ASA/PIX — 配置Cisco IOS路由器LAN到LAN IPsec隧道

目錄

簡介

本文檔演示如何配置從PIX安全裝置7.x及更高版本，或者從一個內部網路到運行加密映像的2611路由器的IPSec隧道。為了簡便起見，使用了靜態路由。

有關路由器和PIX之間的LAN到LAN隧道配置的詳細資訊，請參閱配置IPSec — 路由器到PIX。

有關PIX防火牆和Cisco VPN 3000集中器之間的LAN到LAN隧道配置的詳細資訊，請參閱Cisco VPN 3000集中器和PIX防火牆之間的LAN到LAN IPSec隧道配置示例。

請參閱PIX 7.x和VPN 3000集中器之間的IPsec隧道配置示例，以瞭解有關LAN到LAN隧道位於PIX和VPN集中器之間的方案的詳細資訊。

請參閱採用TACACS+驗證的PIX/ASA 7.x增強型分支到客戶端VPN配置示例，以瞭解更多有關PIX之間的LAN到LAN隧道也允許VPN客戶端通過中心PIX訪問分支PIX的方案的資訊。

請參閱SDM:ASA/PIX和IOS路由器之間的站點到站點IPsec VPN配置示例，以瞭解有關PIX/ASA安全裝置運行軟體版本8.x的相同方案的詳細資訊。

請參閱組態專業版：ASA/PIX和IOS路由器之間的站點到站點IPsec VPN配置示例以瞭解更多有關相同方案的資訊，其中使用ASDM GUI顯示ASA相關配置，使用Cisco CP GUI顯示路由器相關配置。

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：

- PIX-525，帶PIX軟體版本7.0
- 採用Cisco IOS®軟體版本12.2(15)T13的Cisco 2611路由器

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。

背景資訊

在PIX上，**access-list**和**nat 0**命令協同工作。10.1.1.0網路上的使用者進入10.2.2.0網路時，訪問清單用於允許10.1.1.0網路流量在不使用網路地址轉換(NAT)的情況下進行加密。 在路由器上，**route-map**和**access-list**命令用於允許不使用NAT加密10.2.2.0網路流量。但是，當這些相同使用者轉到其他任何位置時，會通過埠地址轉換(PAT)將其轉換為172.17.63.230地址。

以下是在PIX安全裝置上所需的配置命令，以便流量*不通過PAT通過隧道，以及到Internet的流量通過PAT*

```
access-list nonat permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
nat (inside) 0 access-list nonat
nat (inside) 1 10.1.1.0 255.255.255.0 0 0
```

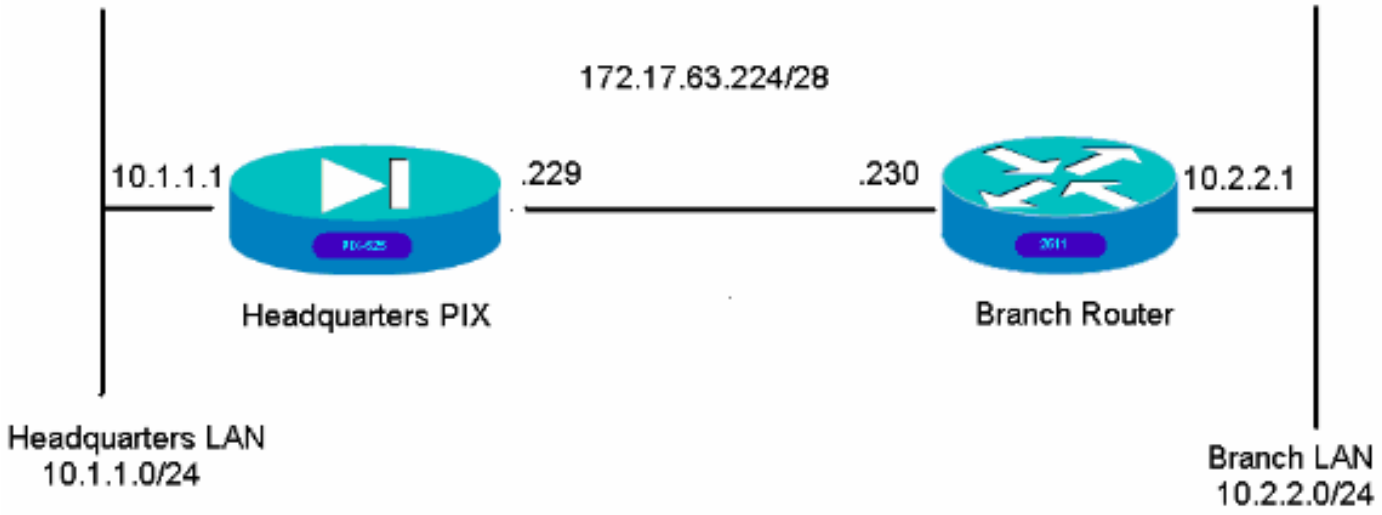
設定

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。

網路圖表

本檔案會使用以下網路設定：



組態

這些配置示例用於命令列介面。如果您希望使用ASDM進行配置，請參閱本文檔的使用自適應安全裝置管理器(ASDM)配置部分。

- 總部PIX
- 分支機構路由器

總部PIX

```
HQPIX(config)#show run
PIX Version 7.0(0)102
names
!
interface Ethernet0
description WAN interface
nameif outside
security-level 0
ip address 172.17.63.229 255.255.255.240
!
interface Ethernet1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface Ethernet2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet3
```

```
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname HQPIX
domain-name cisco.com
ftp mode passive
clock timezone AEST 10

access-list Ipsec-conn extended permit ip 10.1.1.0
255.255.255.0 10.2.2.0 255.255.255.0
access-list nonat extended permit ip 10.1.1.0
255.255.255.0 10.2.2.0 255.255.255.0
pager lines 24
logging enable
logging buffered debugging
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 access-list nonat
nat (inside) 1 10.1.1.0 255.255.255.0
access-group 100 in interface inside
route outside 0.0.0.0 0.0.0.0 172.17.63.230 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
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server partner protocol tacacs+
username cisco password 3USUcOPFUiMCO4Jk encrypted
http server enable
http 10.1.1.2 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp
crypto ipsec transform-set avalanche esp-des esp-md5-
hmac
```

```
crypto ipsec security-association lifetime seconds 3600
crypto ipsec df-bit clear-df outside
crypto map forsberg 21 match address Ipsec-conn
crypto map forsberg 21 set peer 172.17.63.230
crypto map forsberg 21 set transform-set avalanche
crypto map forsberg interface outside
isakmp identity address
isakmp enable outside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash sha
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
tunnel-group 172.17.63.230 type ipsec-l2l
tunnel-group 172.17.63.230 ipsec-attributes
pre-shared-key *
!
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
inspect http
!
service-policy asa_global_fw_policy global
Cryptochecksum:3a5851f7310d14e82bdf17e64d638738
: end
SV-2-8#
```

分支機構路由器

```
BranchRouter#show run
Building configuration...

Current configuration : 1719 bytes
!
! Last configuration change at 13:03:25 AEST Tue Apr 5
2005
! NVRAM config last updated at 13:03:44 AEST Tue Apr 5
2005
```

```
!
version 12.2
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname BranchRouter
!
logging queue-limit 100
logging buffered 4096 debugging
!
username cisco privilege 15 password 0 cisco
memory-size iomem 15
clock timezone AEST 10
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
!
!
crypto isakmp policy 11
encr 3des
authentication pre-share
group 2
crypto isakmp key cisco123 address 172.17.63.229
!
!
crypto ipsec transform-set sharks esp-des esp-md5-hmac
!
crypto map nolan 11 ipsec-isakmp
set peer 172.17.63.229
set transform-set sharks
match address 120
!
!
!
!
!
!
!
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
mta receive maximum-recipients 0
!
!
!
!
interface Ethernet0/0
ip address 172.17.63.230 255.255.255.240
ip nat outside
no ip route-cache
no ip mroute-cache
half-duplex
crypto map nolan
!
interface Ethernet0/1
```

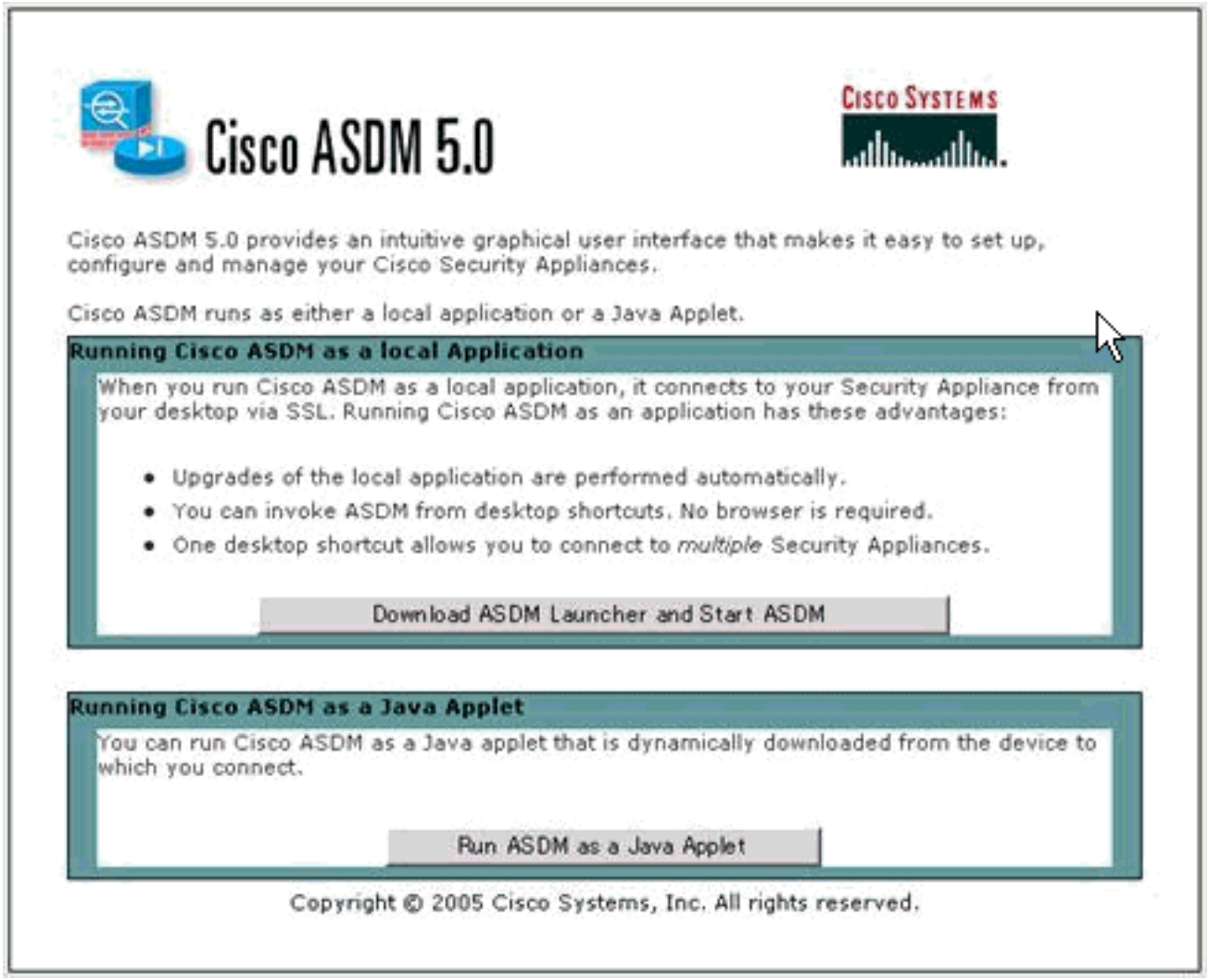
```
ip address 10.2.2.1 255.255.255.0
ip nat inside
half-duplex
!
ip nat pool branch 172.17.63.230 172.17.63.230 netmask
255.255.255.0
ip nat inside source route-map nonat pool branch
overload
no ip http server
no ip http secure-server
ip classless
ip route 10.1.1.0 255.255.255.0 172.17.63.229
!
!
!
access-list 120 permit ip 10.2.2.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 130 deny ip 10.2.2.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 130 permit ip 10.2.2.0 0.0.0.255 any
!
route-map nonat permit 10
match ip address 130
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
login
!
!
end
```

使用ASDM配置

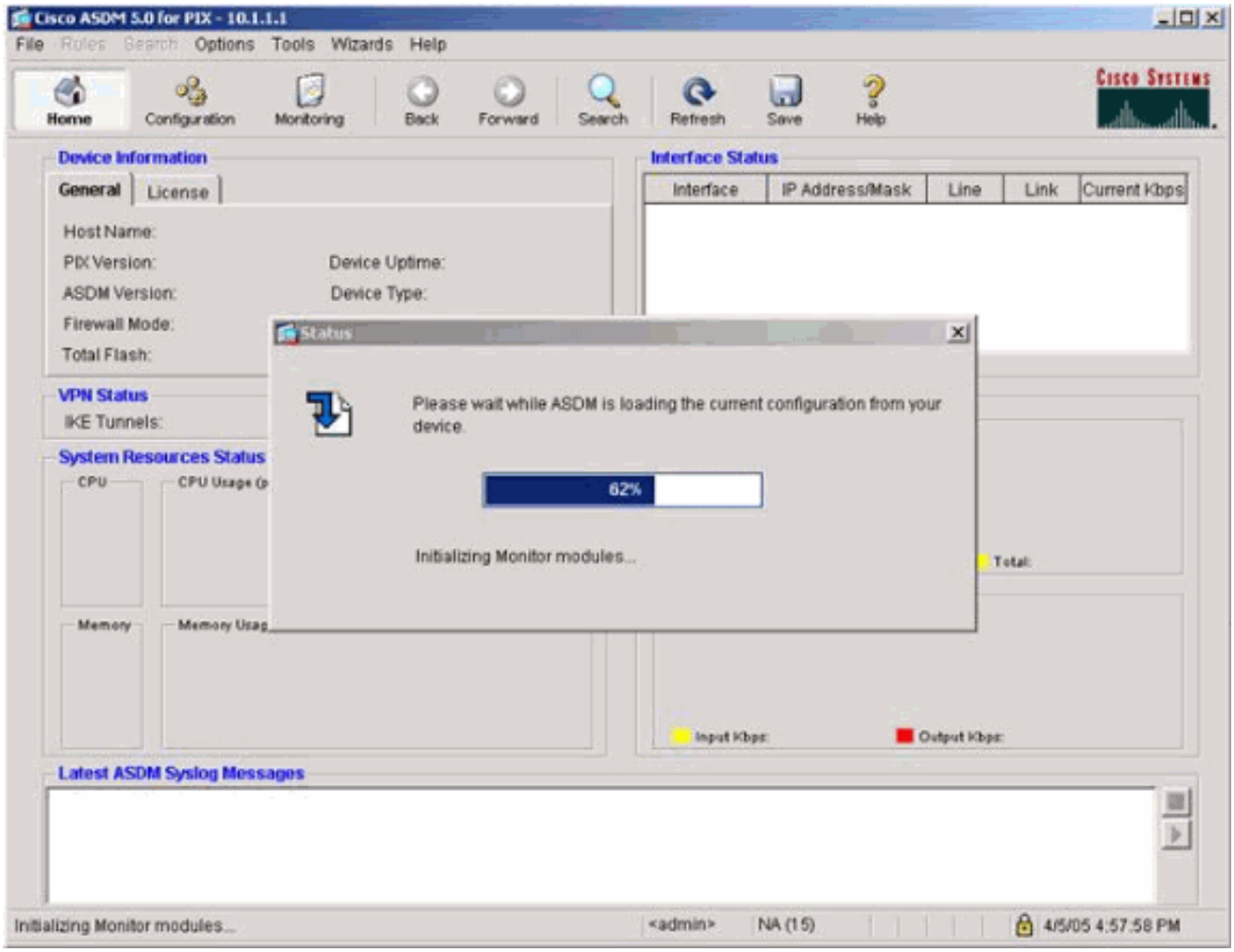
此示例演示如何使用ASDM GUI配置PIX。具有瀏覽器和IP地址10.1.1.2的PC連線到PIX的內部介面e1。確保PIX上啟用了http。

此過程說明總部PIX的ASDM配置。

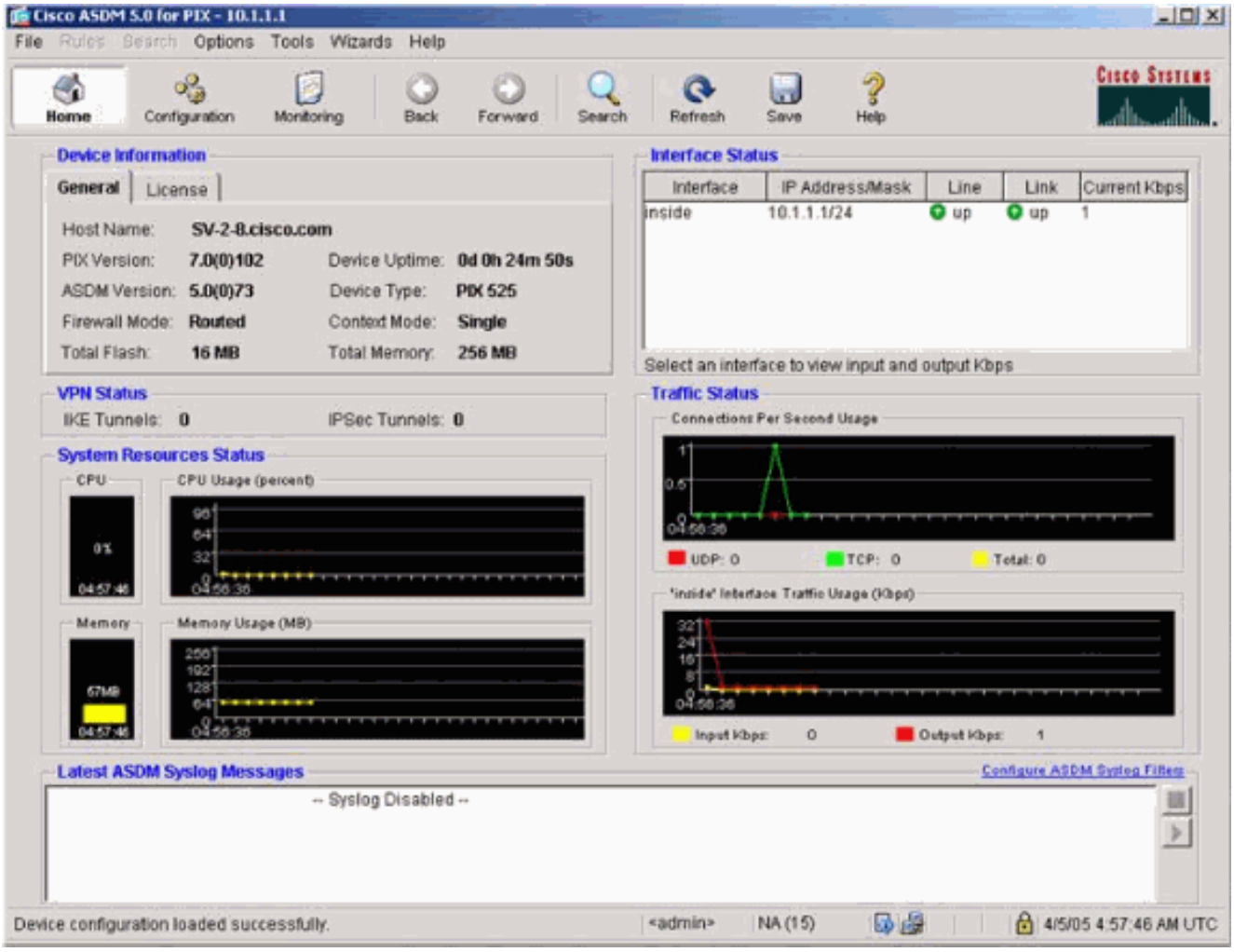
1. 將PC連線到PIX並選擇下載方法。



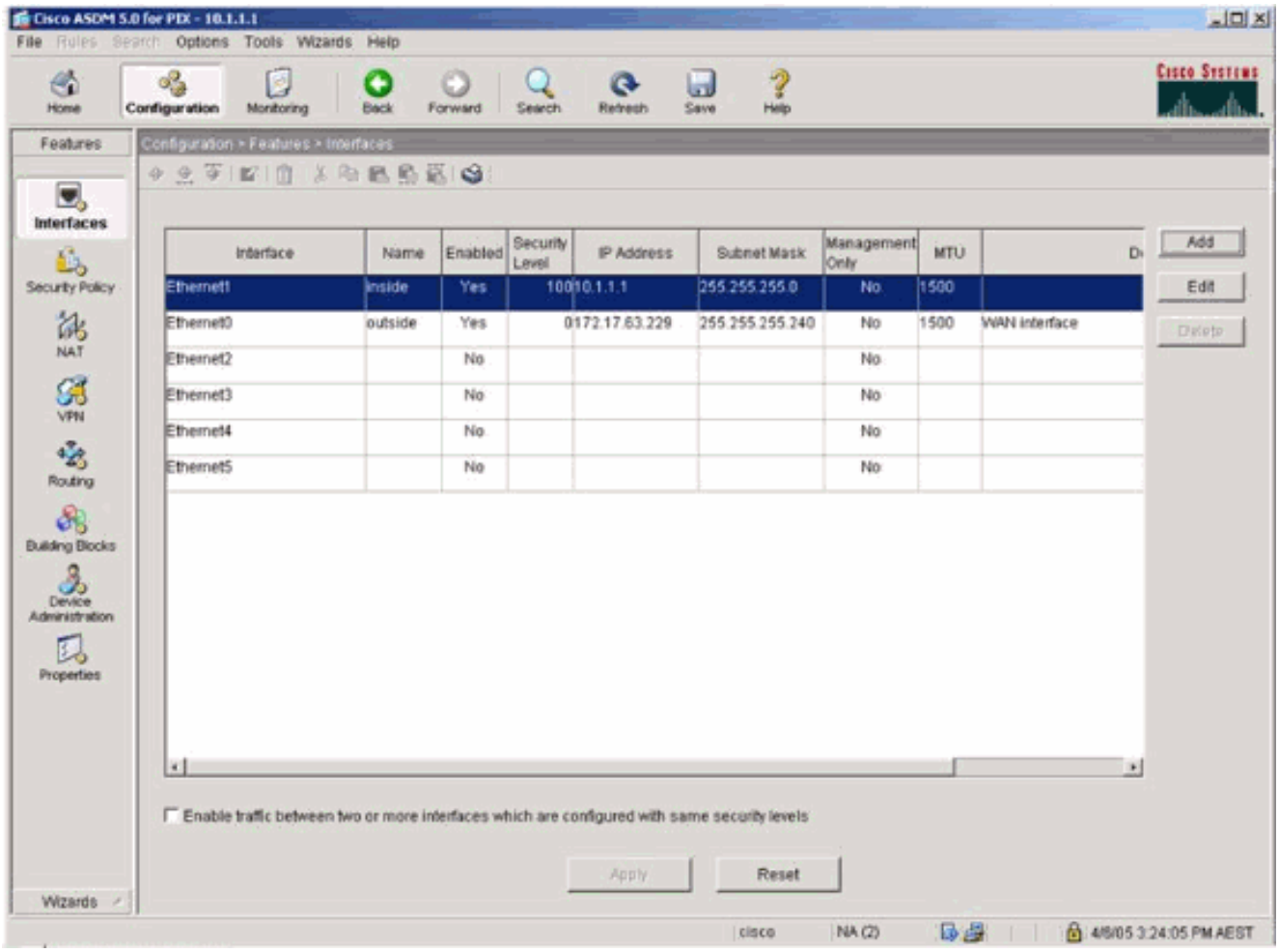
ASDM從PIX載入現有配置。



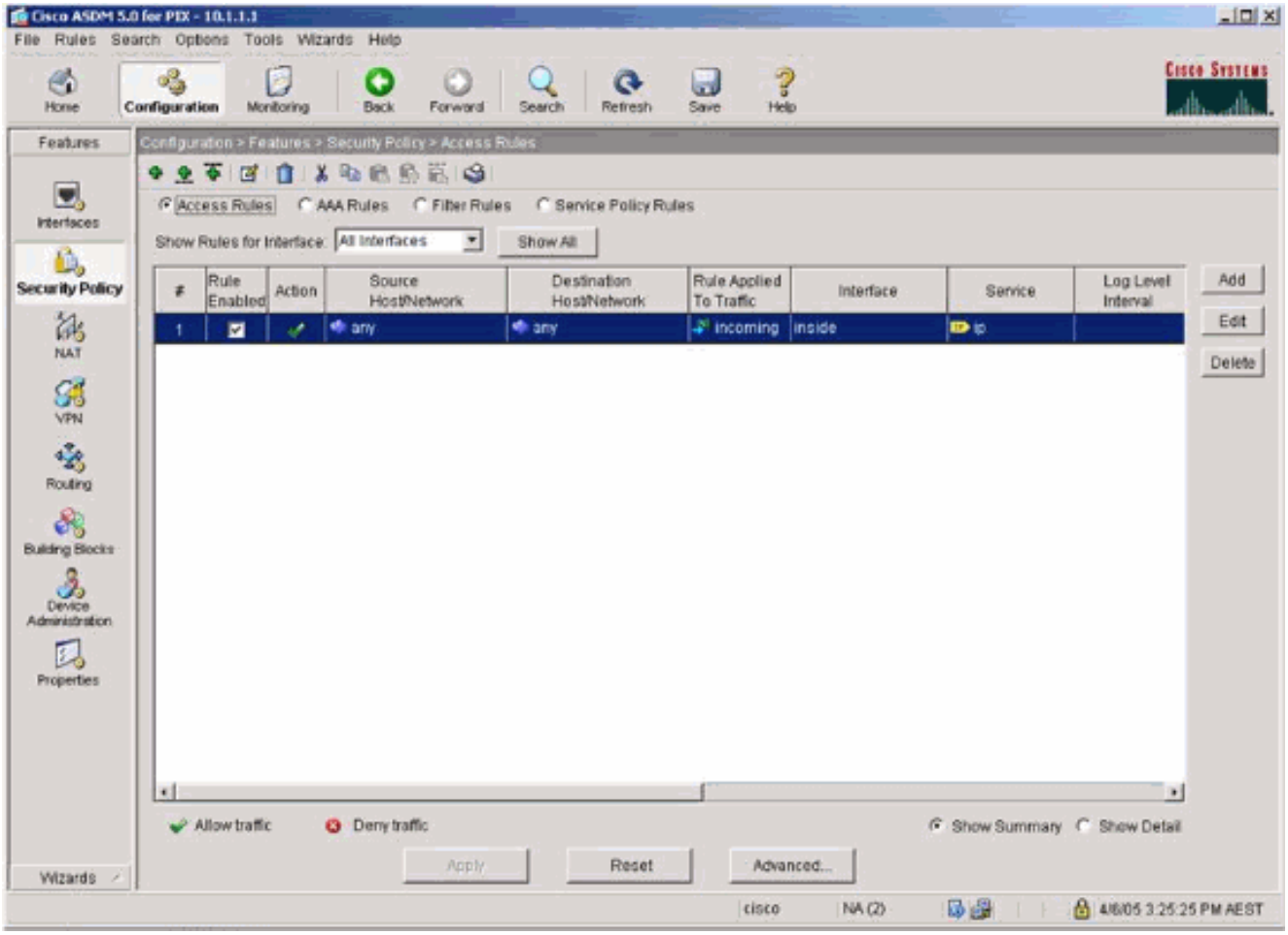
此視窗提供監控儀器和選單。



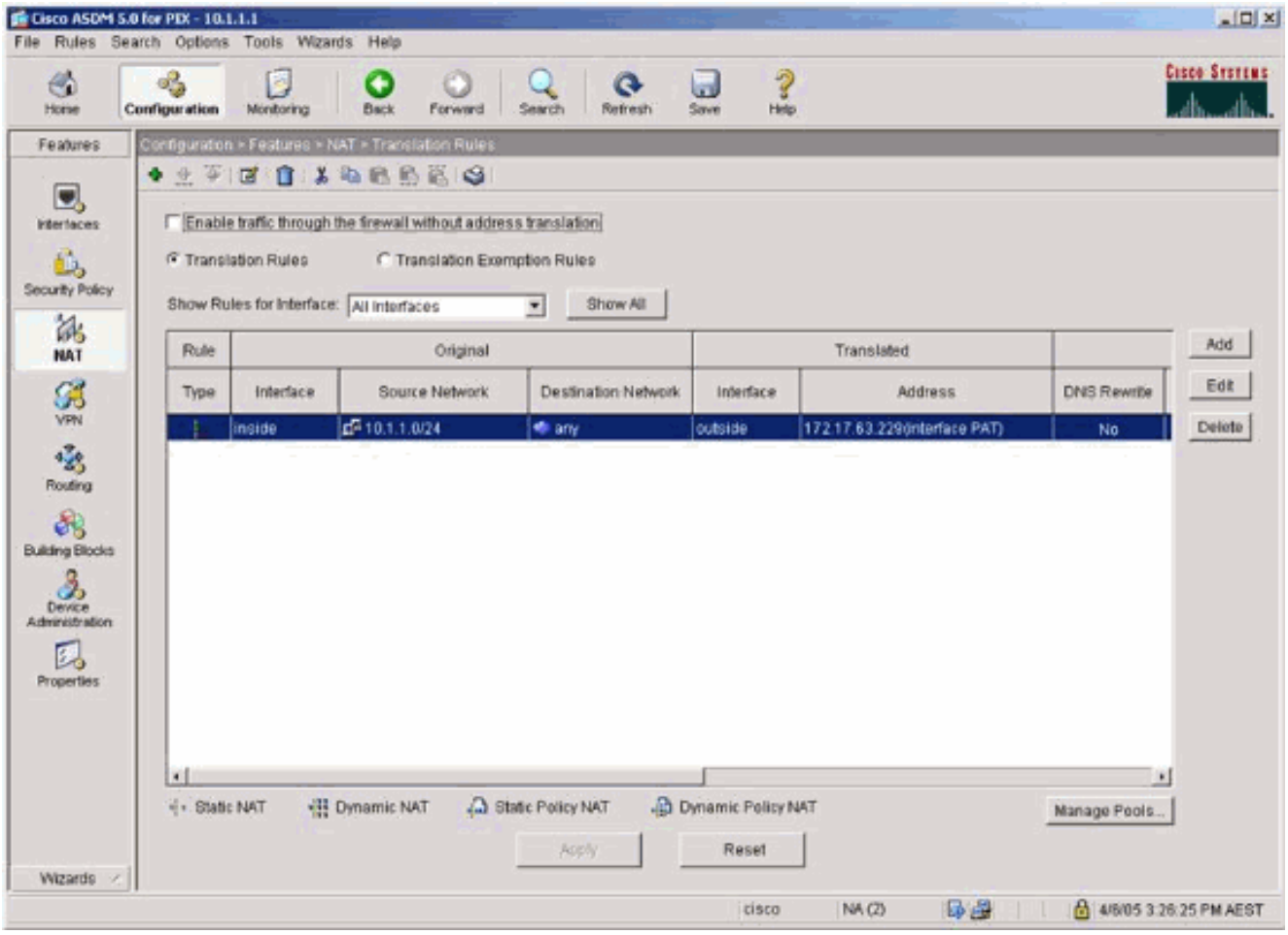
2. 選擇**Configuration > Features > Interfaces**，然後為新介面選擇**Add**，或者為現有配置選擇**Edit**。



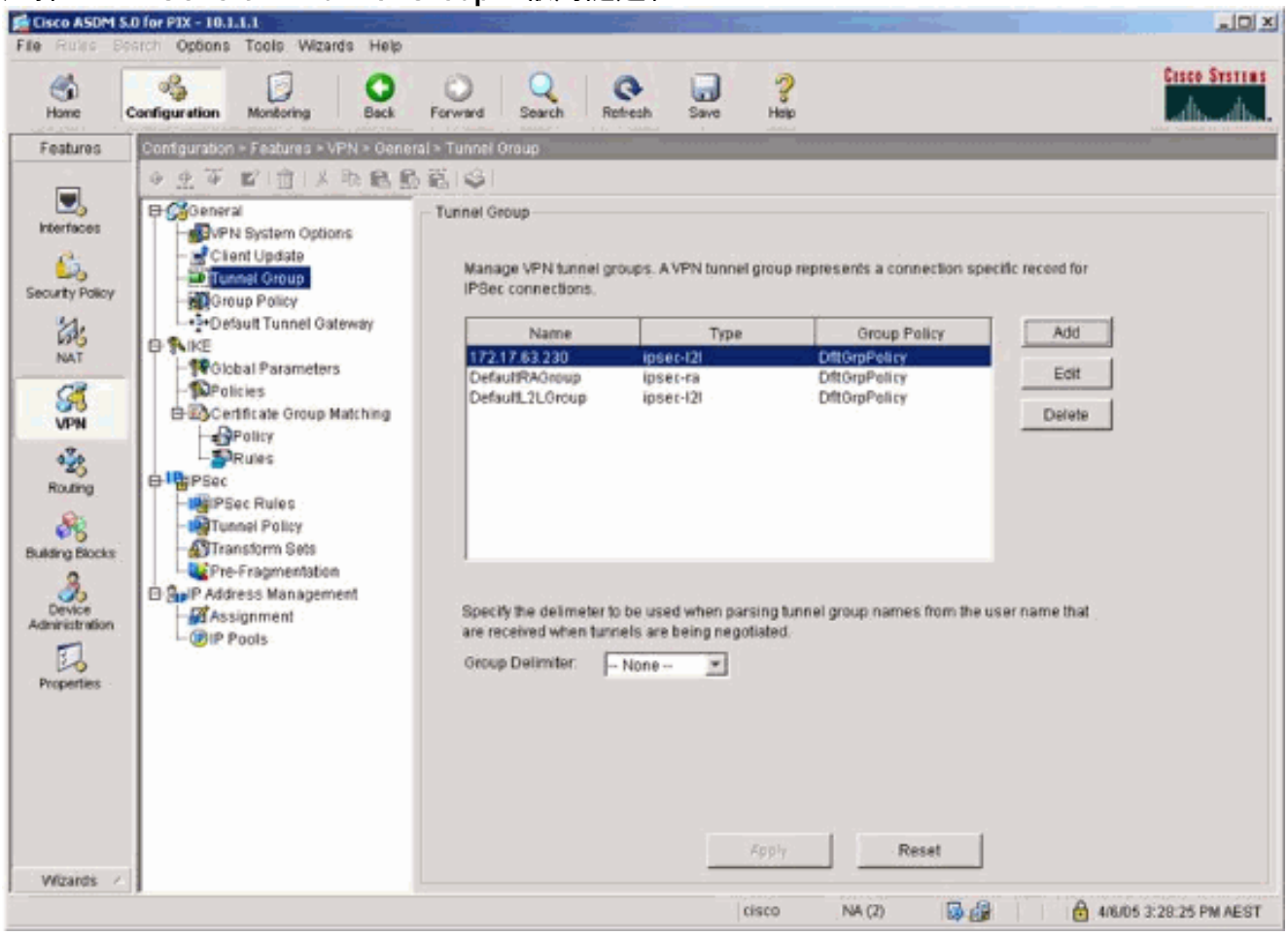
3. 選擇內部介面的安全選項。



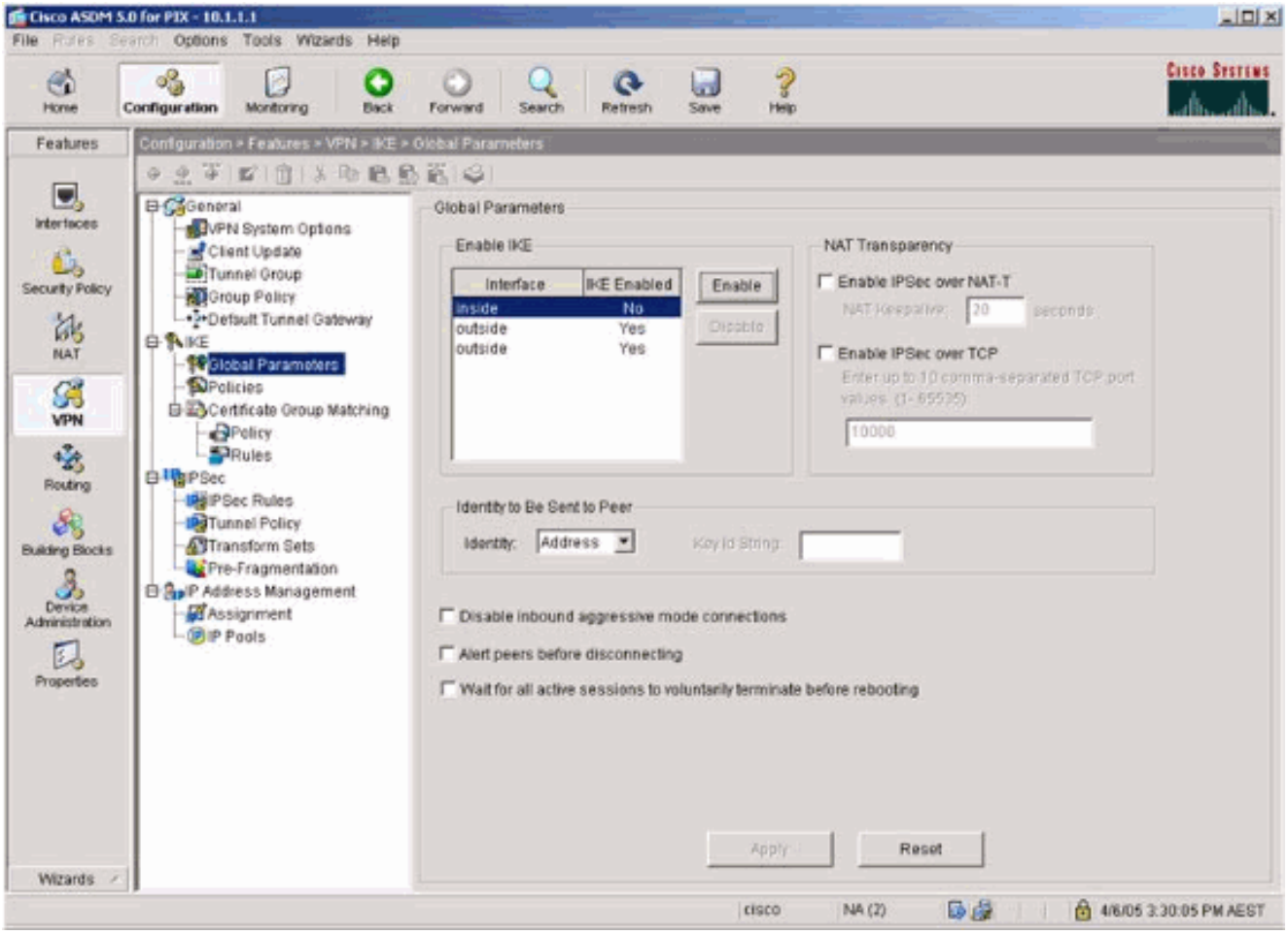
4. 在NAT配置中，加密流量是免除NAT的，所有其他流量是到外部介面的NAT/PAT。



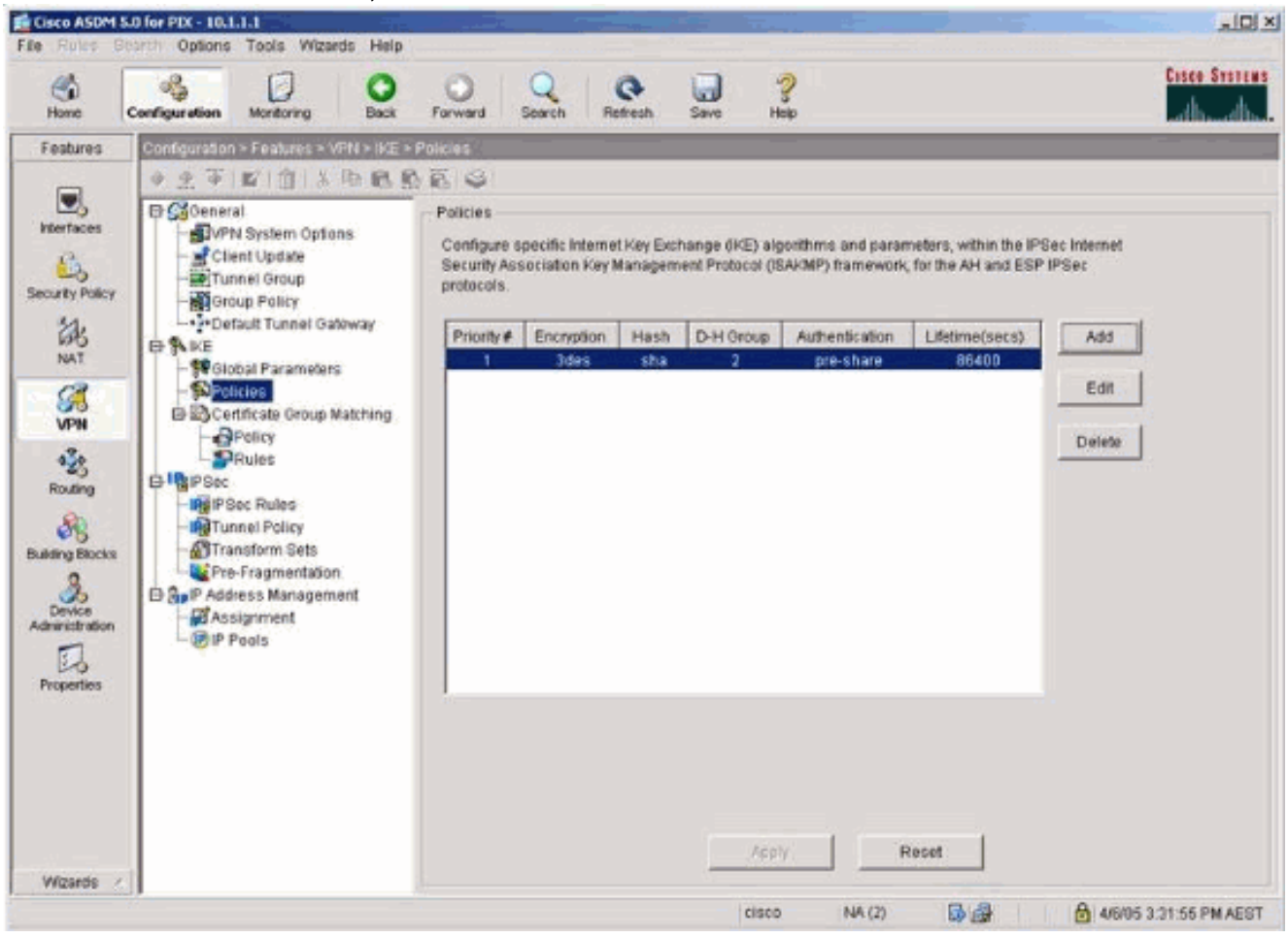
5. 選擇VPN >General > Tunnel Group並啟用隧道組



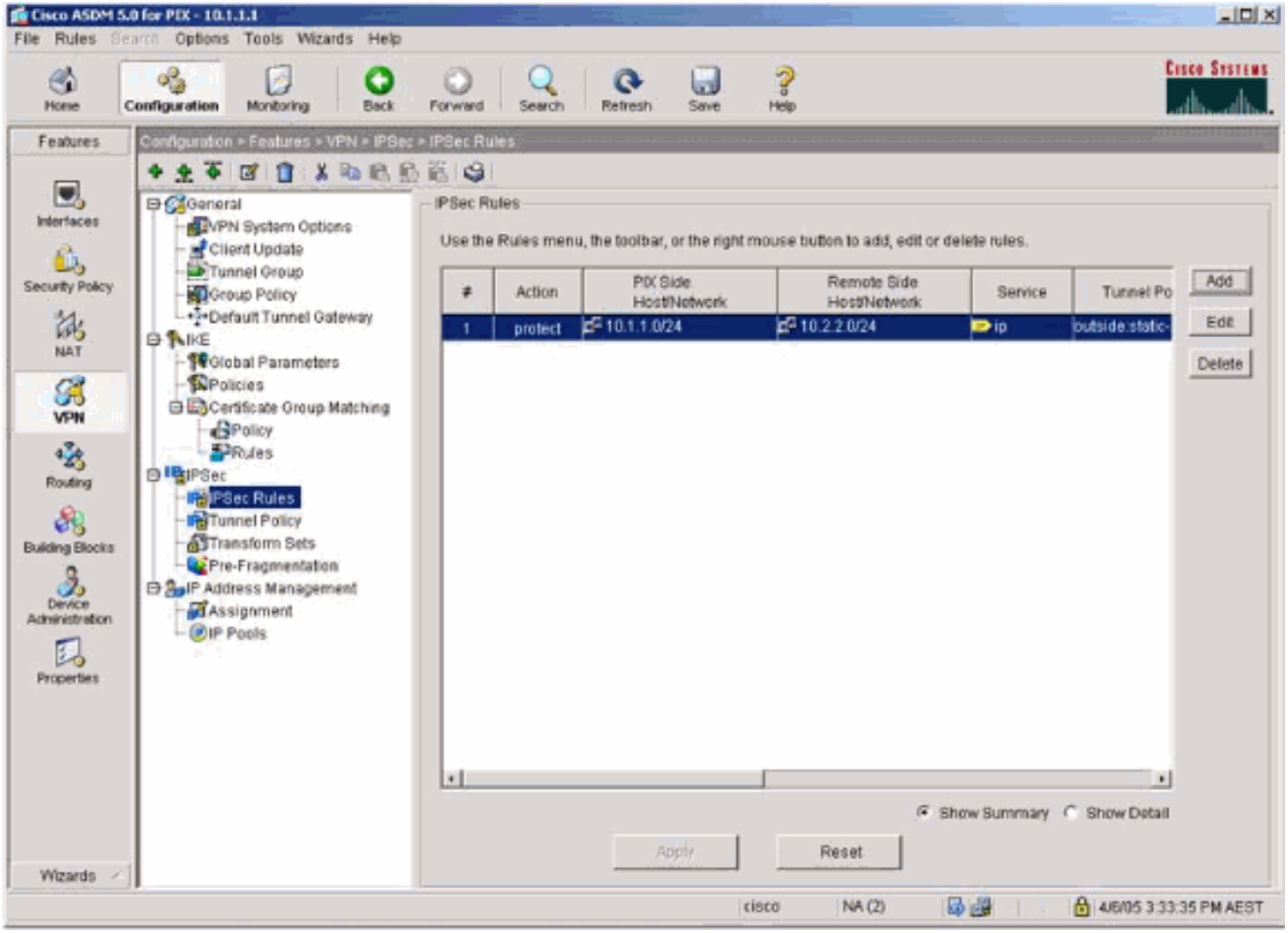
6. 選擇VPN > IKE > Global Parameters，並在外部介面上啟用IKE。



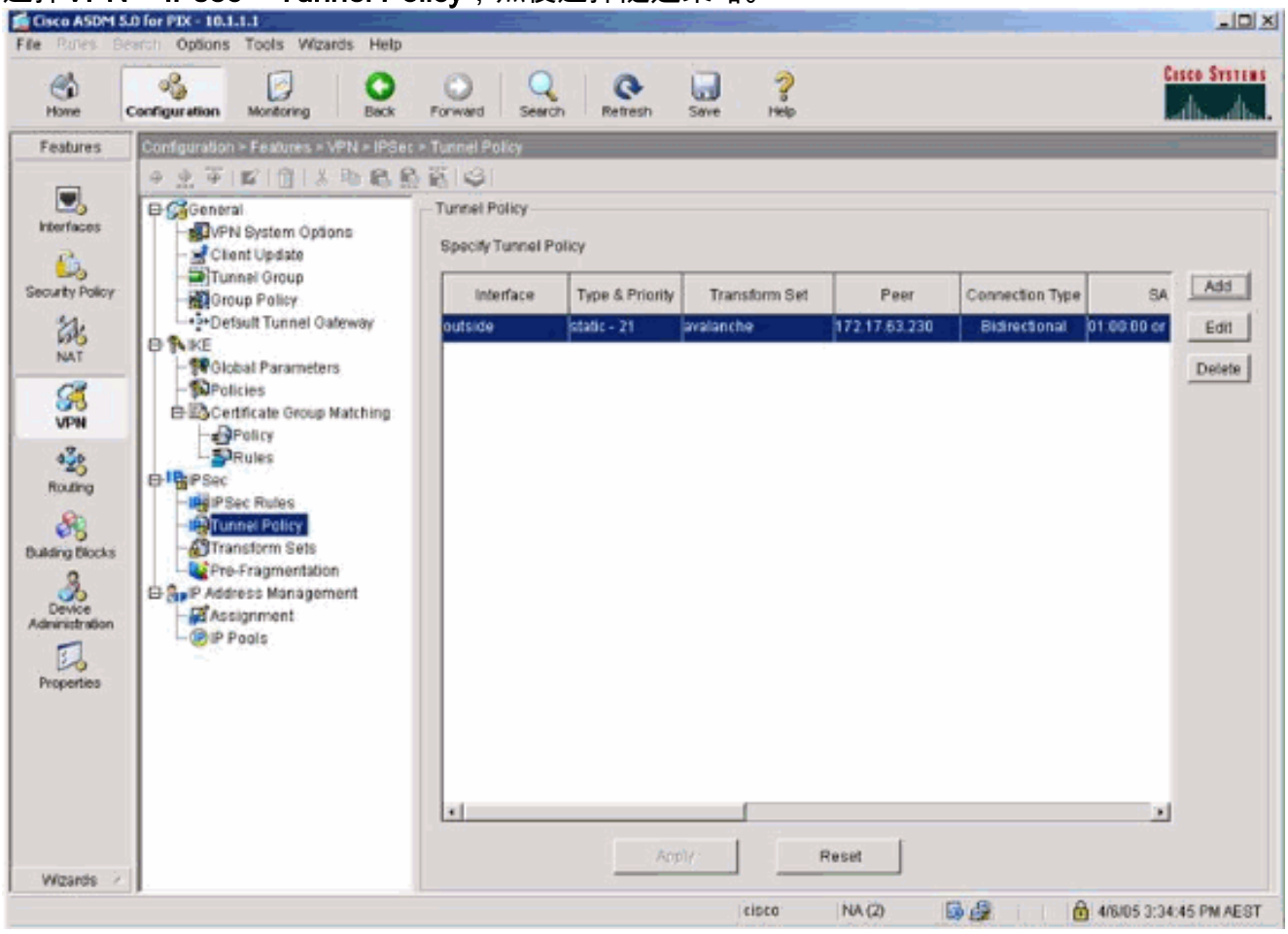
7. 選擇**VPN > IKE > Policies**，然後選擇IKE策略。



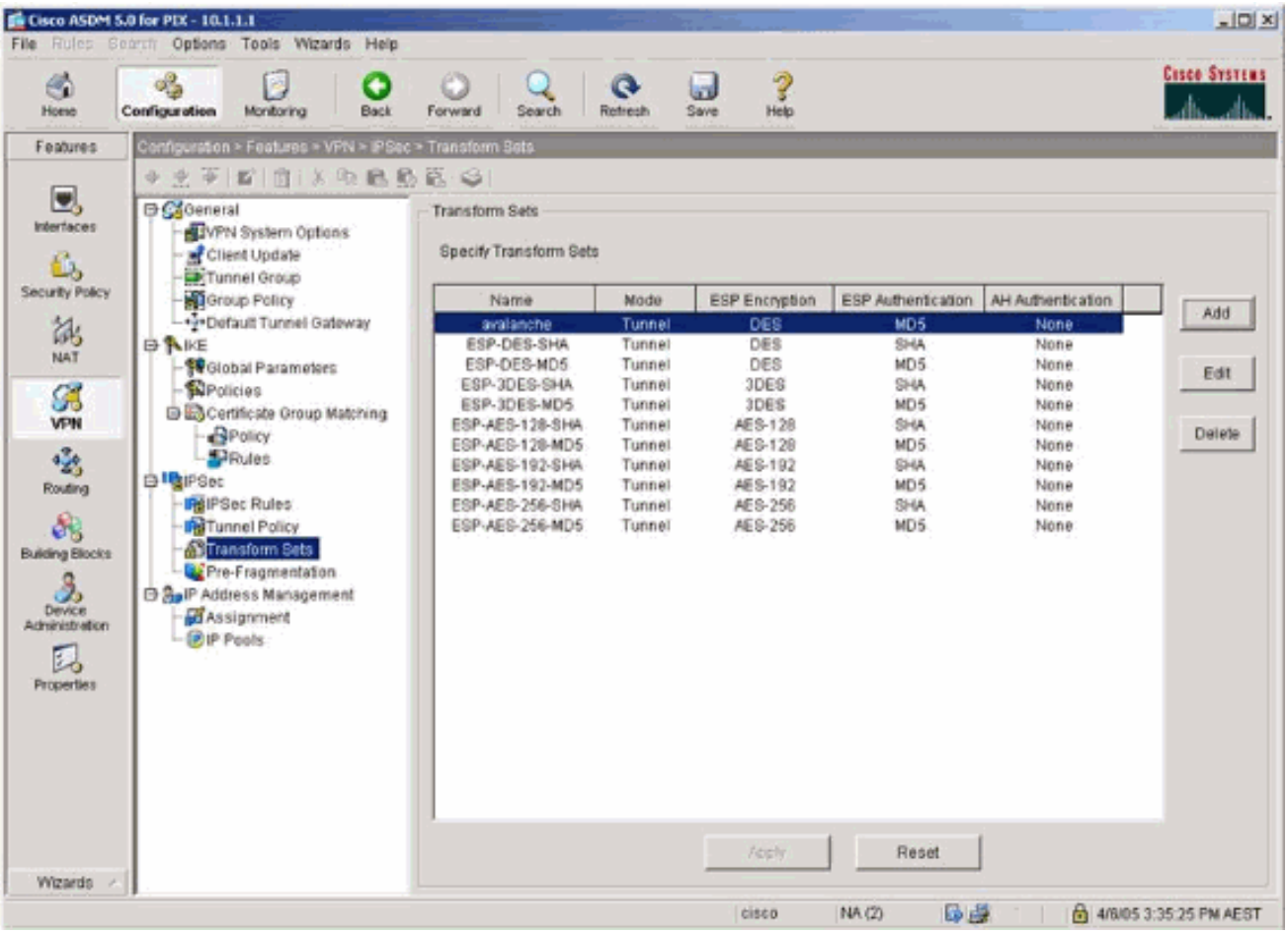
8. 選擇**VPN > IPsec > IPsec Rules**，然後選擇IPsec作為本地隧道和遠端編址。



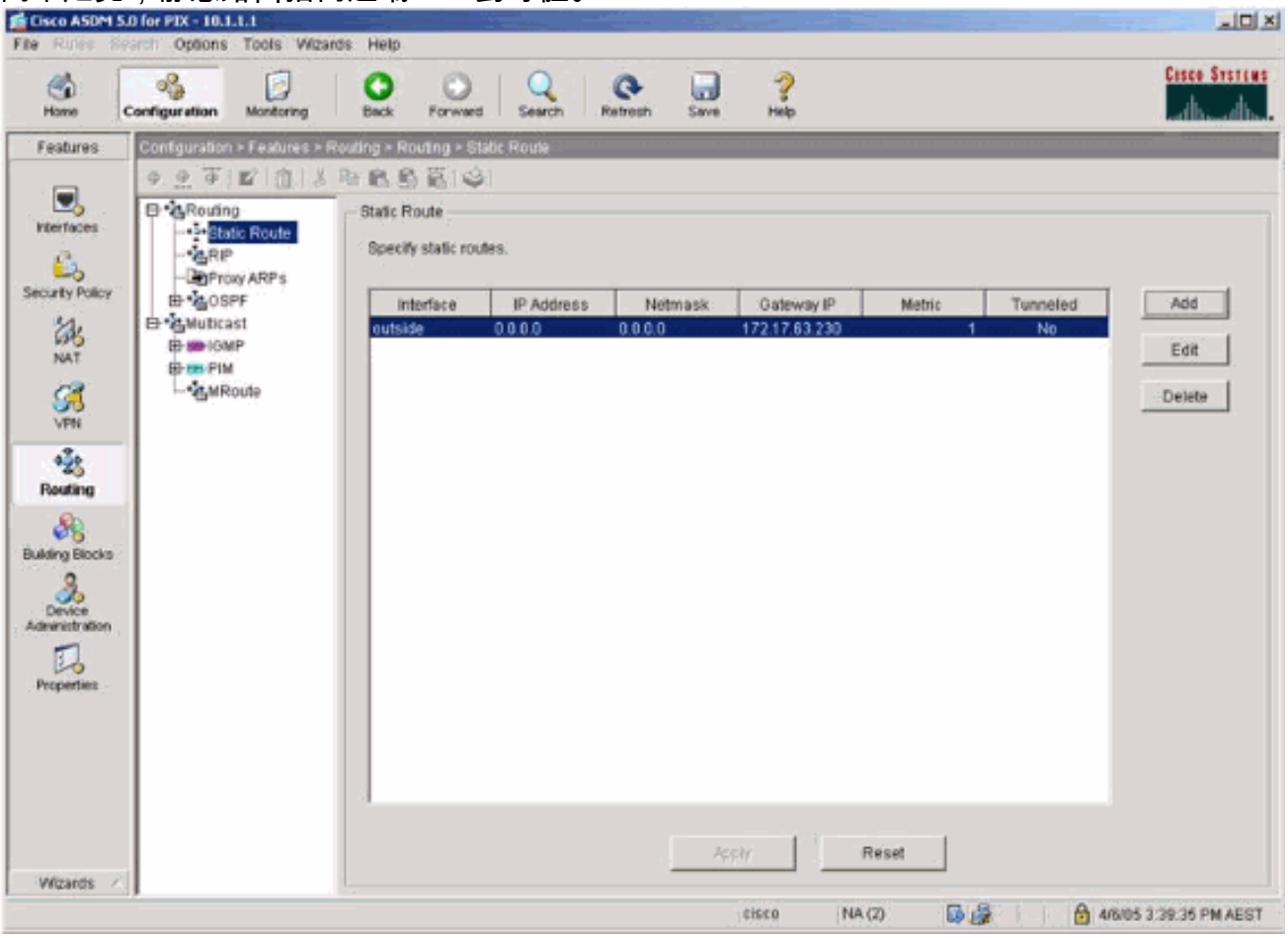
9. 選擇**VPN > IPsec > Tunnel Policy**，然後選擇隧道策略。



10. 選擇**VPN > IPsec > Transform Sets**，然後選擇Transform set。



11. 選擇**Routing > Routing > Static Route**，然後選擇到網關路由器的靜態路由。在本示例中，為簡單起見，靜態路由指向遠端VPN對等體。



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。

疑難排解

您可以使用ASDM啟用日誌記錄並檢視日誌。

- 選擇Configuration > Properties > Logging > Logging Setup，選擇Enable Logging，然後按一下Apply以啟用日誌記錄。
- 選擇Monitoring > Logging > Log Buffer > On Logging Level，選擇Logging Buffer，然後按一下View以檢視日誌。

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 crypto ipsec — 顯示第2階段的IPsec協商。
- debug crypto isakmp — 顯示第1階段的ISAKMP協商。
- debug crypto engine — 顯示加密的流量。
- clear crypto isakmp — 清除與第1階段相關的安全關聯。
- clear crypto sa — 清除與第2階段相關的安全關聯。
- debug icmp trace — 顯示來自主機的ICMP請求是否到達PIX。您需要新增access-list命令來允許組態中的ICMP，才能執行此偵錯。
- logging buffer debugging — 顯示正在建立並拒絕到通過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。

相關資訊

- 最常見的L2L和遠端訪問IPSec VPN故障排除解決方案
- 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)