ASA/PIX：到IOS路由器LAN到LAN IPSec隧道安全工具的配置示例

目录

简介

本文档说明如何配置一个从具有一个内部网络的 PIX 安全设备 7.x 及更高版本或自适应安全设备 (ASA) 到运行加密映像的 2611 路由器的 IPSec 隧道。为了简单起见，使用静态路由。

有关在路由器和 PIX 之间配置 LAN 到 LAN 隧道的详细信息，请参阅配置 Ipsec - 路由器到 PIX。

有关在 PIX 防火墙和 Cisco VPN 3000 集中器之间配置 LAN 到 LAN 隧道的详细信息，请参阅 Cisco VPN 3000 集中器和 PIX 防火墙之间的 LAN 到 LAN IPSec 隧道配置示例。

要了解有关在 PIX 和 VPN 集中器之间配置 LAN 到 LAN 隧道的方案的详细信息，请参阅 PIX 7.x 和 VPN 3000 集中器之间的 IPSec 隧道配置示例。

要了解有关 PIX 之间的 LAN 到 LAN 隧道同时允许 VPN Client 通过中央 PIX 访问分支 PIX 的方案的详细信息，请参阅使用 TACACS+ 身份验证增强的 PIX/ASA 7.x 分支到客户端 VPN 配置示例。

要了解有关 PIX/ASA 安全设备运行软件版本 8.x 的同一方案的详细信息，请参阅 SDM：ASA/PIX 和 IOS 路由器之间的站点到站点 IPsec VPN 配置示例。

参考的配置专业人员：使用思科CP GUI，在ASA/PIX和IOS路由器配置示例之间的站点至站点IPSec VPN为了学习ASA相关配置显示使用ASDM GUI和路由器相关的配置的更加大致同样的方案显示。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 使用 PIX 软件版本 7.0 的 PIX-525
- 使用 Cisco IOS® 软件版本 12.2(15)T13 的 Cisco 2611 路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

在 PIX 上，**access-list** 和 **nat 0** 命令协同工作。当 10.1.1.0 网络上的用户访问 10.2.2.0 网络时，访问列表用于允许 10.1.1.0 网络数据流在没有网络地址转换 (NAT) 的情况下被加密。在路由器上，**route-map** 和 access-list 命令用于允许 10.2.2.0 网络数据流在没有 NAT 的情况下被加密。但是，当这些相同的用户访问别的地方时，它们的地址将通过端口地址转换 (PAT) 被转换为 172.17.63.230。

要使隧道中的流量*不*穿越 PAT，而使到达 Internet 的流量穿越 PAT，必须在 PIX 安全设备上使用以下配置命令：

```
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
```

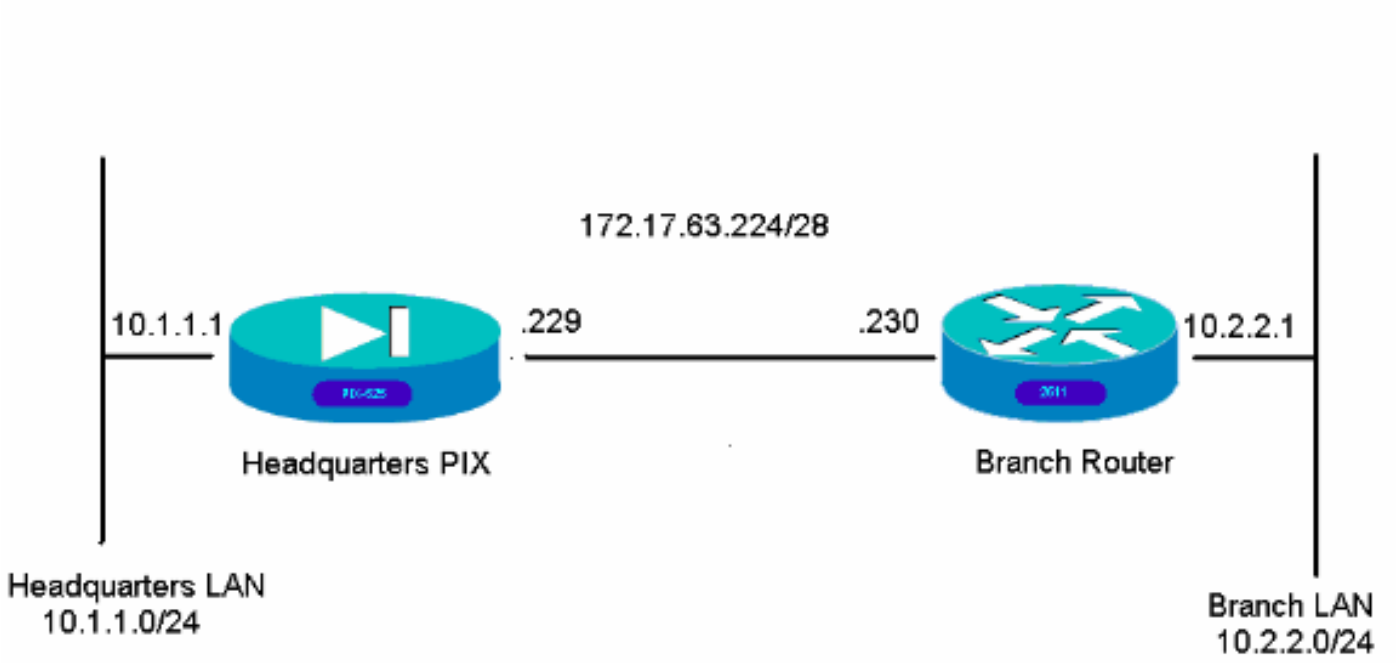
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



配置

以下配置示例是针对命令行界面的。如果您喜欢使用 ASDM 进行配置，请参阅本文档的使用自适应安全设备管理器 (ASDM) 进行配置部分。

- 总部 PIX
- 分支路由器

总部 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
```

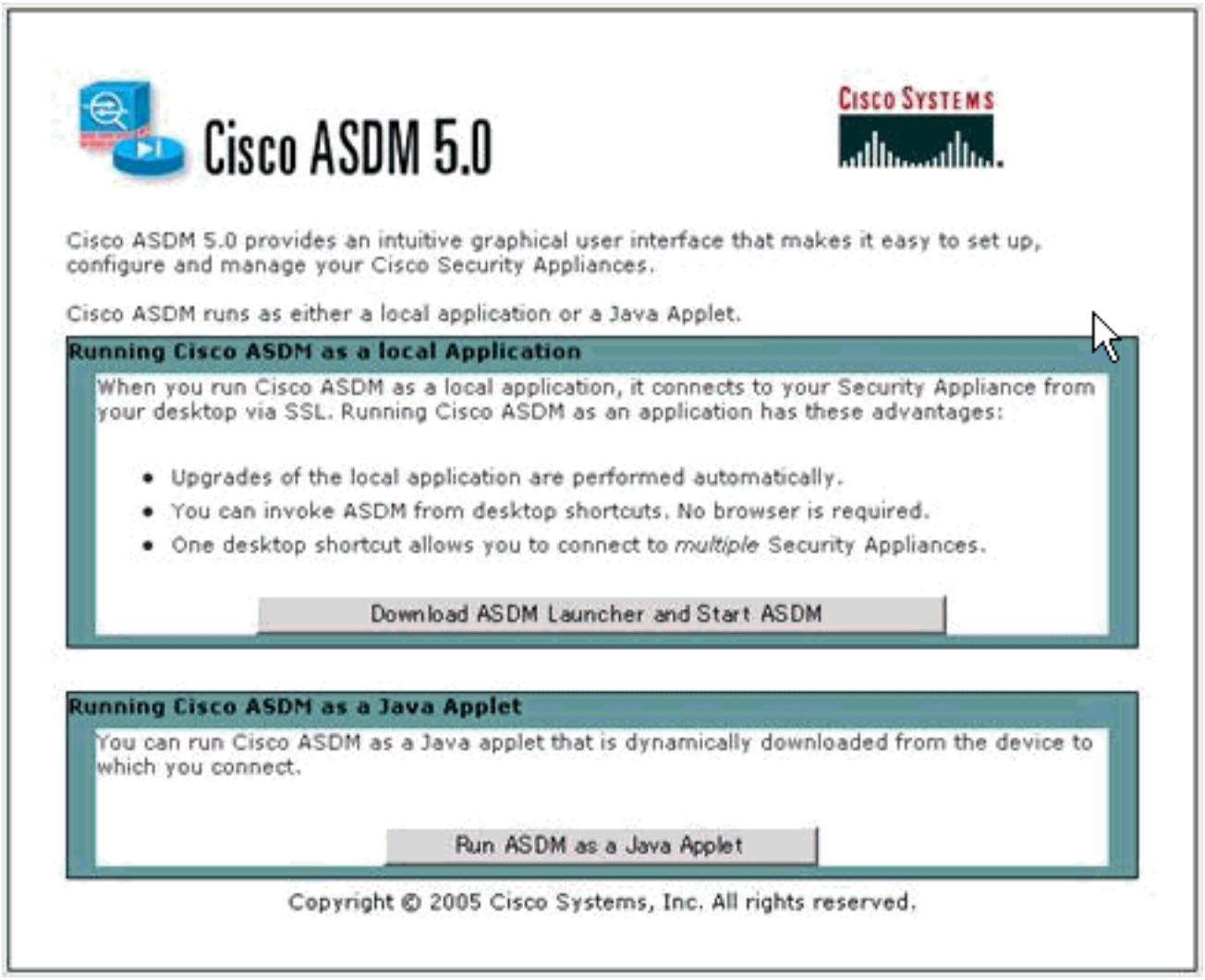
```
no ip http secure-server ip classless ip route 10.1.1.0
255.255.255.0 172.17.63.229 ! ! ! access-list 120 permit
ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255 access-list 130
deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255 access-
list 130 permit ip 10.2.2.0 0.0.0.255 any ! route-map
nonat permit 10 match 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 进行配置

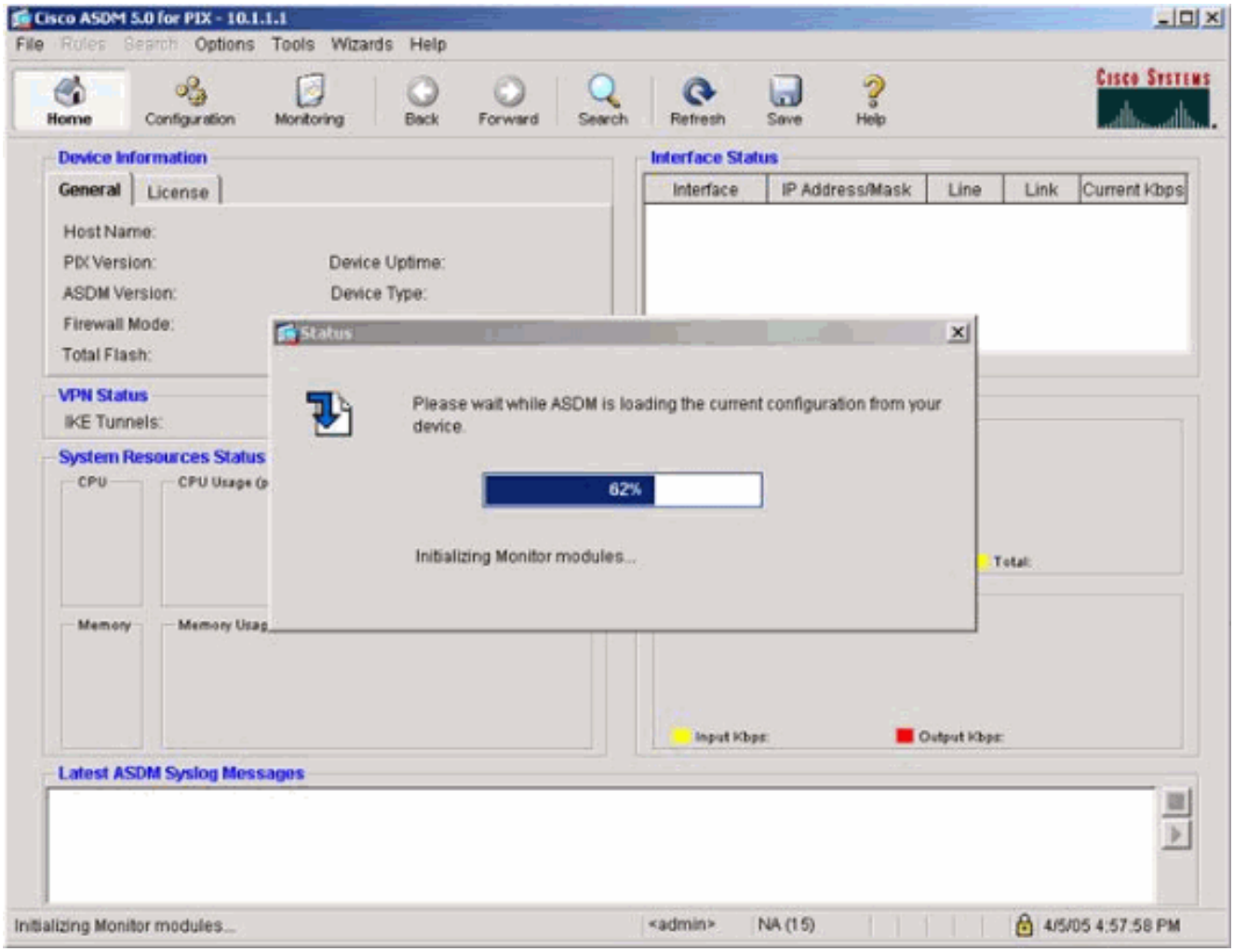
本示例说明如何使用 ASDM GUI 配置 PIX。带有浏览器且 IP 地址为 10.1.1.2 的 PC 被连接到 PIX 的内部接口 E1。请确保已在 PIX 上启用 http。

此过程说明总部 PIX 的 ASDM 配置。

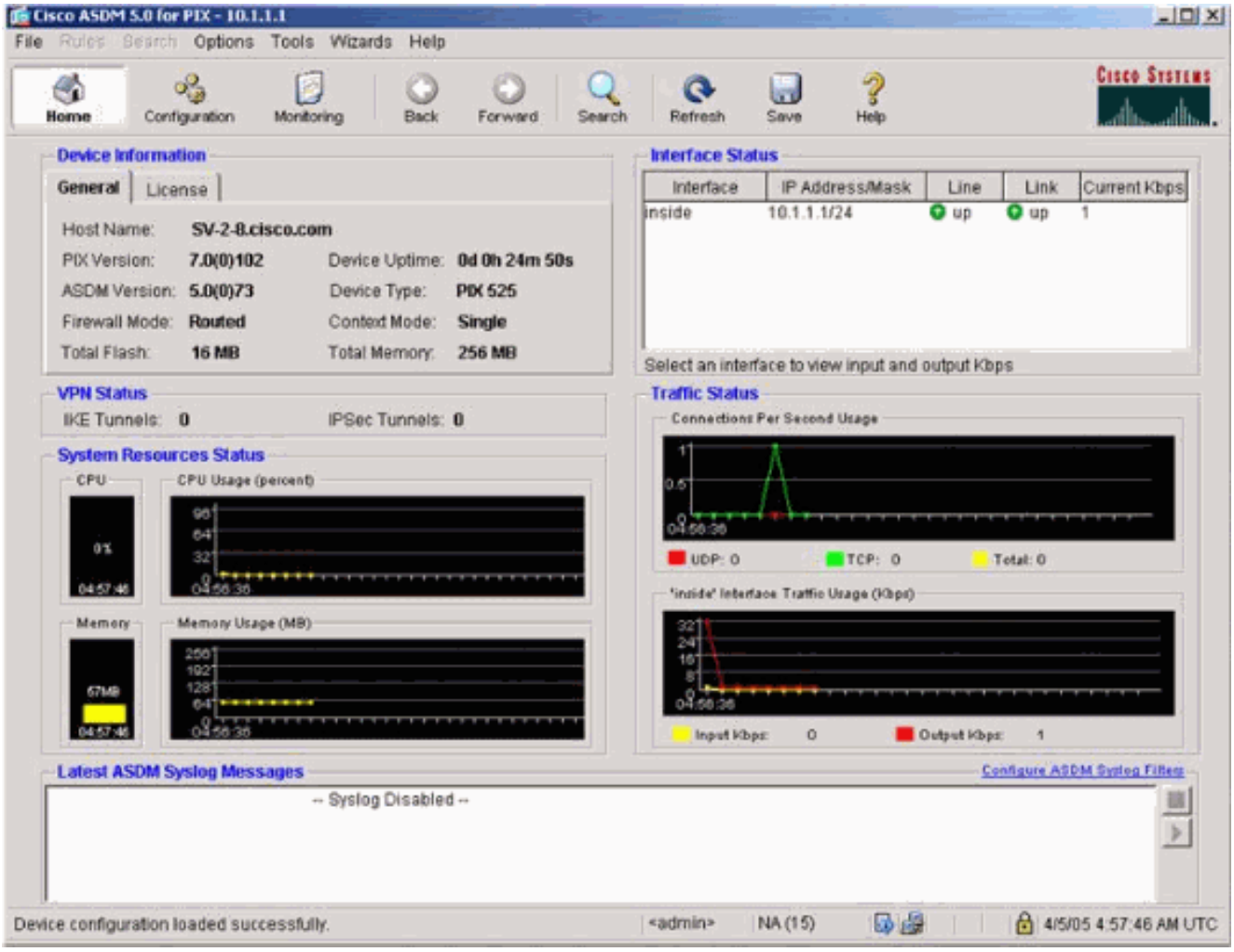
1. 将 PC 连接到 PIX 并选择一种下载方法。



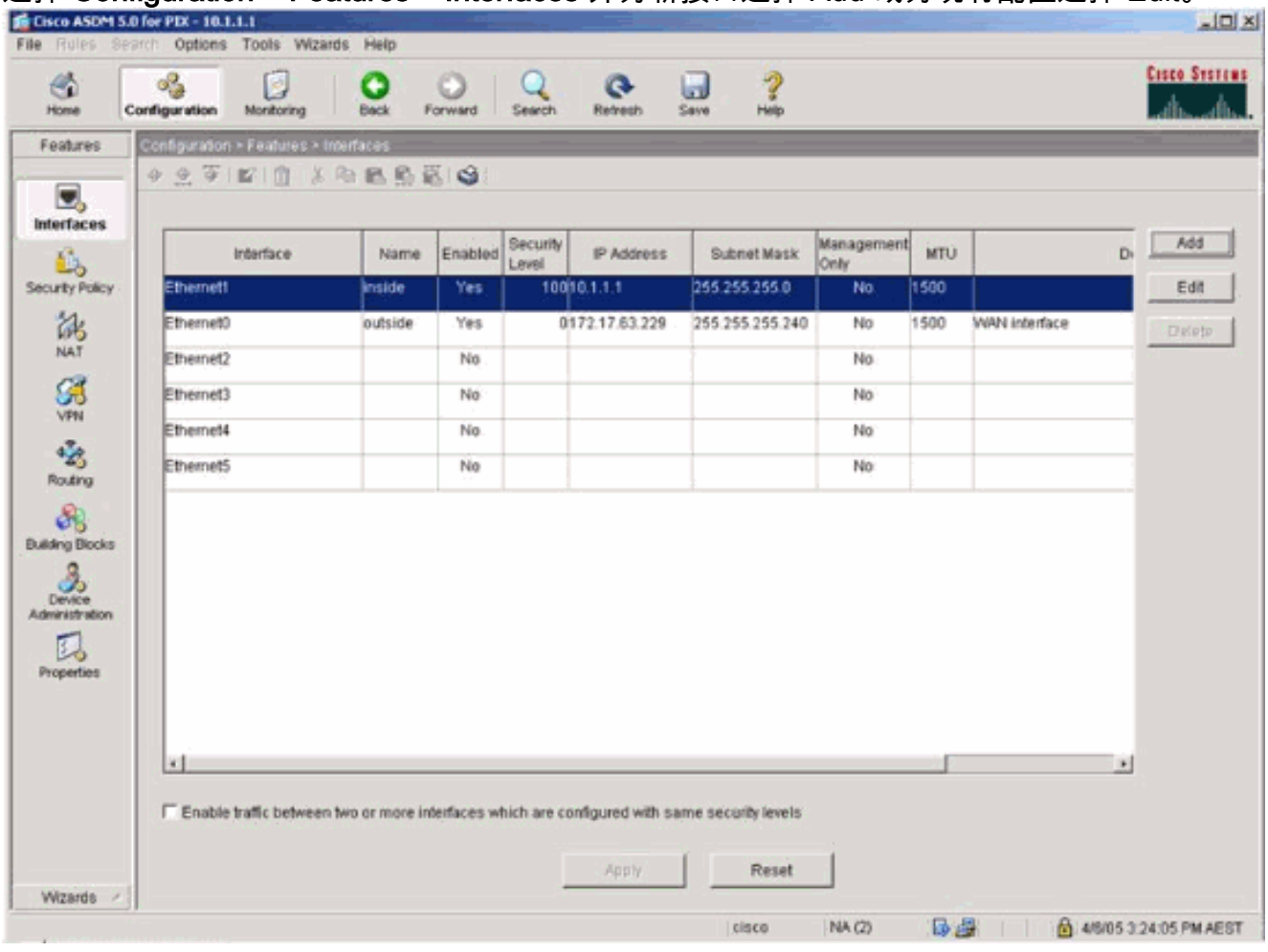
ASDM 从 PIX 中加载现有配置。



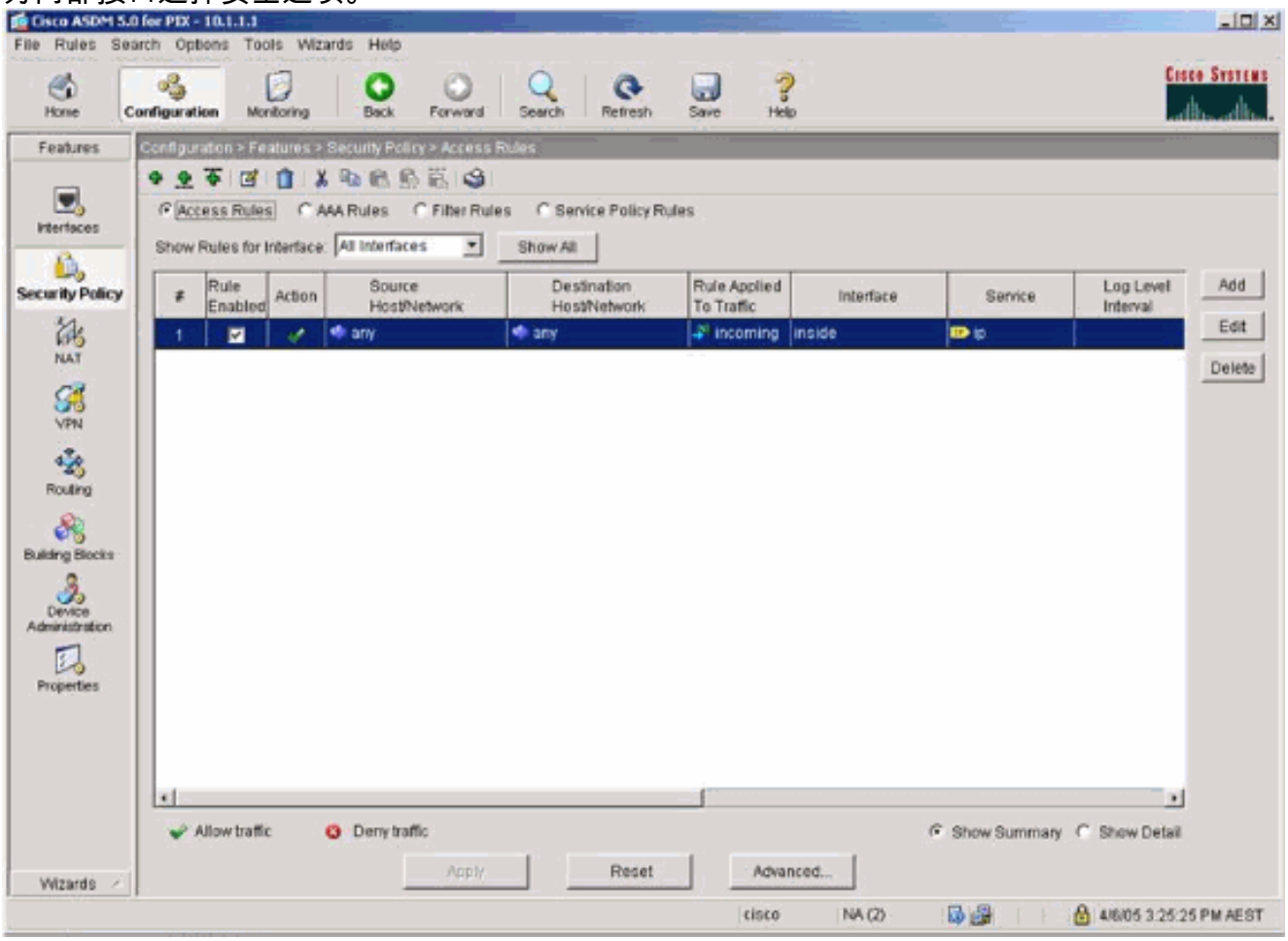
以下窗口提供监控仪表和菜单。



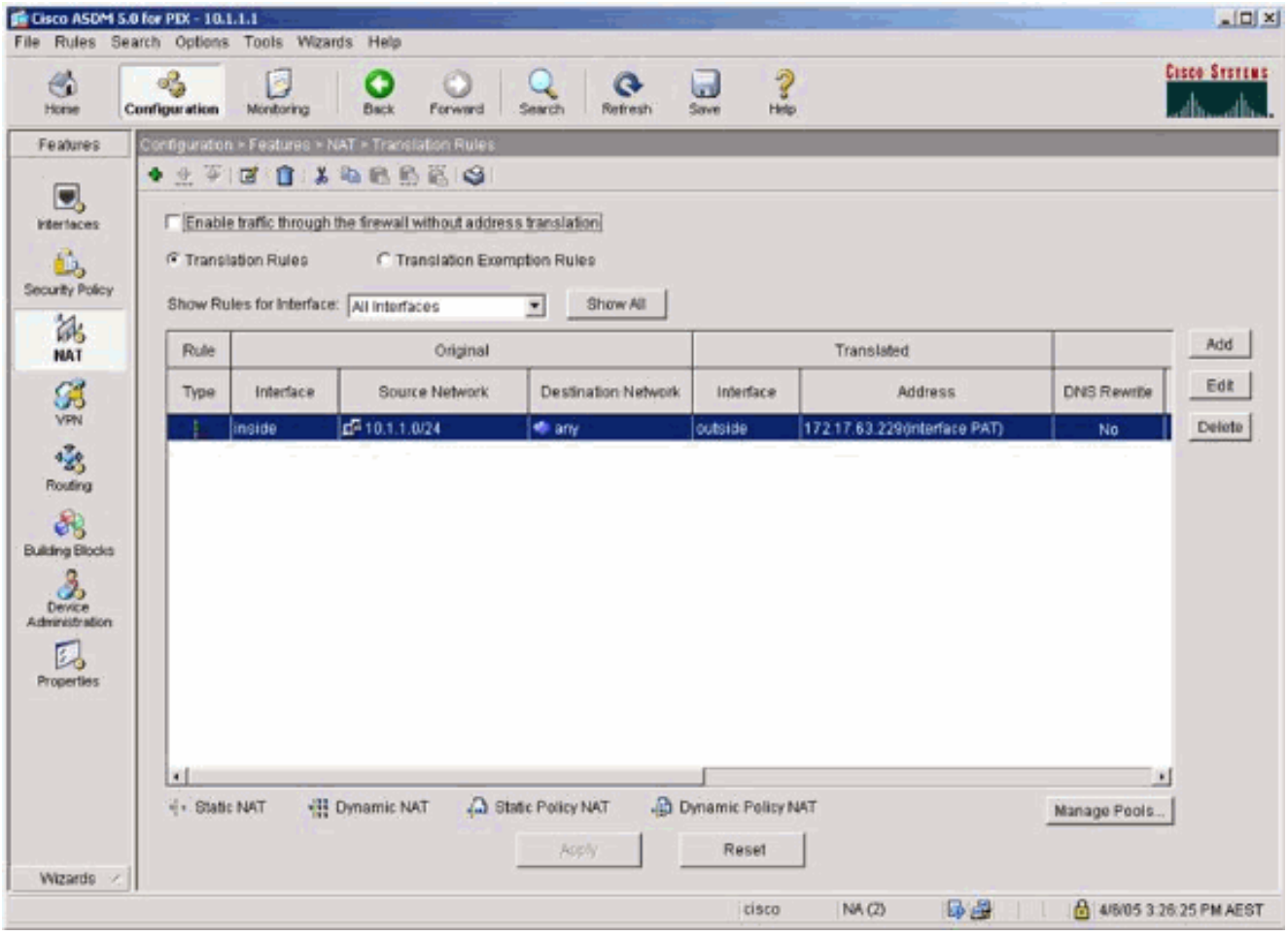
2. 选择 **Configuration > Features > Interfaces** 并为新接口选择 Add 或为现有配置选择 Edit。



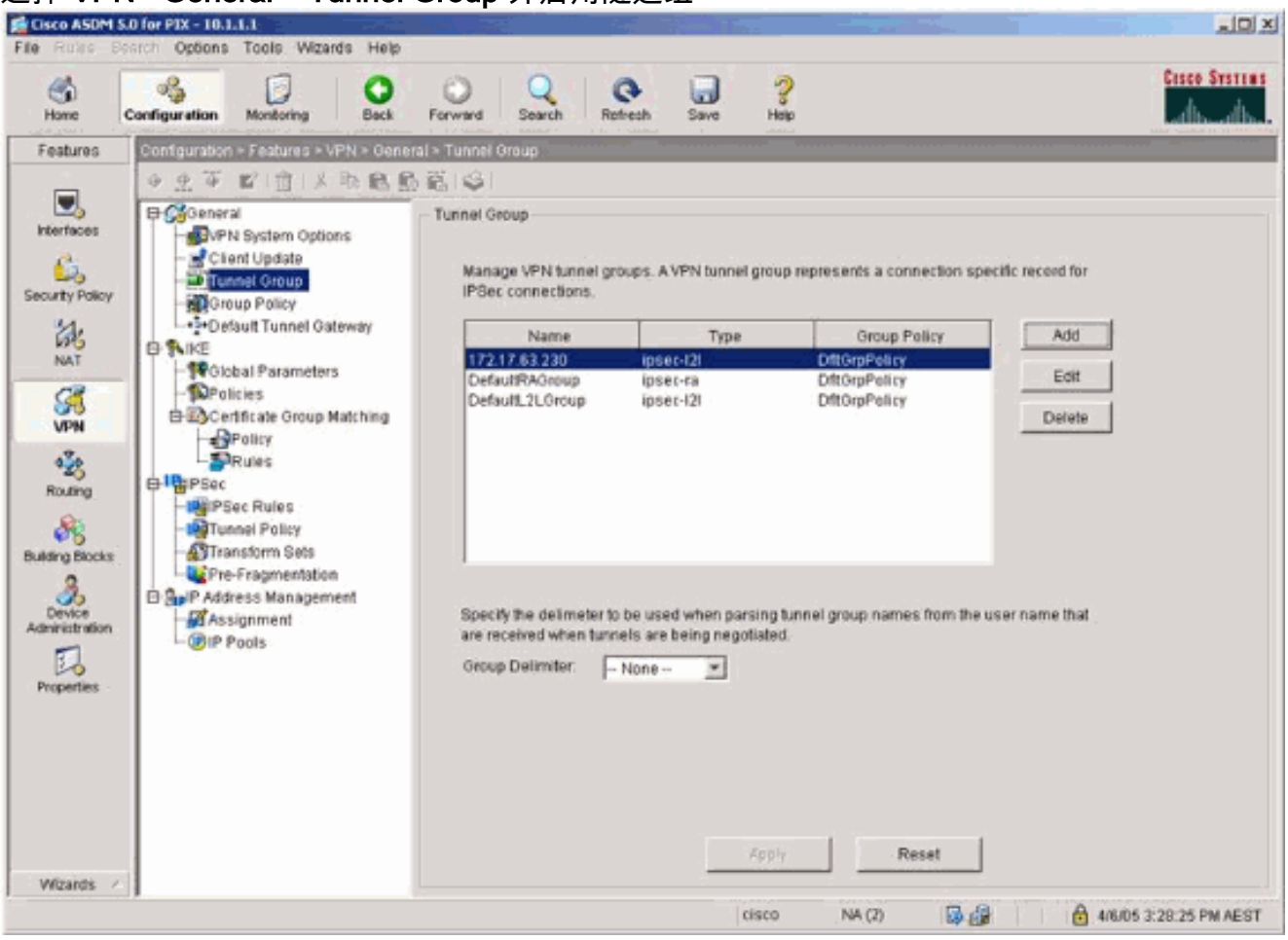
3. 为内部接口选择安全选项。



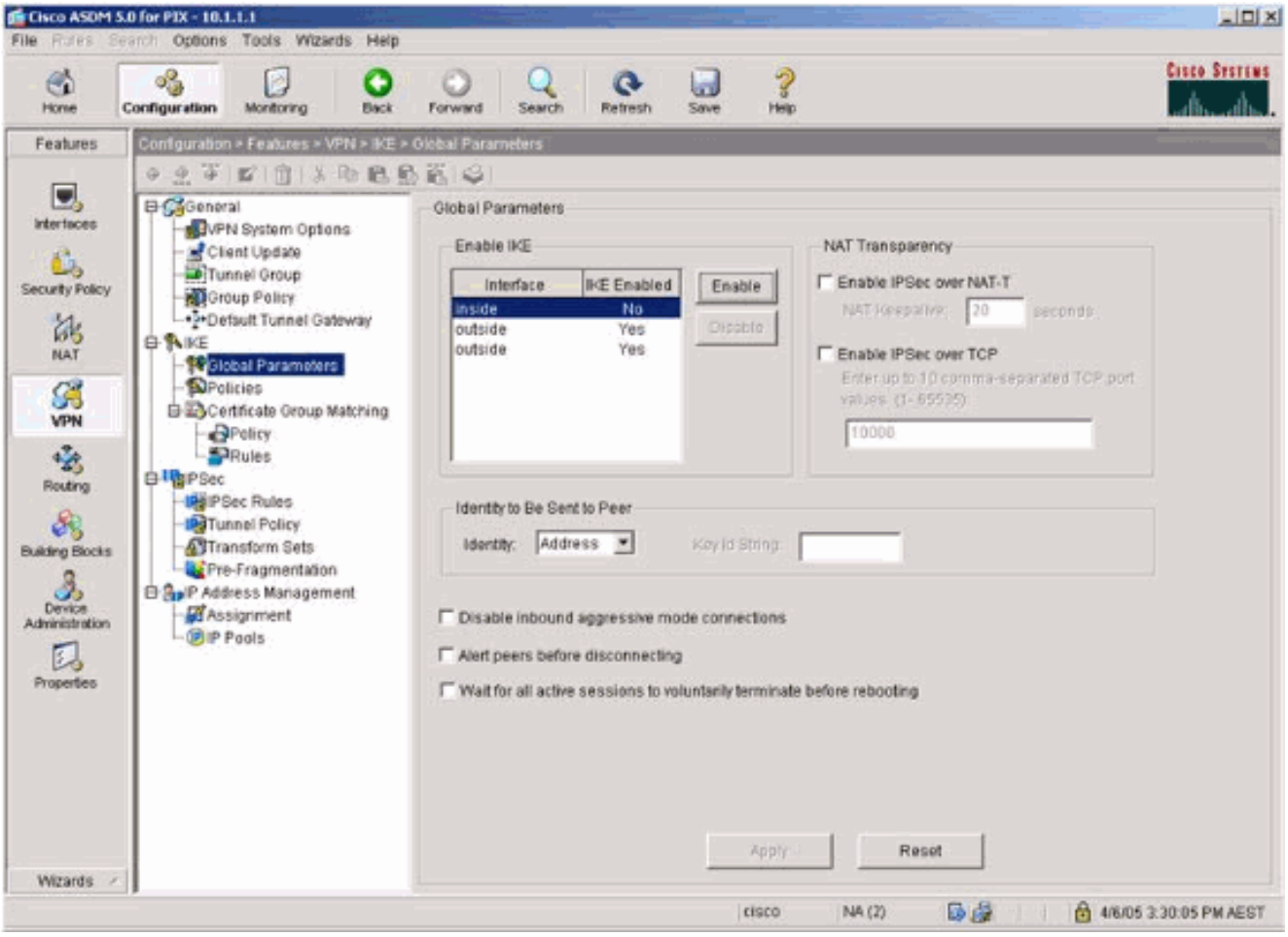
4. 在 NAT 配置中，加密数据流是免除 NAT 的，所有其他数据流都经过 NAT/PAT 流向外部接口。



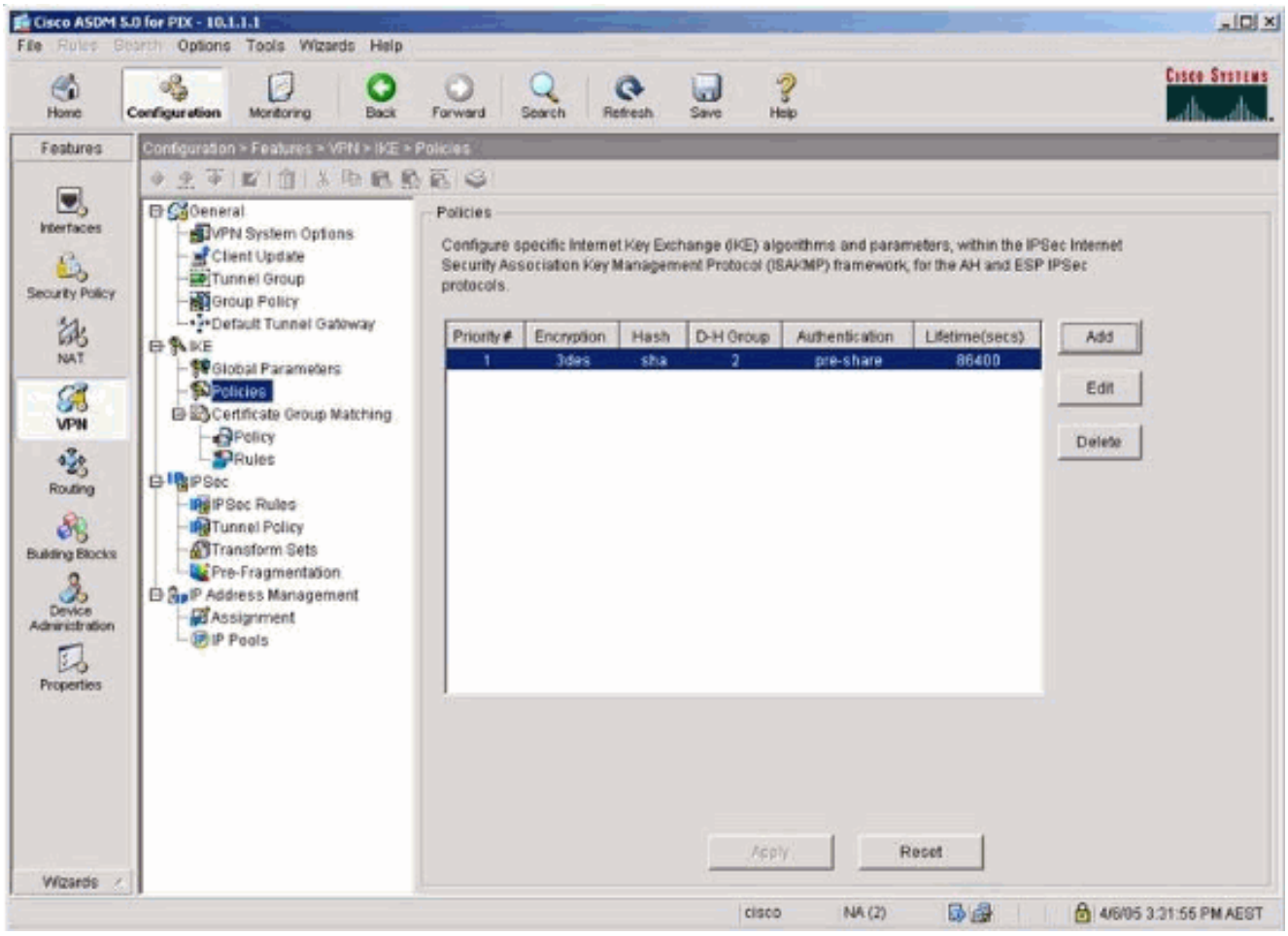
5. 选择 VPN >General > Tunnel Group 并启用隧道组



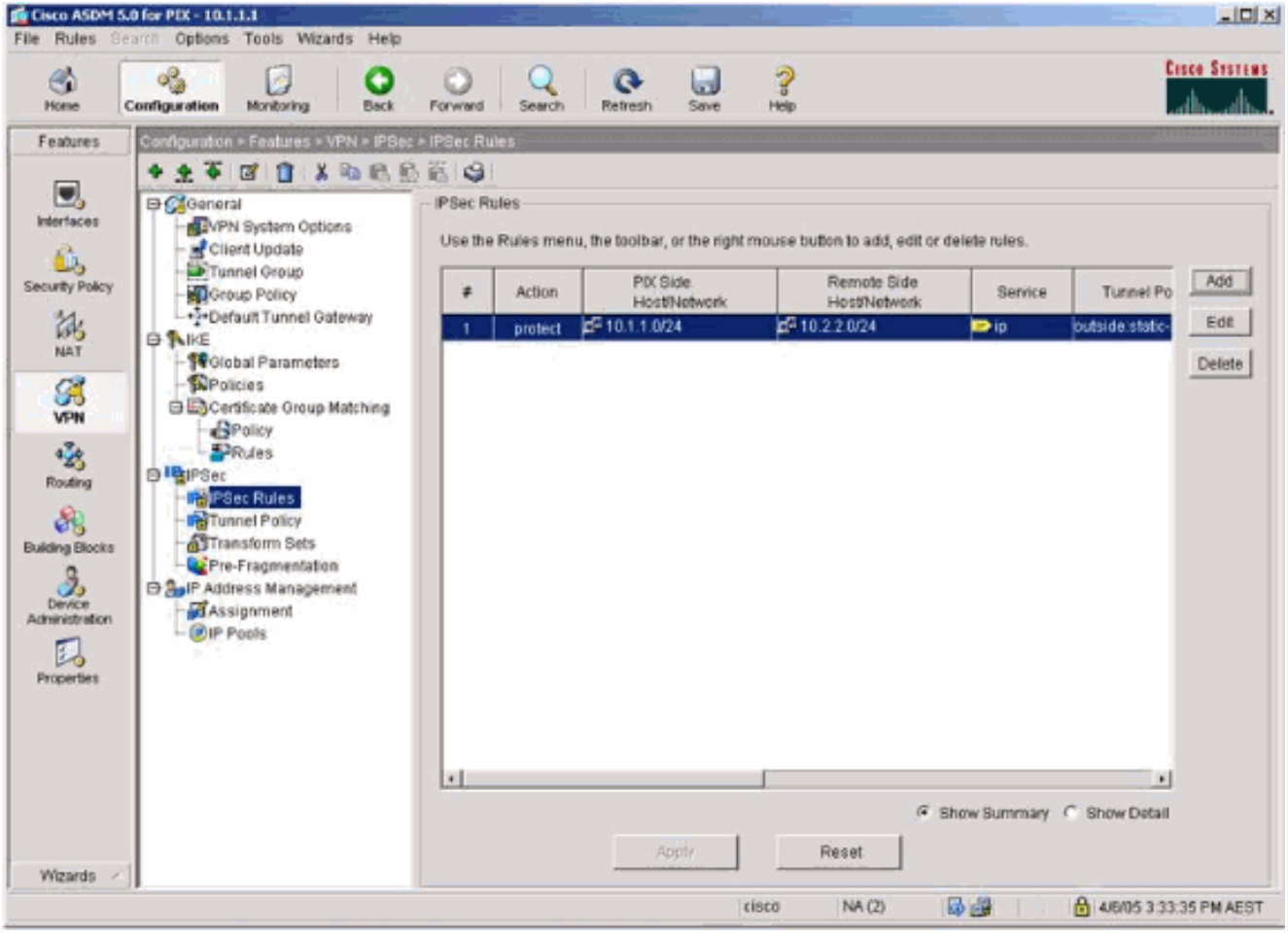
6. 选择 VPN > IKE > Global Parameters 并在外部接口上启用 IKE。



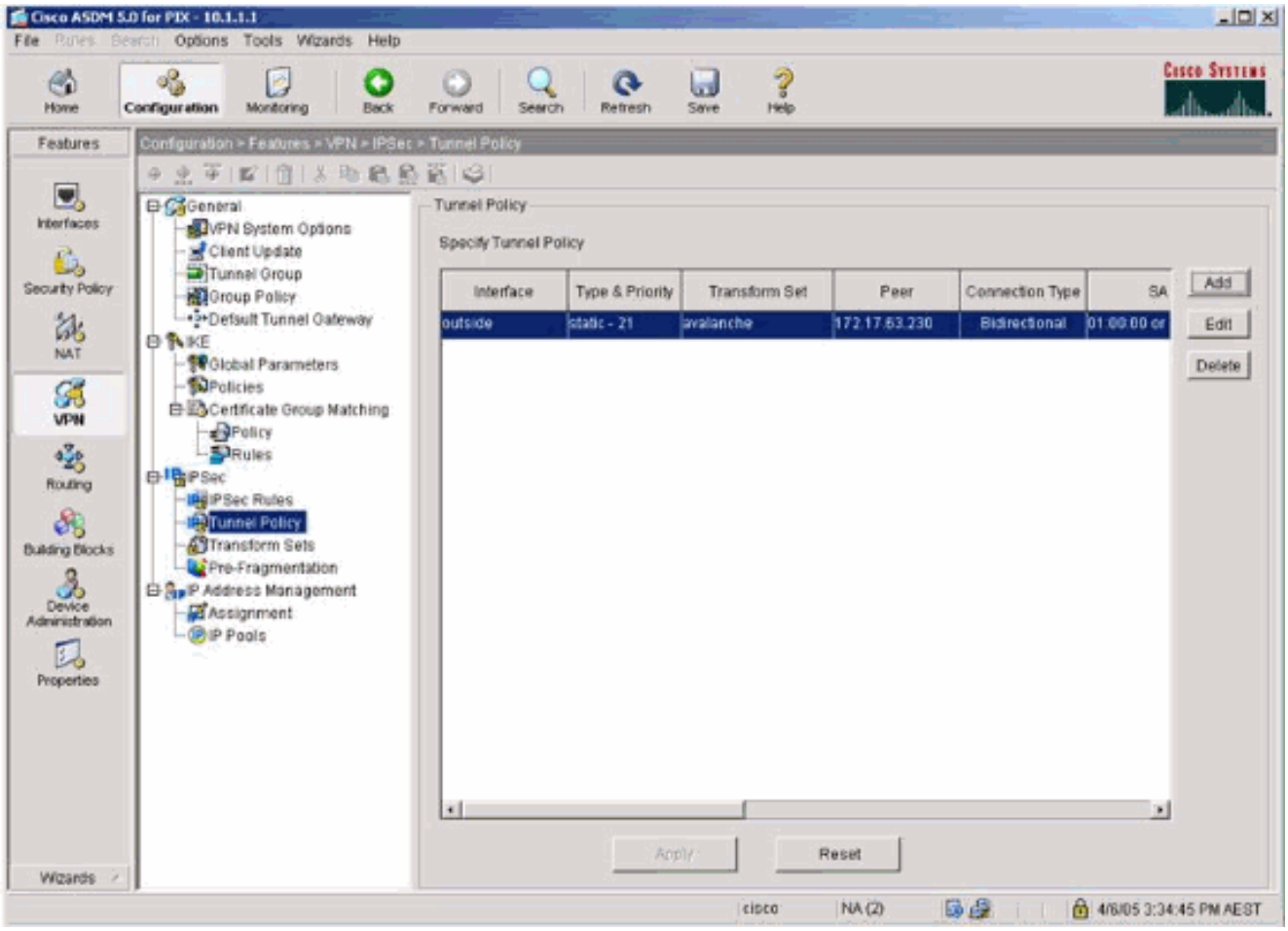
7. 选择 VPN > IKE > Policies 并选择 IKE 策略。



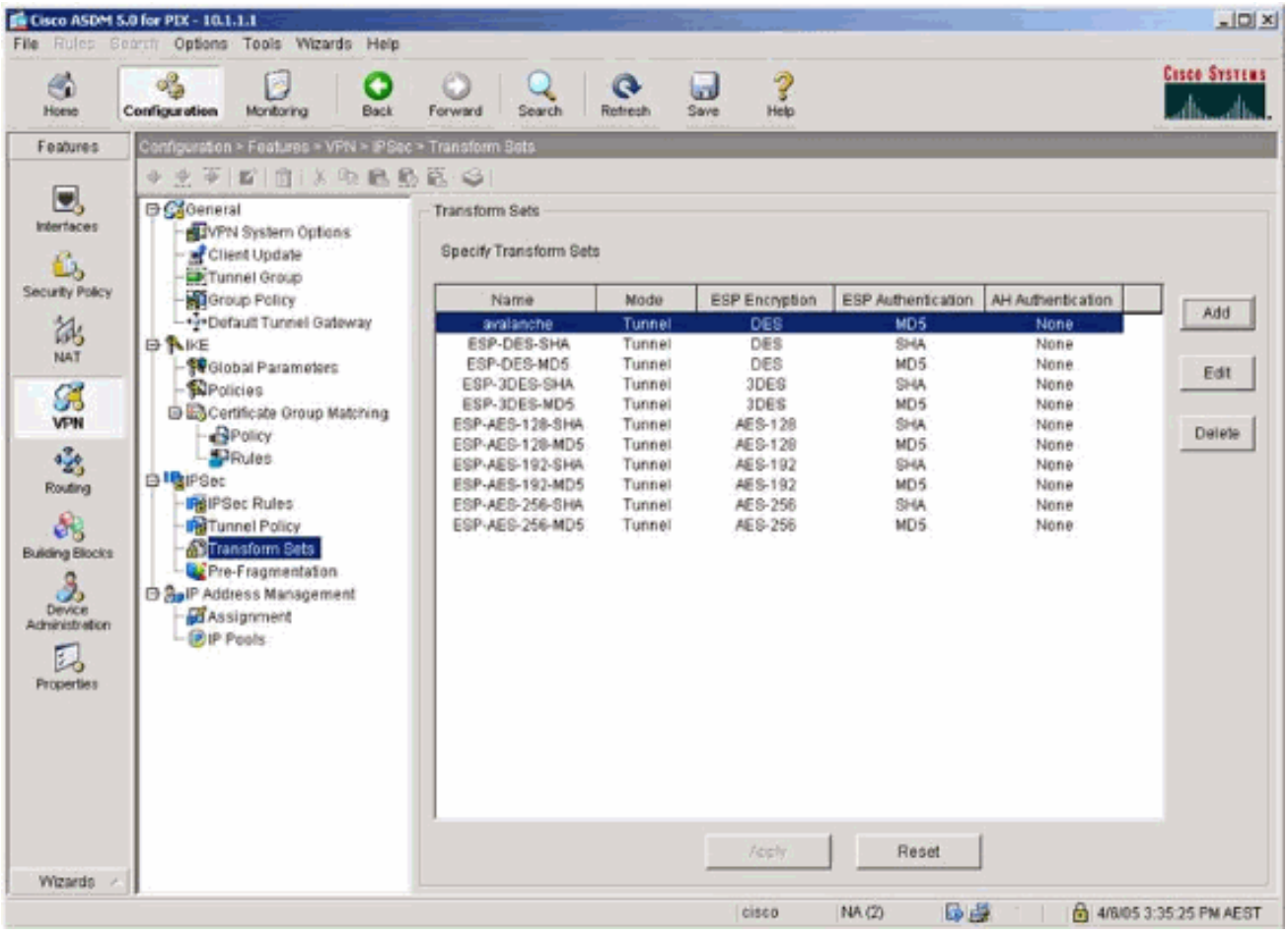
8. 选择 VPN > IPsec > IPsec Rules 并为本地隧道和远程编址选择 IPsec。



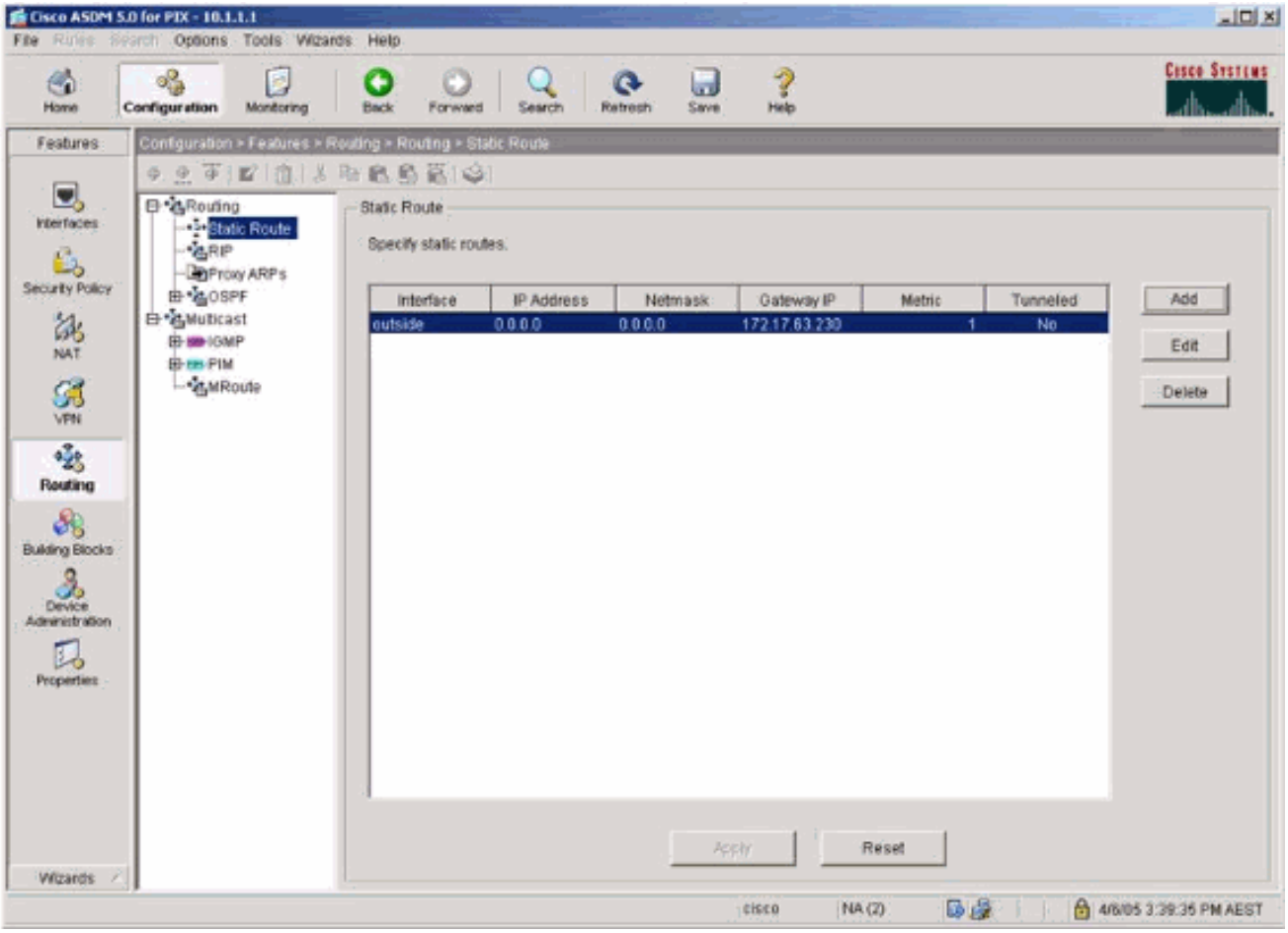
9. 选择 VPN > IPsec > Tunnel Policy 并选择隧道策略。



10. 选择 **VPN > IPsec > Transform Sets** 并选择转换集。



11. 选择 **Routing > Routing > Static Route** 并选择到网关路由器的静态路由。在本示例中，为了简单起见，静态路由指向远程 VPN 对等体。



验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show crypto ipsec sa** — 显示第 2 阶段安全连接。
- **show crypto isakmp sa** - 显示第 1 阶段的安全关联。

故障排除

您可以使用 ASDM 启用日志记录和查看日志。

- 选择 **Configuration > Properties > Logging > Logging Setup**，选择 Enable Logging，并单击 Apply 以启用日志记录。
- 选择 **Monitoring > Logging > Log Buffer > On Logging Level**，选择 Logging Buffer，并单击 View 以查看日志。

故障排除命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **debug crypto ipsec** - 显示第 2 阶段的 IPsec 协商。
- **debug crypto isakmp** - 显示第 1 阶段的 ISAKMP 协商。
- **debug crypto engine** - 显示已加密的数据流。
- **clear crypto isakmp** - 清除与第 1 阶段相关的安全关联。
- **clear crypto sa** - 清除与第 2 阶段相关的安全关联。
- **debug icmp trace** - 显示来自主机的 ICMP 请求是否到达 PIX。需要添加 **access-list** 命令，在您的配置中允许 ICMP，以便运行此 debug 命令。
- **logging buffer debugging** - 显示正在建立和已拒绝的连接，这些连接通过 PIX 指向主机。信息存储在 PIX 日志缓冲区中，使用 **show log** 命令可查看输出。

相关信息

- **最常用的 L2L 和远程访问 IPSec VPN 故障排除解决方案**
- Cisco PIX 防火墙软件
- Cisco Secure PIX 防火墙命令参考
- 安全产品 Field Notices（包括 PIX）
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems