

ASA/PIX : Security Appliance to an IOS Router LAN-to-LAN IPsec Tunnel Configuration Example

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Configuration using ASDM](#)

[Verify](#)

[Troubleshoot](#)

[Troubleshooting Commands](#)

[Related Information](#)

[Introduction](#)

This document demonstrates how to configure an IPsec tunnel from PIX Security Appliance 7.x and later or the Adaptive Security Appliance (ASA) with one internal network to a 2611 router that runs a crypto image. Static routes are used for simplicity.

Refer to [Configuring IPsec - Router to PIX](#) for more information about a LAN-to-LAN tunnel configuration between a router and the PIX.

Refer to [LAN-to-LAN IPsec Tunnel Between the Cisco VPN 3000 Concentrator and PIX Firewall Configuration Example](#) for more information about a LAN-to-LAN tunnel configuration between the PIX Firewall and Cisco VPN 3000 Concentrator.

Refer to [IPsec Tunnel Between PIX 7.x and VPN 3000 Concentrator Configuration Example](#) in order to learn more about the scenario where the LAN-to-LAN tunnel is between the PIX and VPN Concentrator.

Refer to [PIX/ASA 7.x Enhanced Spoke-to-Client VPN with TACACS+ Authentication Configuration Example](#) in order to learn more about the scenario where the LAN-to-LAN tunnel between the PIXes also allows for a VPN Client to access the spoke PIX through the hub PIX.

Refer to [SDM: Site-to-Site IPsec VPN Between ASA/PIX and an IOS Router Configuration](#)

[Example](#) in order to learn more about the same scenario where the PIX/ASA Security Appliance runs software version 8.x.

Refer to [Configuration Professional: Site-to-Site IPsec VPN Between ASA/PIX and an IOS Router Configuration Example](#) in order to learn more about the same scenario where the ASA-related configuration is shown using ASDM GUI and the Router-related configuration is shown using Cisco CP GUI.

[Prerequisites](#)

[Requirements](#)

There are no specific requirements for this document.

[Components Used](#)

The information in this document is based on these software and hardware versions:

- PIX-525 with PIX Software version 7.0
- Cisco 2611 router with Cisco IOS® Software Release 12.2(15)T13

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

[Conventions](#)

Refer to the [Cisco Technical Tips Conventions](#) for more information on document conventions.

[Background Information](#)

On the PIX, the **access-list** and **nat 0** commands work together. When a user on the 10.1.1.0 network goes to the 10.2.2.0 network, the access list is used to permit the 10.1.1.0 network traffic to be encrypted without Network Address Translation (NAT). On the router, the **route-map** and **access-list** commands are used to permit the 10.2.2.0 network traffic to be encrypted without NAT. However, when those same users go anywhere else, they are translated to the 172.17.63.230 address through Port Address Translation (PAT).

These are the configuration commands required on the PIX Security Appliance in order for traffic *not* to run through PAT over the tunnel, and traffic to the Internet to run through 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
```

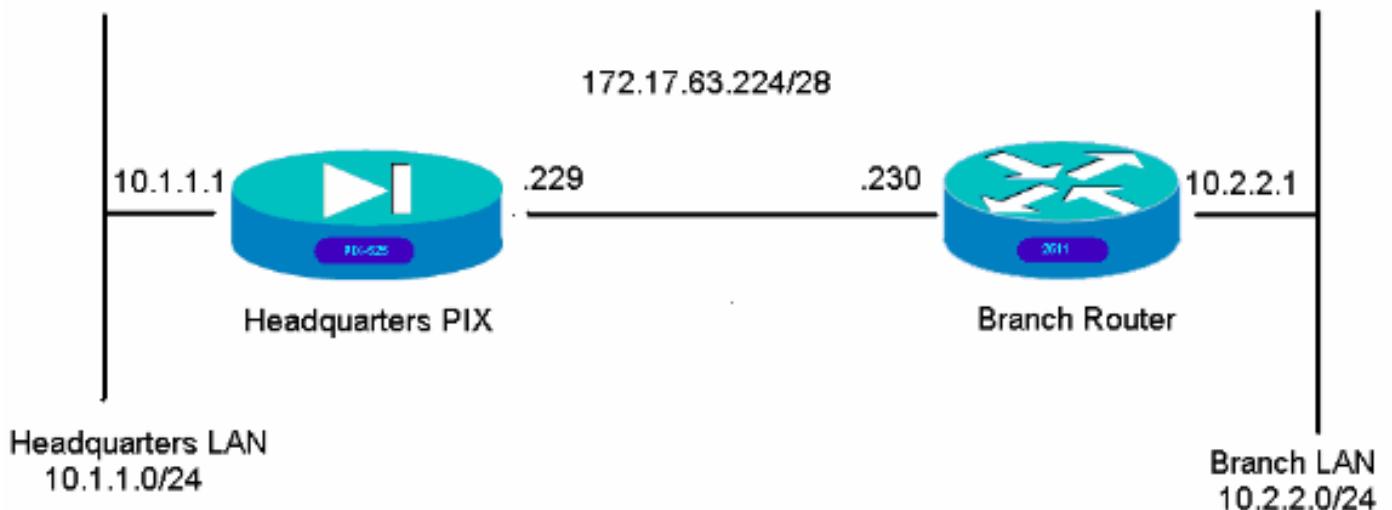
[Configure](#)

In this section, you are presented with the information to configure the features described in this document.

Note: Use the [Command Lookup Tool](#) ([registered](#) customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Configurations

These configuration examples are for the command line interface. See the [Configuration using Adaptive Security Device Manager \(ASDM\)](#) section of this document if you prefer to configure using ASDM.

- [Headquarters PIX](#)
- [Branch Router](#)

Headquarters 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 Isec-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
Isec-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#

```

Branch Router

```

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
```

[Configuration using ASDM](#)

This example demonstrates how to configure the PIX using the ASDM GUI. A PC with a browser and IP address 10.1.1.2 is connected to the inside interface e1 of the PIX. Ensure http is enabled on the PIX.

This procedure illustrates the ASDM configuration of the Headquarters PIX.

1. Connect the PC to the PIX and choose a download method.



Cisco ASDM 5.0



Cisco ASDM 5.0 provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco Security Appliances.

Cisco ASDM runs as either a local application or a Java Applet.

Running Cisco ASDM as a local Application

When you run Cisco ASDM as a local application, it connects to your Security Appliance from your desktop via SSL. Running Cisco ASDM as an application has these advantages:

- Upgrades of the local application are performed automatically.
- You can invoke ASDM from desktop shortcuts. No browser is required.
- One desktop shortcut allows you to connect to *multiple* Security Appliances.

[Download ASDM Launcher and Start ASDM](#)

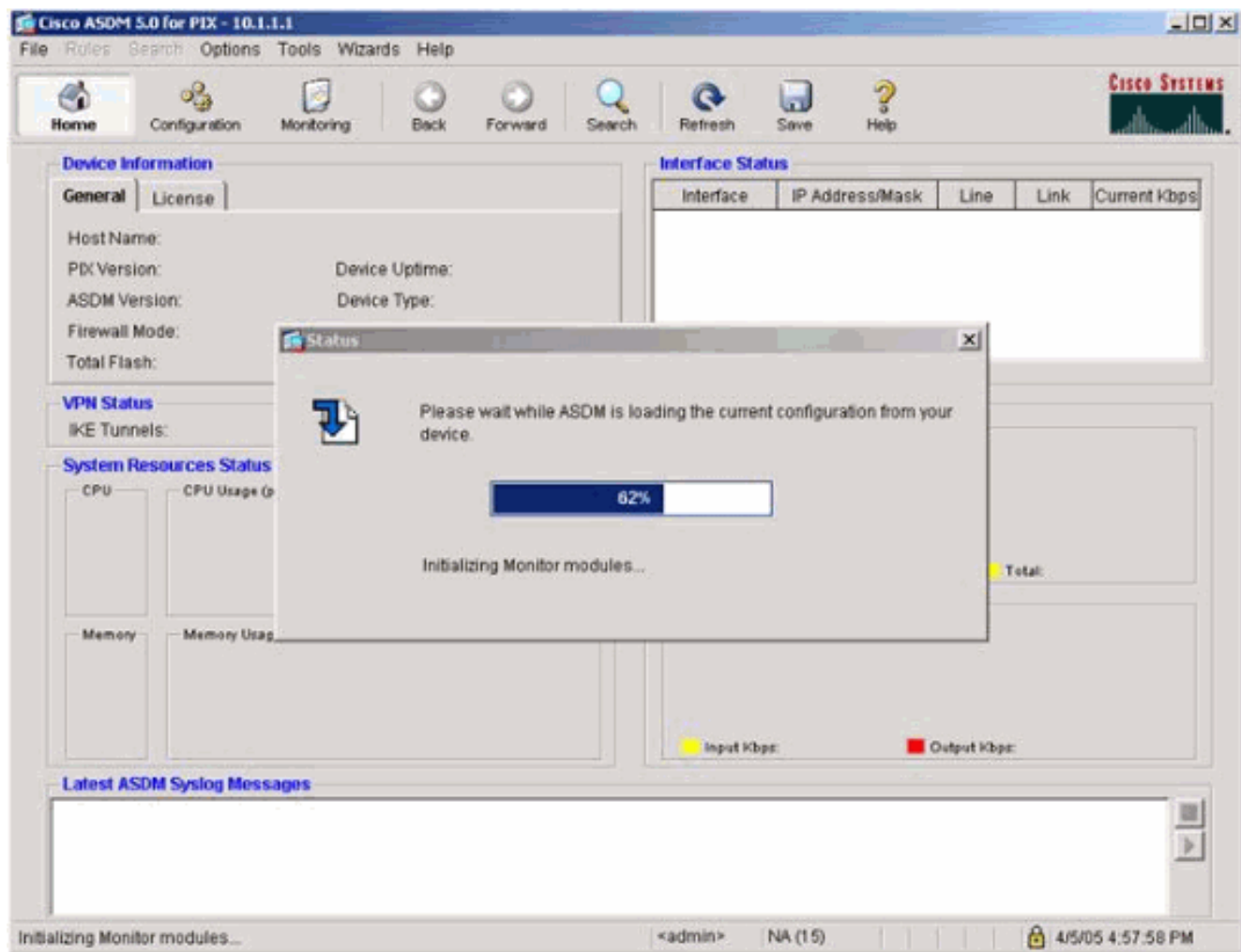
Running Cisco ASDM as a Java Applet

You can run Cisco ASDM as a Java applet that is dynamically downloaded from the device to which you connect.

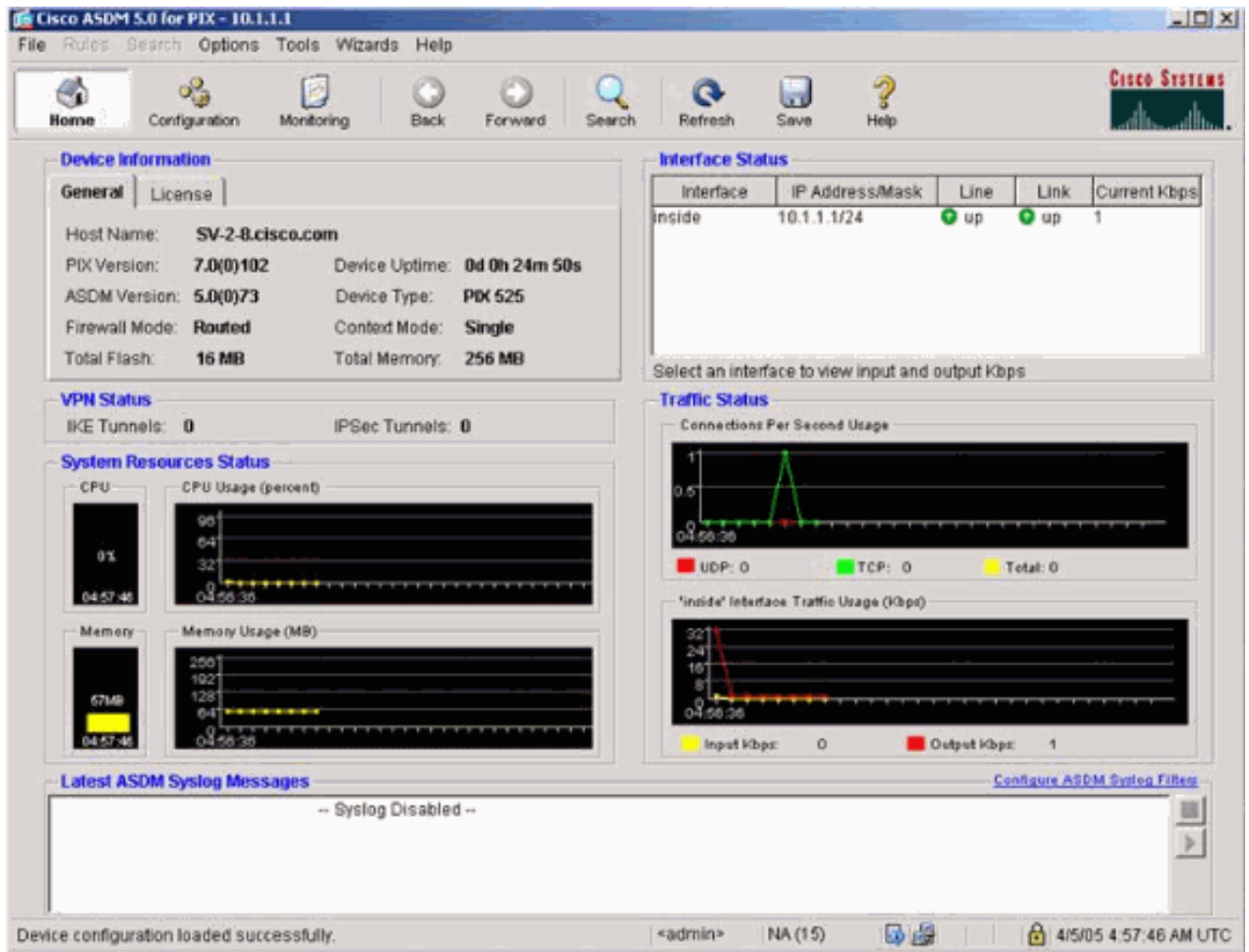
[Run ASDM as a Java Applet](#)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

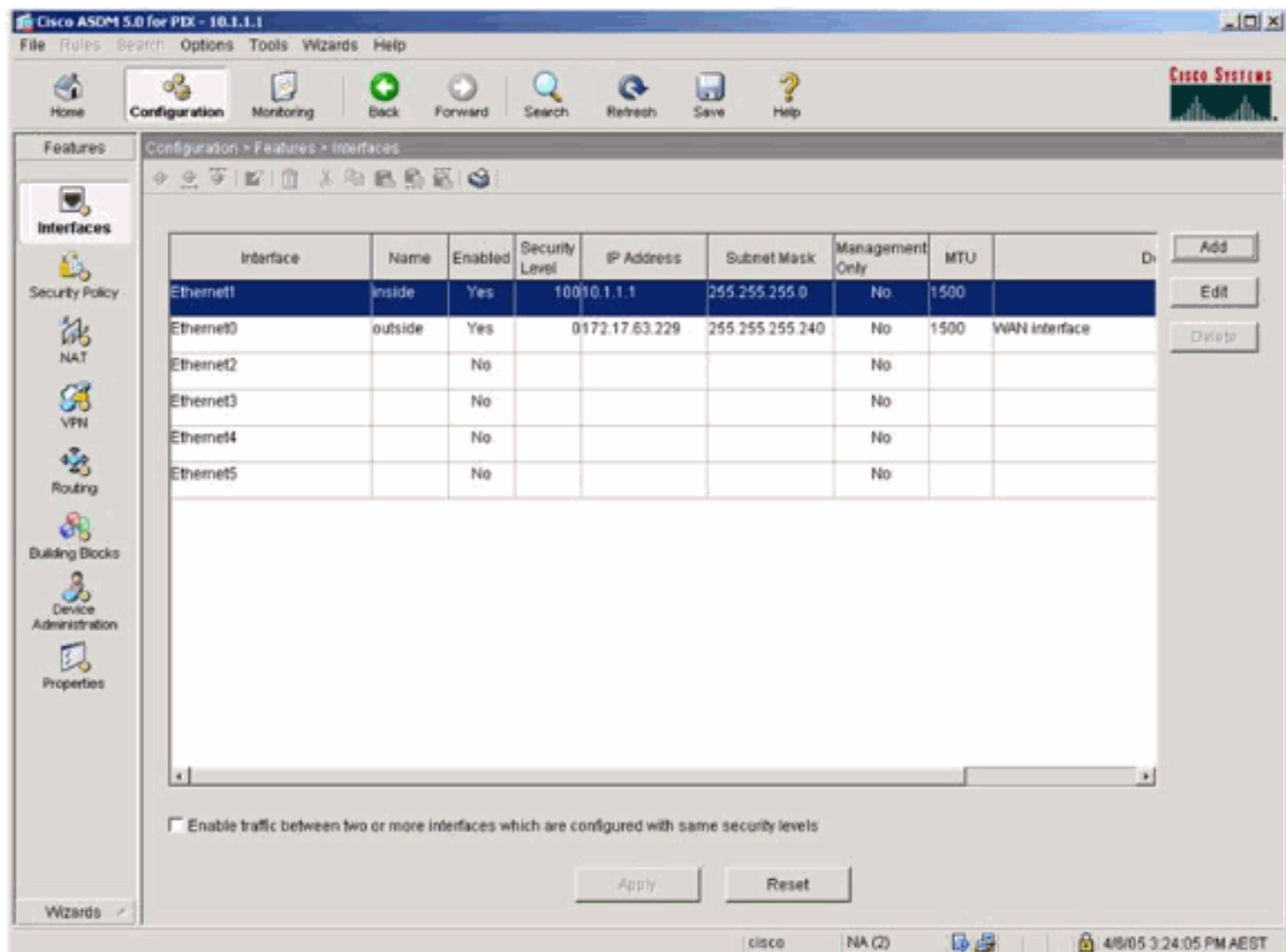
ASDM loads the existing configuration from the PIX.



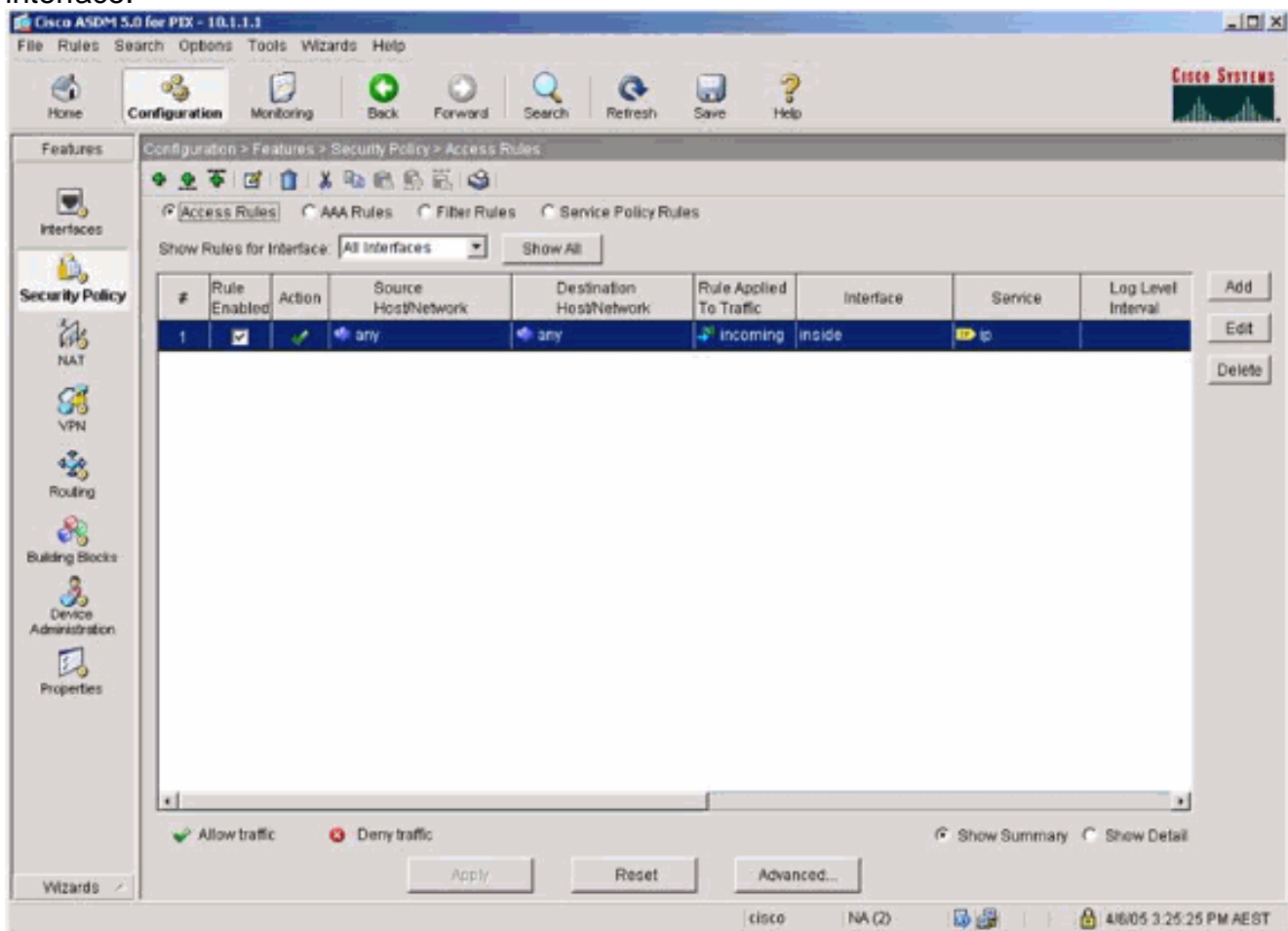
This window provides monitoring instruments and menus.



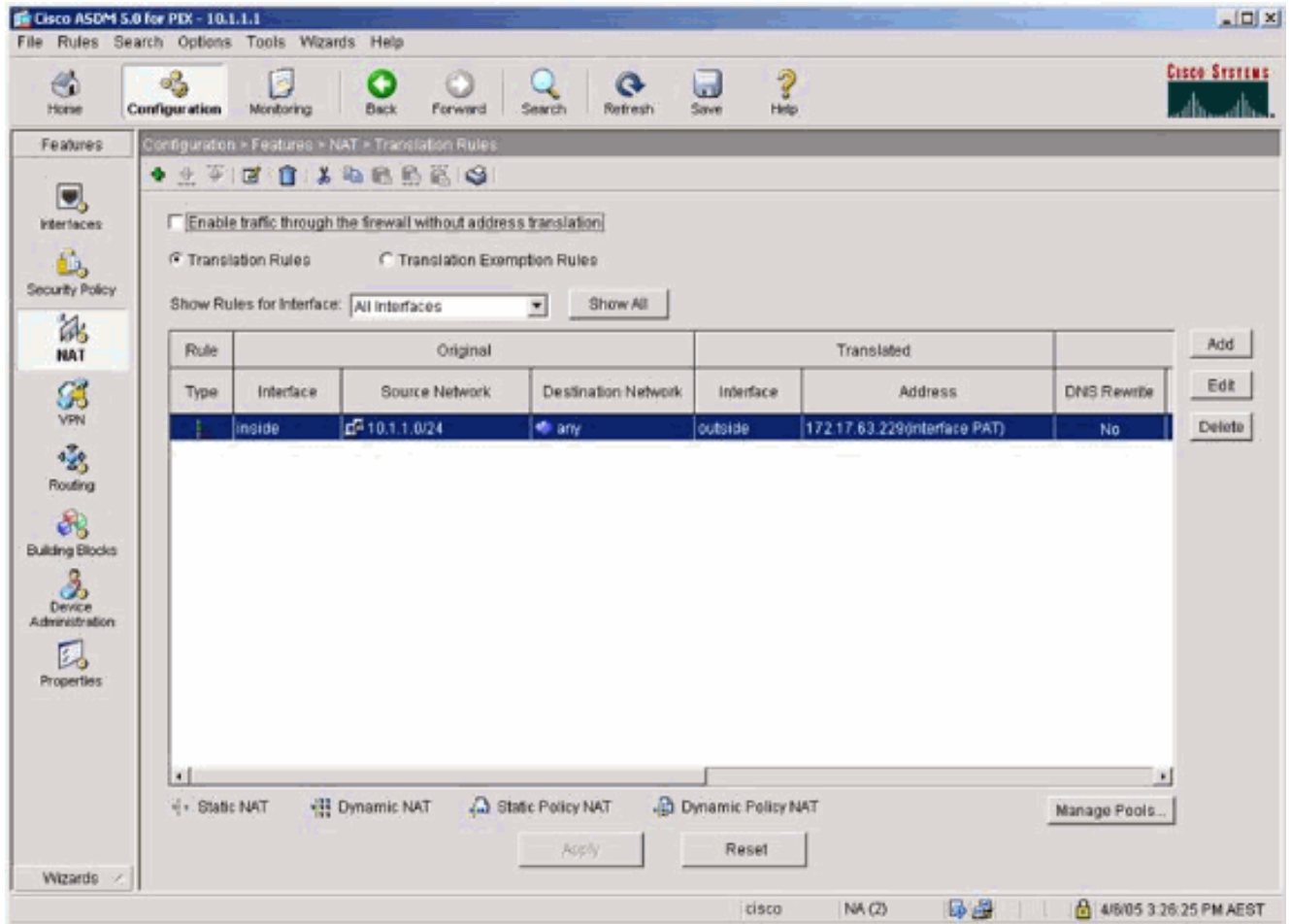
2. Select **Configuration > Features > Interfaces** and select **Add** for new interfaces or **Edit** for an existing configuration.



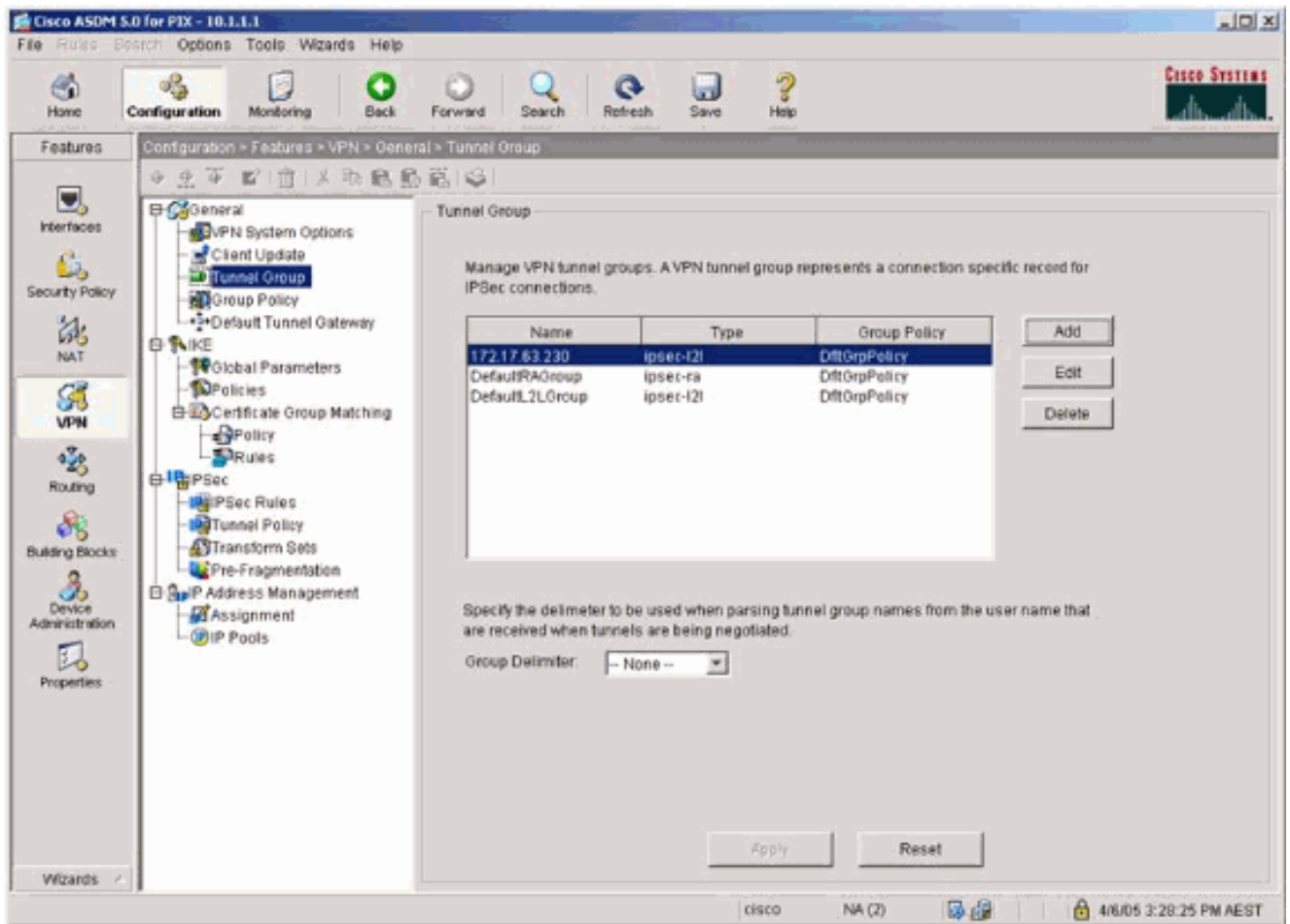
3. Select the security options for the inside interface.



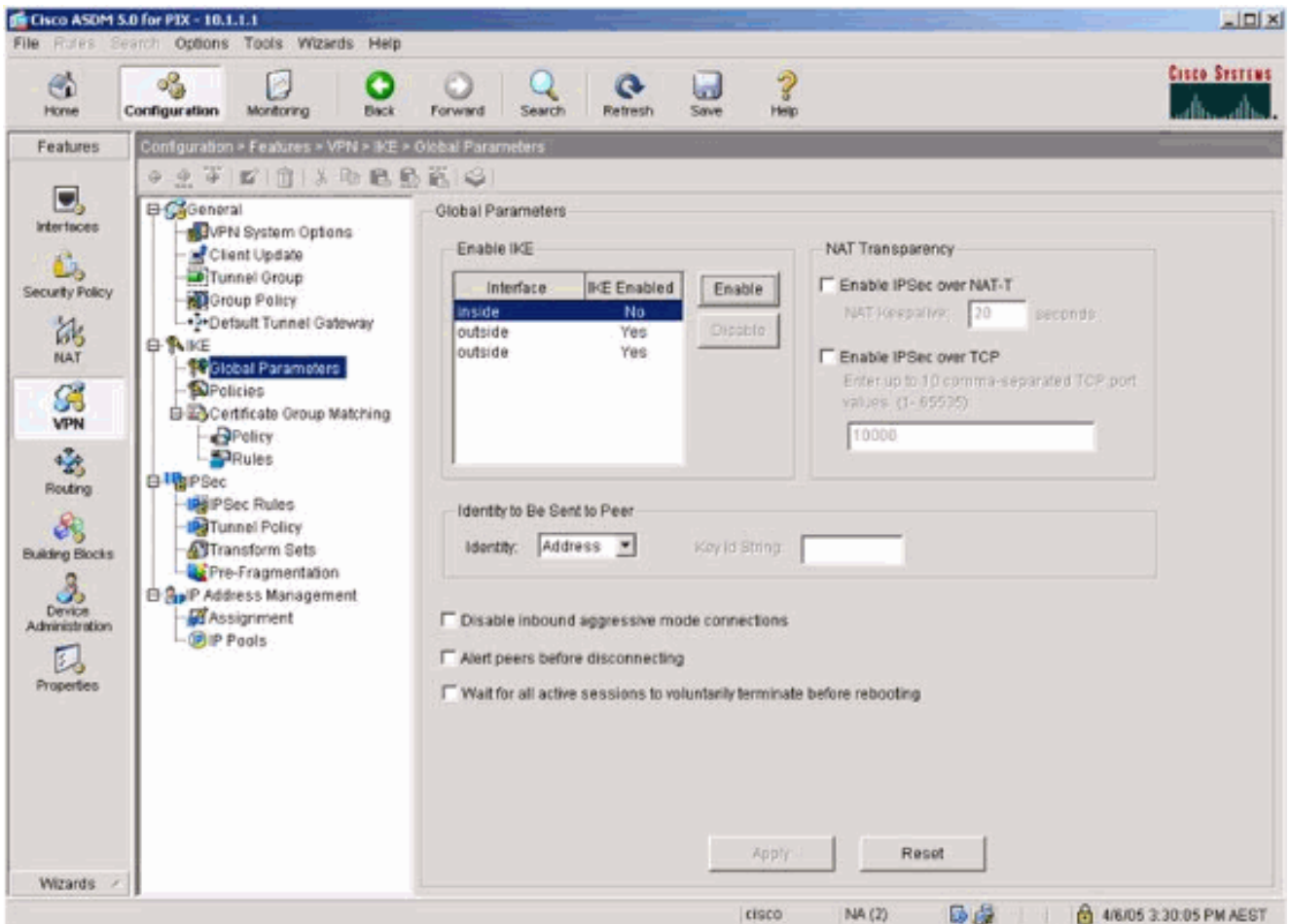
4. In the NAT configuration, encrypted traffic is NAT-exempt and all other traffic is NAT/PAT to the outside interface.



5. Select **VPN > General > Tunnel Group** and enable a Tunnel Group

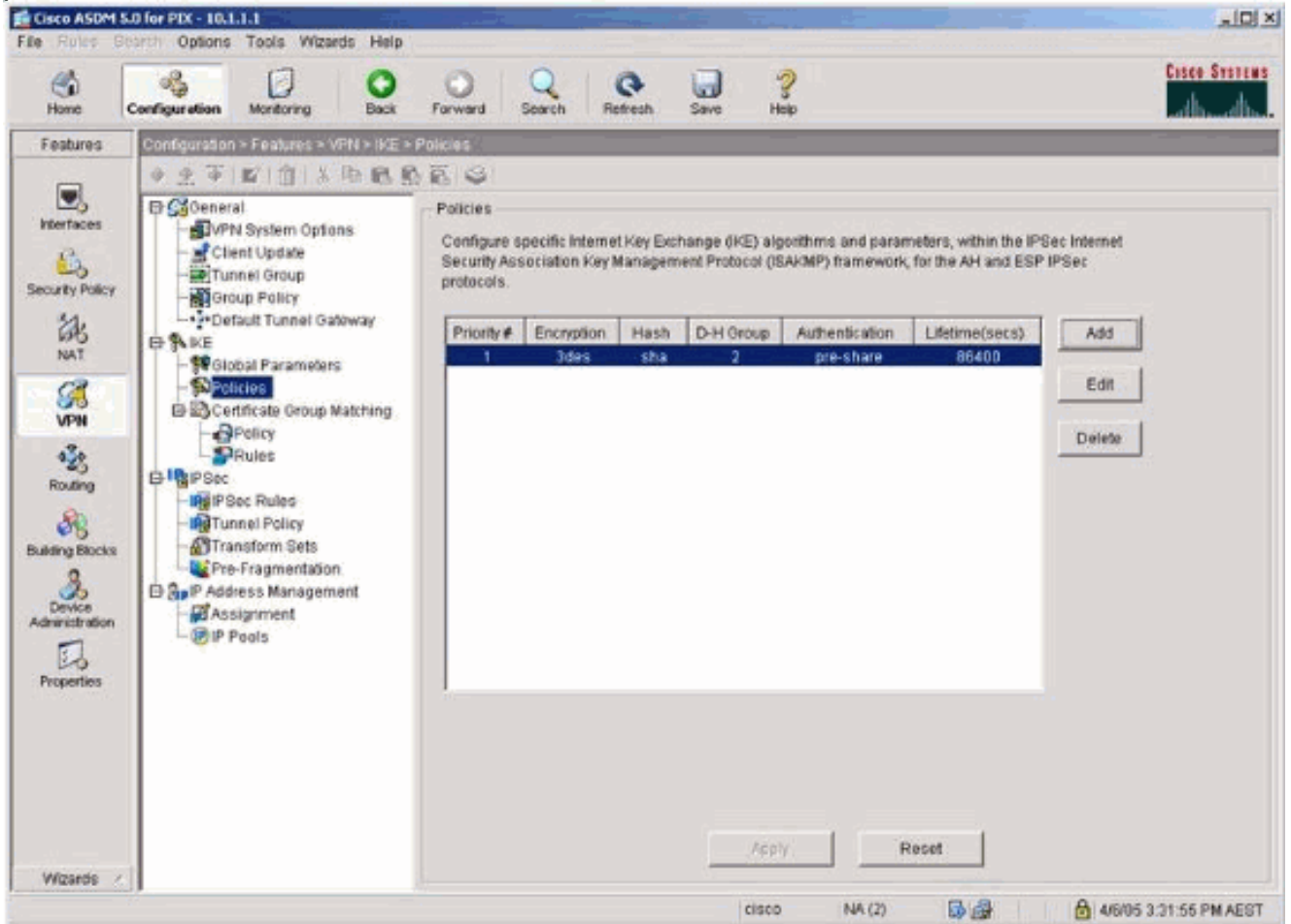


6. Select **VPN > IKE > Global Parameters** and enable IKE on the outside interface.

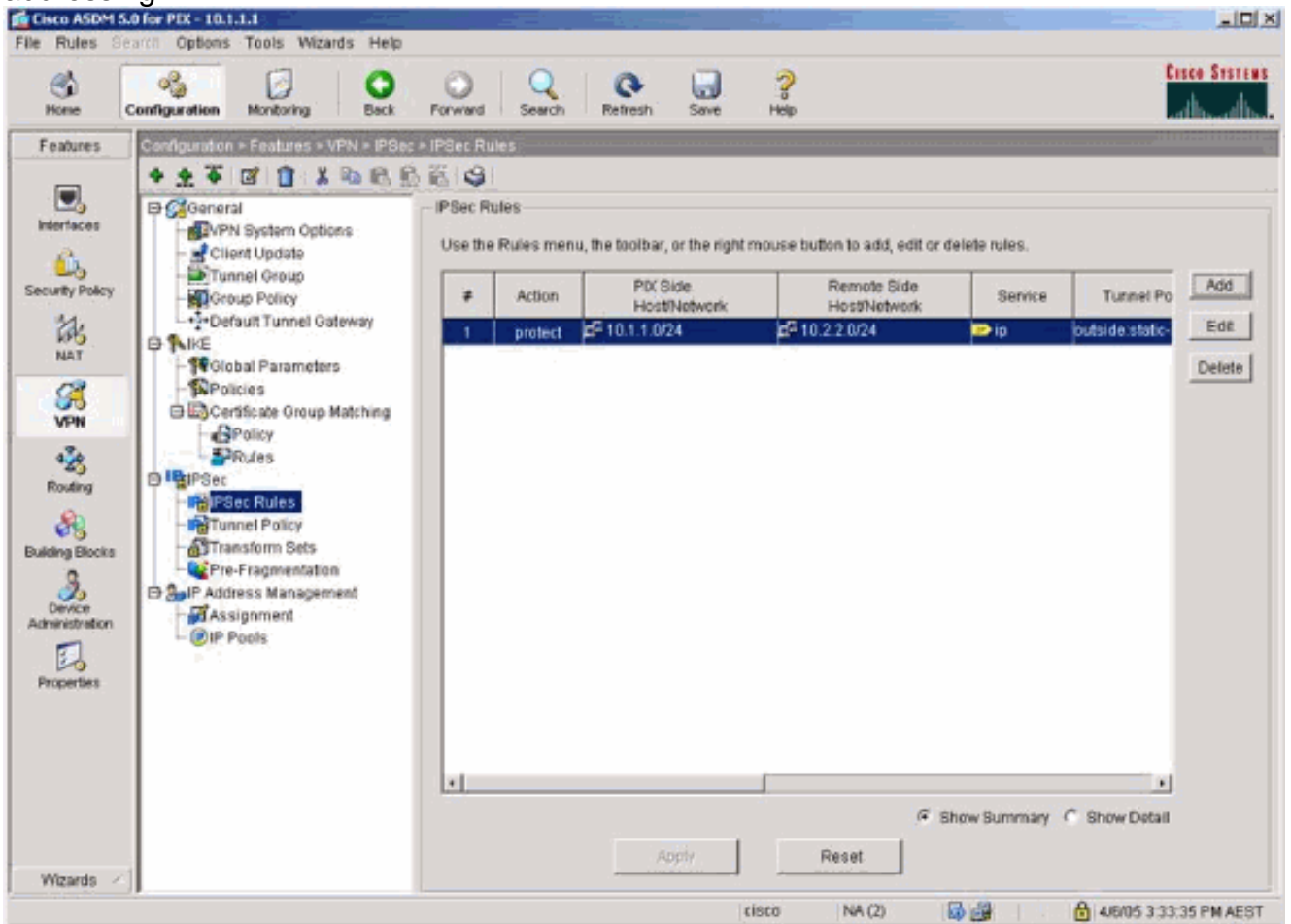


7. Select **VPN > IKE > Policies** and choose the IKE

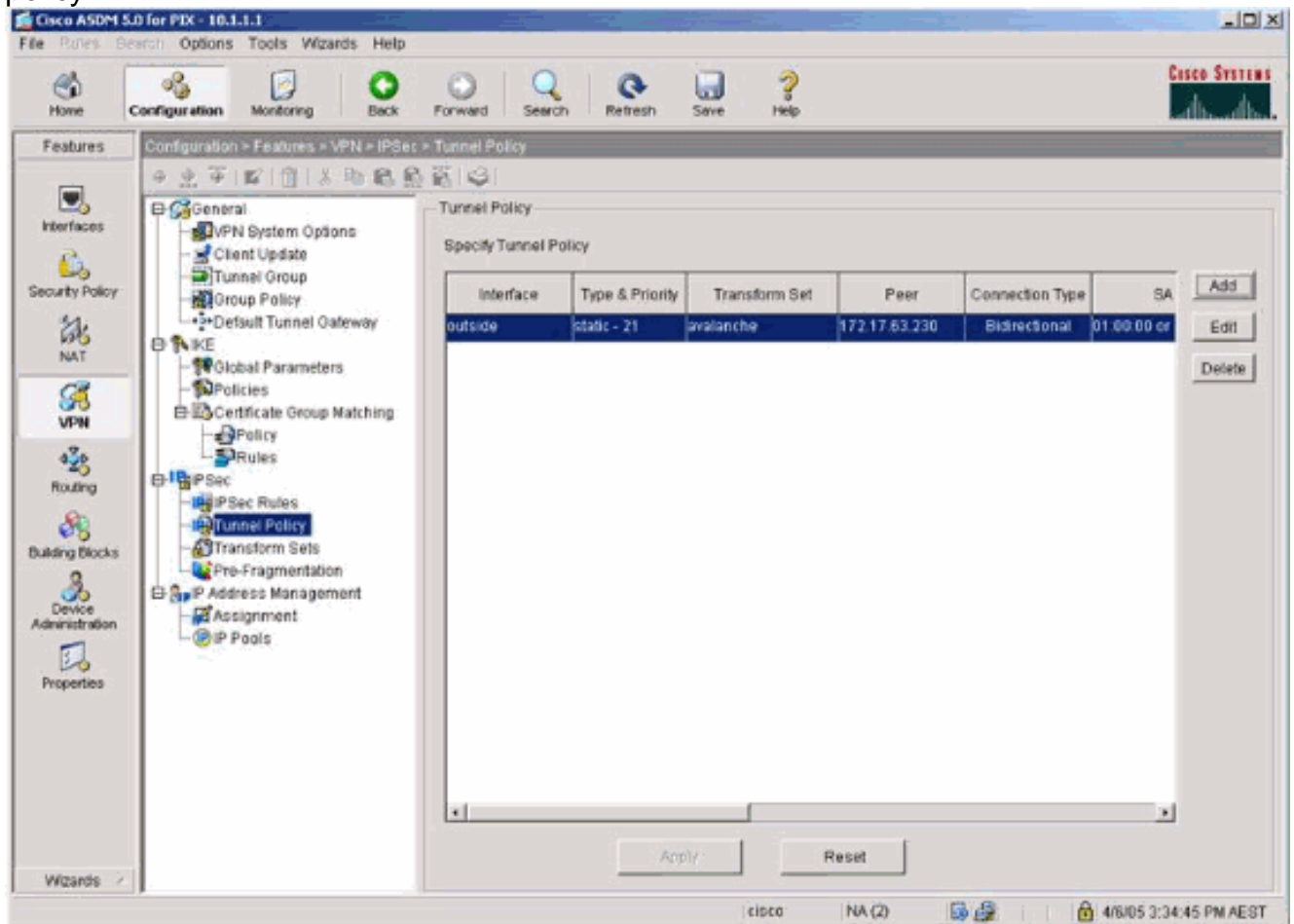
policies.



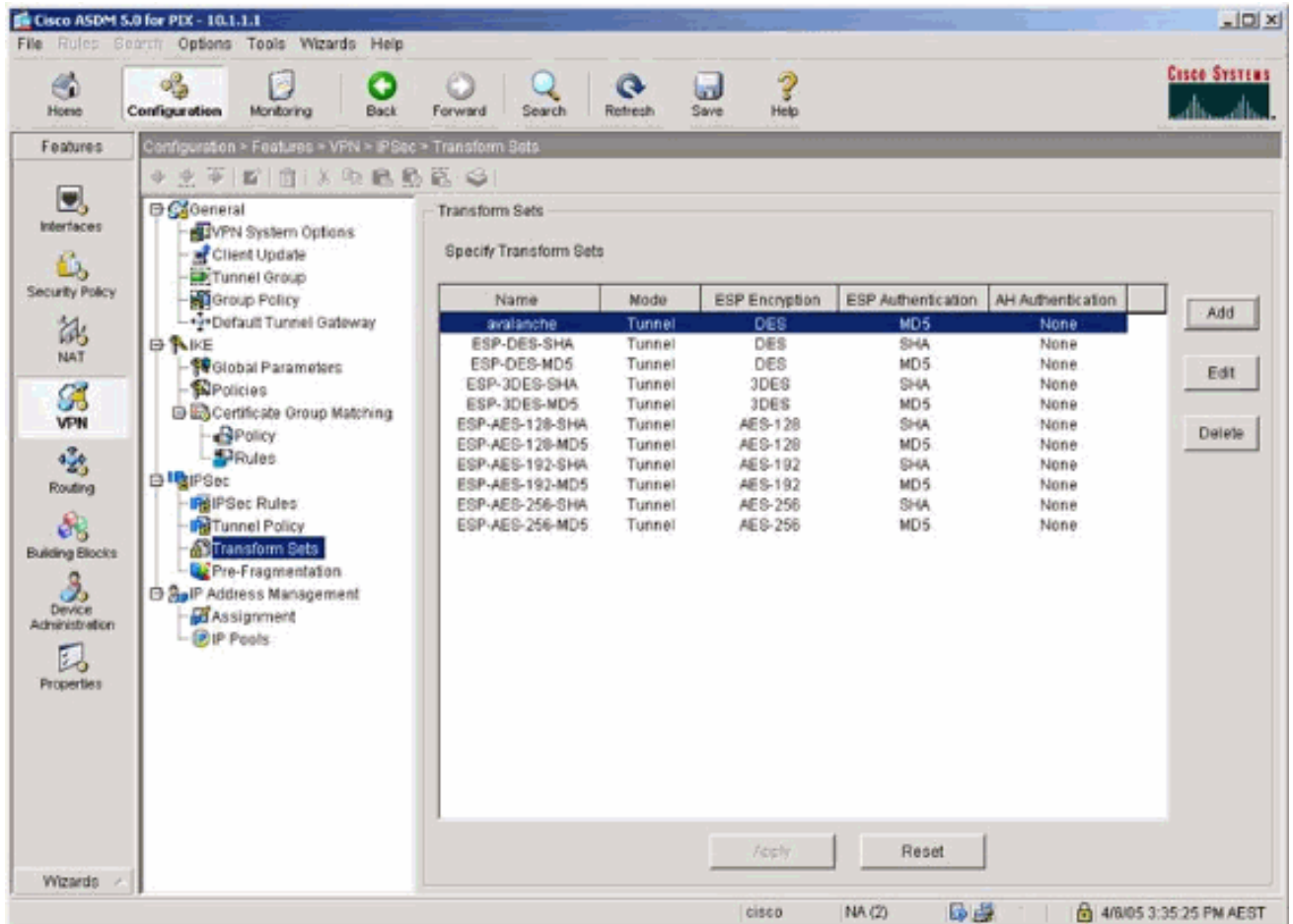
8. Select **VPN > IPsec > IPsec Rules** and choose **IPsec** for the local tunnel and remote addressing.



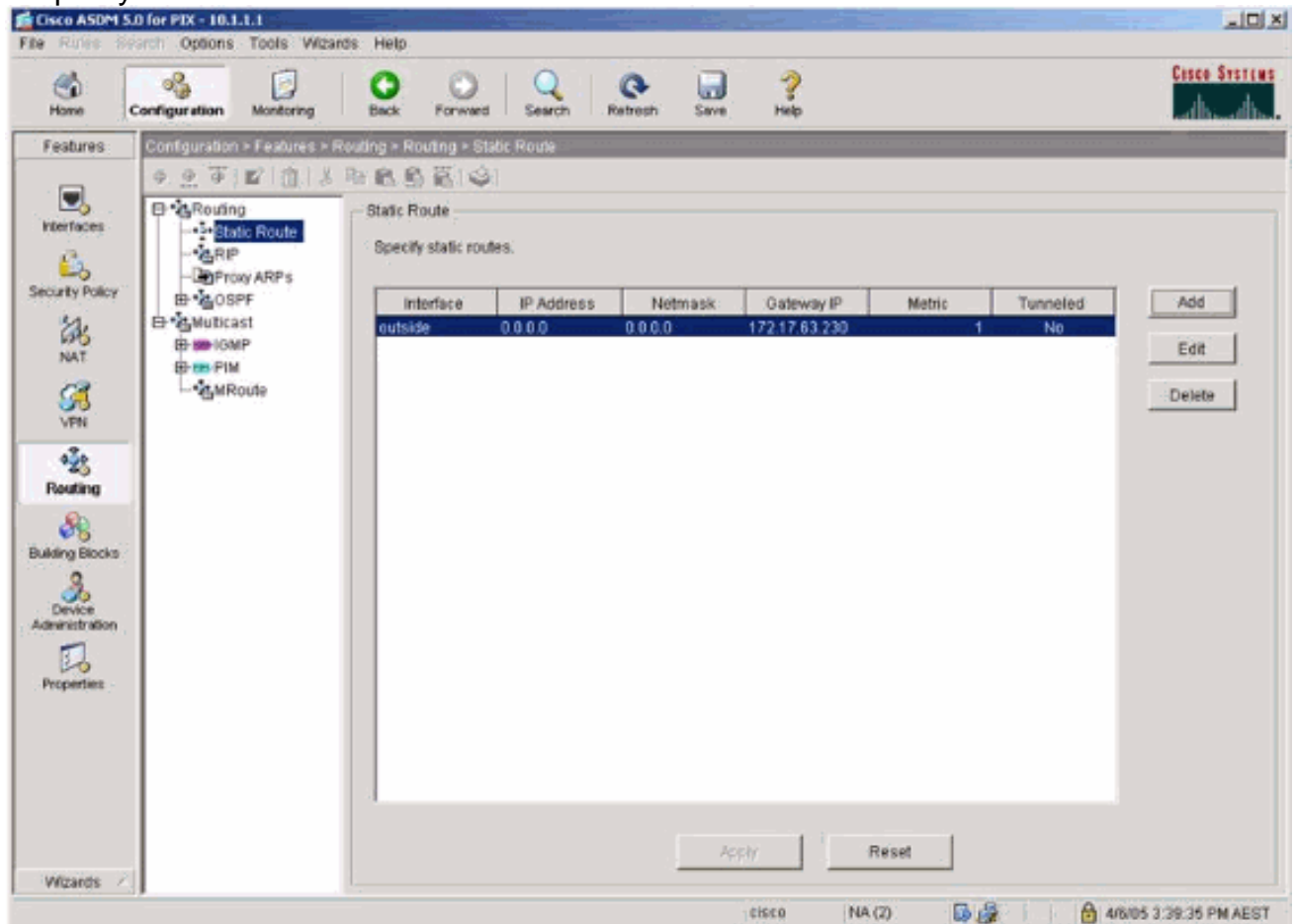
9. Select **VPN > IPsec > Tunnel Policy** and choose the tunnel policy.



10. Select **VPN > IPsec > Transform Sets** and choose a Transform set.



11. Select **Routing > Routing > Static Route** and choose a static route to gateway router. In this example, the static route points to the remote VPN peer for simplicity.



Verify

Use this section to confirm that your configuration works properly.

The [Output Interpreter Tool](#) ([registered](#) customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show crypto ipsec sa**—Shows the phase 2 security associations.
- **show crypto isakmp sa**—Shows the phase 1 security associations.

Troubleshoot

You can use ASDM to enable logging and to view the logs.

- Select **Configuration > Properties > Logging > Logging Setup**, choose **Enable Logging** and click **Apply** to enable logging.
- Select **Monitoring > Logging > Log Buffer > On Logging Level**, choose **Logging Buffer**, and click **View** to view the logs.


Troubleshooting Commands

The [Output Interpreter Tool](#) ([registered](#) customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to [Important Information on Debug Commands](#) before you use **debug** commands.

- **debug crypto ipsec**—Shows the IPsec negotiations of phase 2.
- **debug crypto isakmp**—Shows the ISAKMP negotiations of phase 1.
- **debug crypto engine**—Shows the traffic that is encrypted.
- **clear crypto isakmp**—Clears the security associations related to phase 1.
- **clear crypto sa**—Clears the security associations related to phase 2.
- **debug icmp trace**—Shows whether ICMP requests from the hosts reach the PIX. You need to add the **access-list** command to permit ICMP in your configuration in order to run this debug.
- **logging buffer debugging**—Shows connections being established and denied to hosts that go through the PIX. The information is stored in the PIX log buffer and you can see the output with the **show log** command.

Related Information

- [Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions](#)
- [Cisco PIX Firewall Software](#)
- [Cisco Secure PIX Firewall Command References](#)
- [Security Product Field Notices \(including PIX\)](#)
- [Requests for Comments \(RFCs\)](#) 
- [Technical Support & Documentation - Cisco Systems](#)