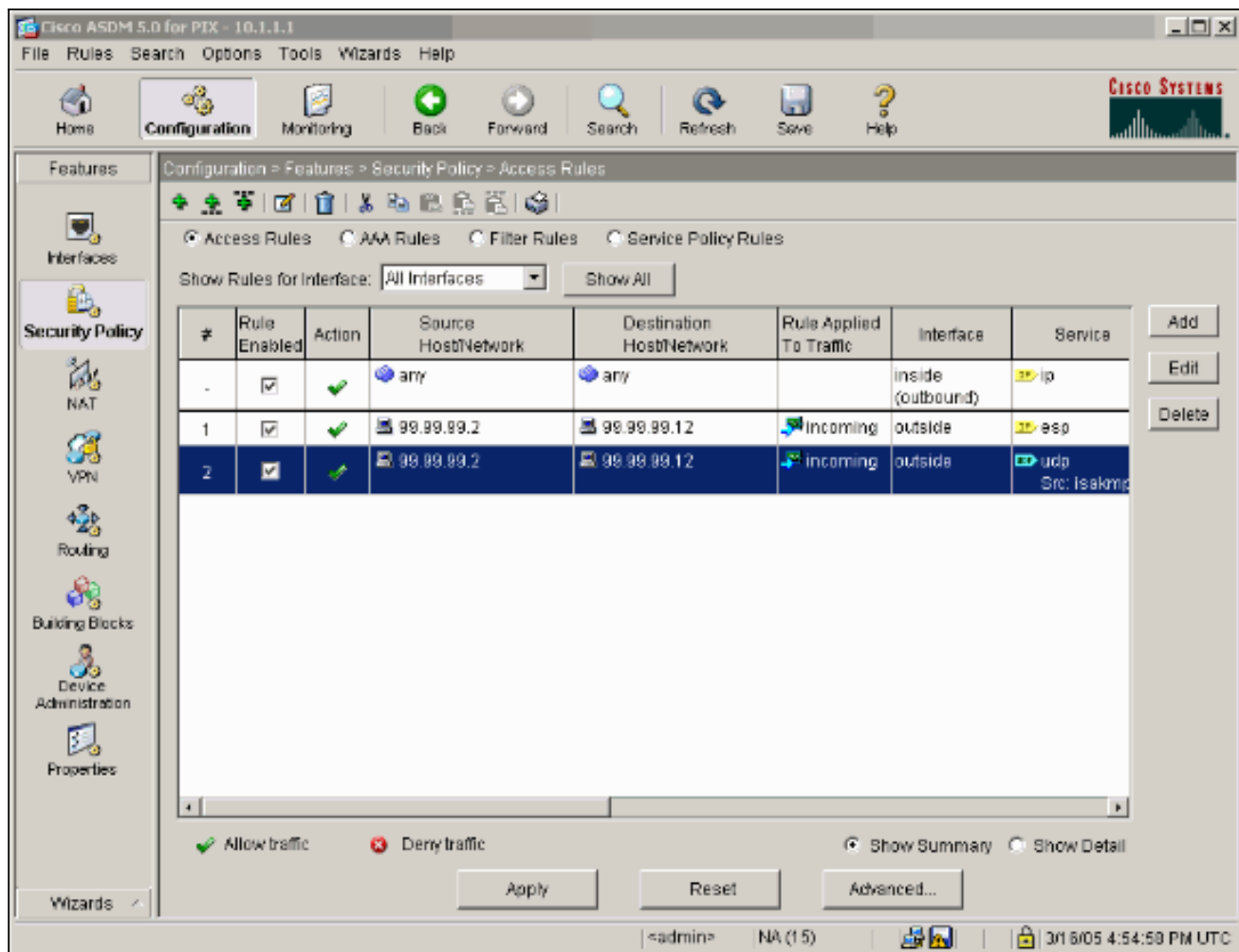
Please enter the description below (optional):

OK Cancel Help

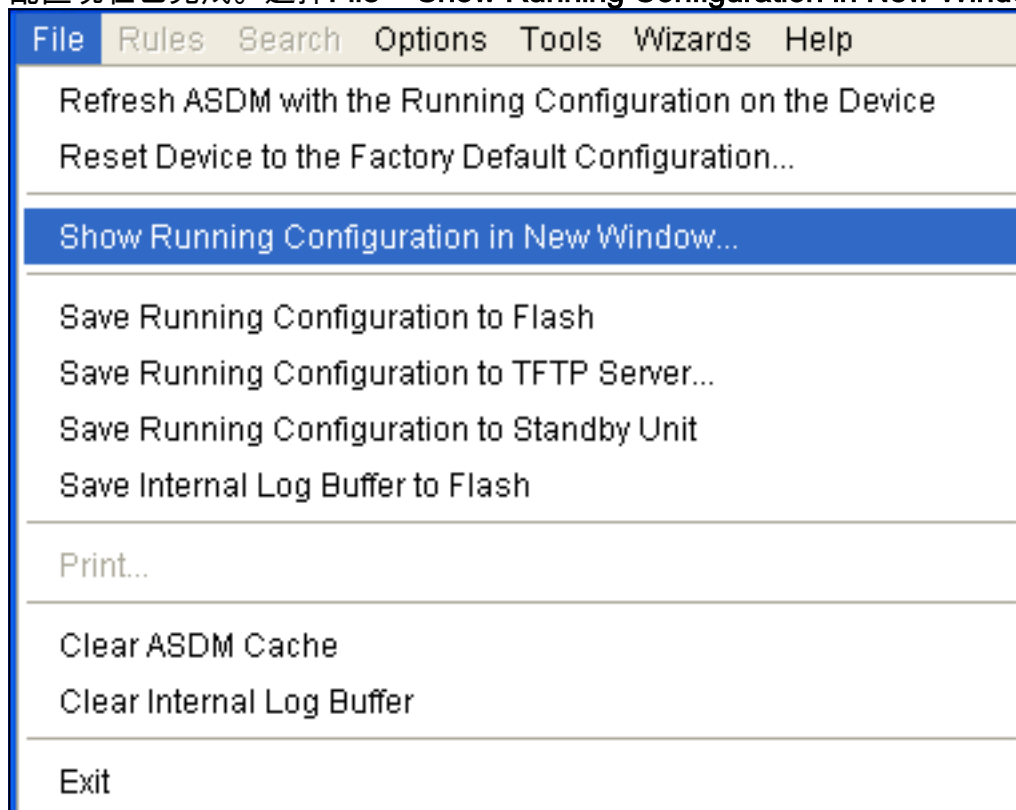
25. 按一下**Add**以允許NAT-T的UDP埠4500流量，然後按一下**OK**以繼續。



26. 按一下「Apply」以接受介面組態。該配置也將推到PIX上。



27. 配置現在已完成。選擇File > Show Running Configuration in New Window以檢視CLI配置。



PIX防火牆配置

PIX防火牆


```
pixfirewall# show run
: Saved
:
PIX Version 7.0(0)102
names
!
interface Ethernet0
  nameif outside
  security-level 0
  ip address 99.99.99.1 255.255.255.0
!
interface Ethernet1
  nameif inside
  security-level 100
  ip address 10.1.1.1 255.255.255.0
!
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
domain-name cisco.com
ftp mode passive

access-list outside_access_in remark Access Rule to
Allow ESP traffic
access-list outside_access_in
  extended permit esp host 99.99.99.2 host
99.99.99.12

access-list outside_access_in
  remark Access Rule to allow ISAKMP to host
99.99.99.12
access-list outside_access_in
  extended permit udp host 99.99.99.2 eq
isakmp host 99.99.99.12

access-list outside_access_in
  remark Access Rule to allow port 4500 (NAT-
T) to host 99.99.99.12
access-list outside_access_in
  extended permit udp host 99.99.99.2
eq 4500 host 99.99.99.12
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
monitor-interface inside
monitor-interface outside
asdm image flash:/asdmfile.50073
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 0 0.0.0.0 0.0.0.0
static (inside,outside) 99.99.99.12 10.1.1.2 netmask
255.255.255.255
access-group outside_access_in in interface outside
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1
route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
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
http 10.1.1.3 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map asa_global_fw_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
!
service-policy asa_global_fw_policy global
Cryptochecksum:0a12956036ce4e7a97f351cde61fba7e
: end

```

[PIX安全裝置和MPF \(模組化策略框架 \) 配置](#)

使用命令**inspect ipsec-pass-thru** in MPF(Modular Policy Framework)而不是訪問清單，以便通過PIX/ASA安全裝置傳遞IPsec流量。

此檢測配置為開啟ESP流量的針孔。如果存在轉發流，則允許所有ESP資料流，並且允許的最大連線數沒有限制。不允許使用AH。預設情況下，ESP資料流的預設空閒超時設定為10分鐘。此檢查可應用於可以應用其他檢查的所有位置，包括類和match命令模式。IPSec直通應用檢測提供了與IKE UDP埠500連線關聯的ESP (IP協定50) 流量的便捷遍歷。它可避免冗長的訪問清單配置來允許ESP流量，還可通過超時和最大連線提供安全性。使用**class-map**、**policy-map**和**service-policy**命令可定義流量類、將**inspect**命令應用於該類，以及將策略應用於一個或多個介面。啟用時，**inspect IPsec-pass-thru**命令允許無限制ESP流量，超時為10分鐘，這是不可配置的。允許NAT和非NAT流量。

```

hostname(config)#access-list test-udp-acl extended permit udp any any eq 500
hostname(config)#class-map test-udp-class
hostname(config-cmap)#match access-list test-udp-acl
hostname(config)#policy-map test-udp-policy
hostname(config-pmap)#class test-udp-class
hostname(config-pmap-c)#inspect ipsec-pass-thru
hostname(config)#service-policy test-udp-policy interface outside

```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

[輸出直譯器工具](#)(僅供註冊客戶使用)支援某些show命令，此工具可讓您檢視show命令輸出的分析。

- show crypto ipsec sa — 顯示第2階段安全關聯。
- show crypto isakmp sa — 顯示第1階段安全關聯。
- show crypto engine connections active — 顯示加密和解密的資料包。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

路由器IPsec的故障排除命令

註：發出debug指令之前，請先參閱有關Debug指令的**重要**資訊。

- debug crypto engine — 顯示加密的流量。
- debug crypto ipsec — 顯示第2階段的IPsec協商。
- debug crypto isakmp — 顯示第1階段的網際網路安全關聯和金鑰管理協定(ISAKMP)協商。

清除安全關聯

- clear crypto isakmp — 清除網際網路金鑰交換(IKE)安全關聯。
- clear crypto ipsec sa — 清除IPsec安全關聯。

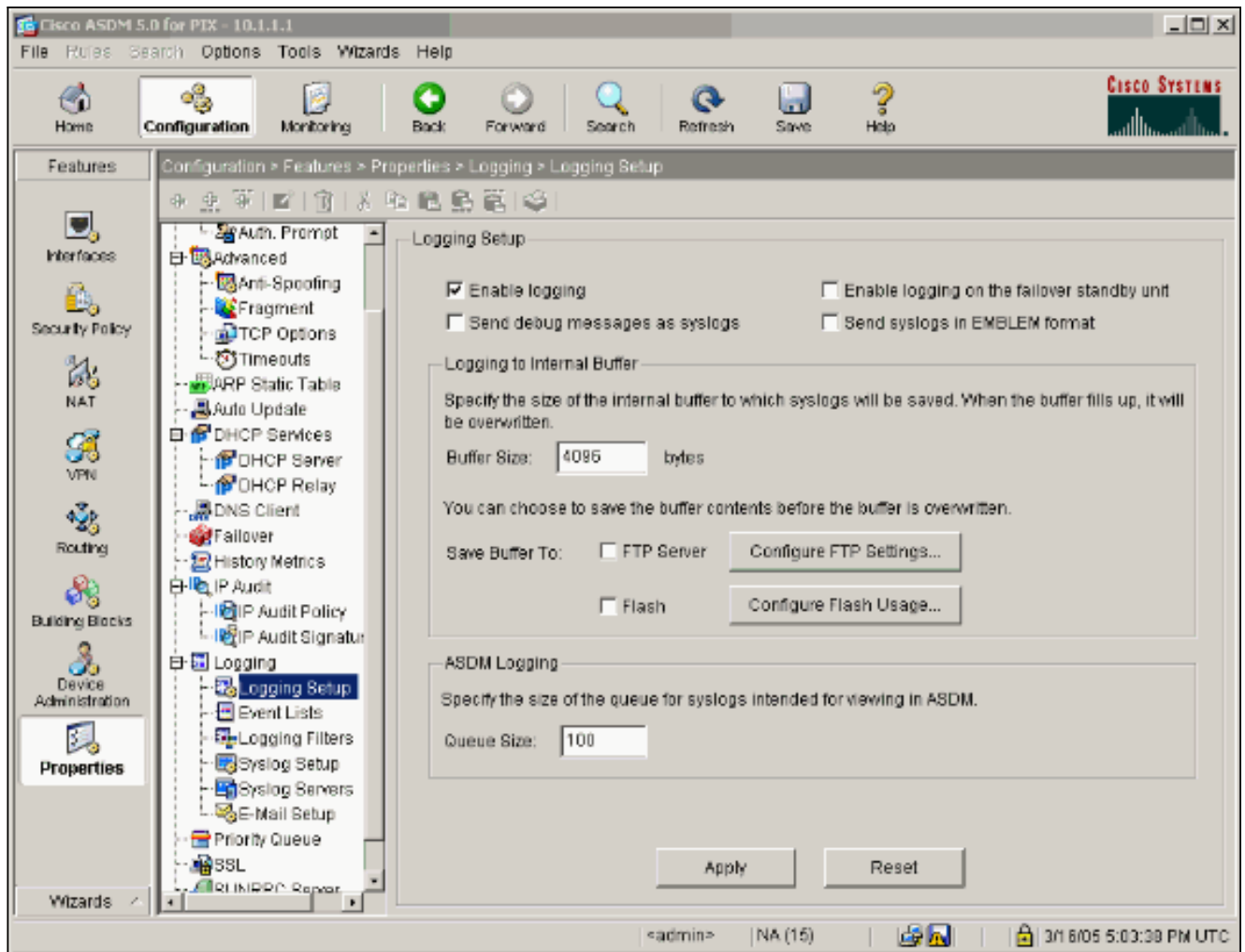
PIX故障排除命令

[輸出直譯器工具](#)(僅供註冊客戶使用)支援某些show命令，此工具可讓您檢視show命令輸出的分析。

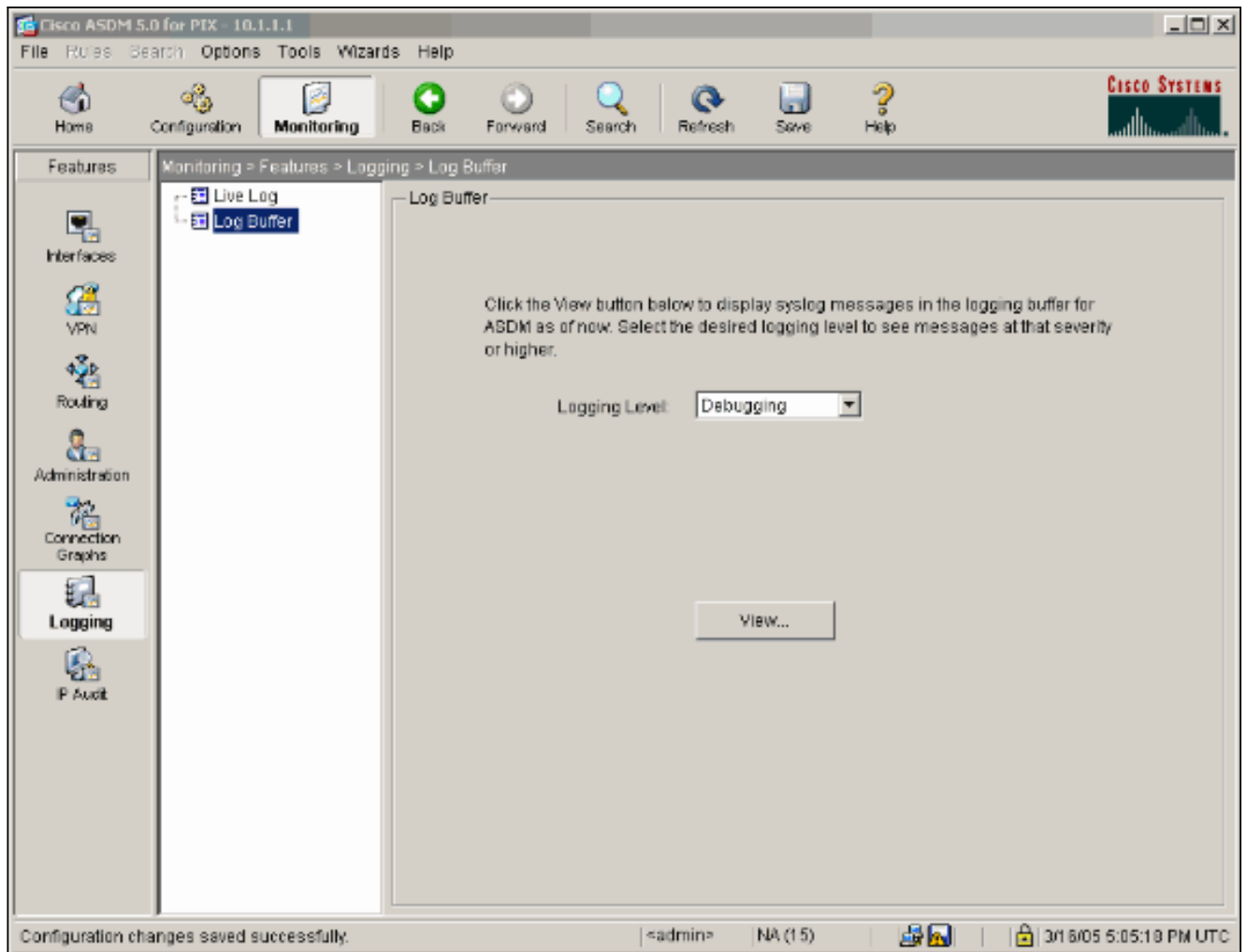
註：發出debug指令之前，請先參閱有關Debug指令的**重要**資訊。

- logging buffer debugging — 顯示正在建立並拒絕到通過PIX的主機的連線。資訊儲存在PIX日誌緩衝區中，可以使用show log命令檢視輸出。
- ASDM可用於啟用日誌記錄以及檢視日誌，如以下步驟所示。

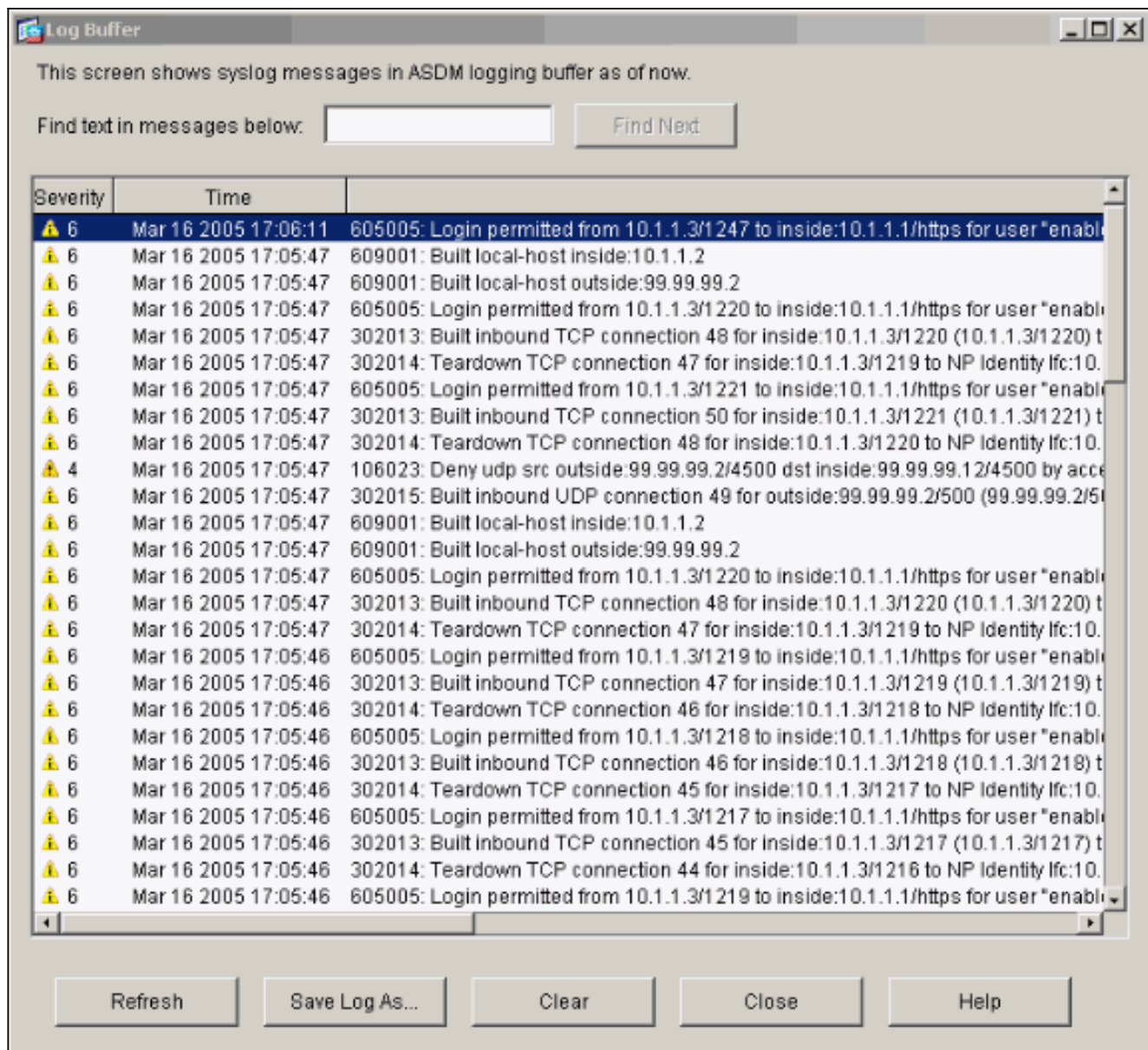
1. 選擇Configuration > Properties > Logging > Logging Setup > Enable Logging，然後按一下Apply。



2. 選擇 Monitoring > Logging > Log Buffer > On Logging Level > Logging Buffer，然後按一下 View。



以下是日誌緩衝區的示例。



相關資訊

- [IPsec協商/IKE通訊協定支援頁面](#)
- [PIX支援頁](#)
- [PIX命令參考](#)
- [NAT支援頁面](#)
- [要求建議 \(RFC\)](#)
- [技術支援與文件 - Cisco Systems](#)