

ASA/PIX - configureren van een Cisco IOS router LAN-to-LAN IPsec tunnel

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Configuratie met ASDM](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Opdrachten voor troubleshooting](#)

[Gerelateerde informatie](#)

Inleiding

Dit document demonstreert hoe u een IPsec-tunnel kunt configureren van PIX security applicatie 7.x en hoger of van de adaptieve security applicatie (ASA) via één intern netwerk naar een router uit 2611 met een crypto-afbeelding. Statische routes worden gebruikt voor eenvoud.

Raadpleeg [IPSec configureren - router naar PIX](#) voor meer informatie over een LAN-to-LAN tunnelconfiguratie tussen een router en de PIX.

Raadpleeg [LAN-to-LAN IPSec-tunnels tussen de Cisco VPN 3000 Concentrator en PIX-firewall Configuratievoorbeeld](#) voor meer informatie over een LAN-to-LAN tunnelconfiguratie tussen de PIX-firewall en Cisco VPN 3000 Concentrator.

Raadpleeg [IPsec-tunnelheid tussen PIX 7.x en VPN 3000 Concentrator Configuration Voorbeeld](#) om meer te weten te komen over het scenario waarin de LAN-to-LAN-tunnel tussen de PIX- en VPN-centrator ligt.

Raadpleeg [PIX/ASA 7.x Enhanced Spoke-to-Client VPN met het Configuratievoorbeeld van TACACS+ verificatie](#) om meer te weten te komen over het scenario waarin de LAN-to-LAN tunnel tussen de PIX-apparaten ook een VPN-client toestaat om de opgenomen PIX te benaderen via de hub PIX.

Raadpleeg [DM: Site-to-Site IPsec VPN tussen ASA/PIX en een IOS routerconfiguratievoorbeeld](#) om meer te weten te komen over hetzelfde scenario waarin PIX/ASA security applicatie

softwareversie 8.x uitvoert.

Raadpleeg [Configuration Professional: Site-to-Site IPsec VPN tussen ASA/PIX en een IOS routerconfiguratievoorbeld](#) om meer te weten te komen over hetzelfde scenario waarin de ASA-gerelateerde configuratie wordt weergegeven met behulp van ASDM GUI en de routergerelateerde configuratie wordt weergegeven met behulp van Cisco CP GUI.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- PIX-525 met PIX-softwareversie 7.0
- Cisco 2611 router met Cisco IOS® softwarerelease 12.2(15)T13

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

Achtergrondinformatie

In de PIX werken de **toeganglijst** en de **nat 0** opdrachten samen. Wanneer een gebruiker op het 10.1.1.0-netwerk naar het 10.2.2.0-netwerk gaat, wordt de toeganglijst gebruikt om ervoor te zorgen dat het 10.1.1.0-netwerkverkeer kan worden versleuteld zonder Netwerkadresomzetting (NAT). Op de router worden de **route-kaart** en de **toeganglijst** opdrachten gebruikt om het netwerkverkeer 10.2.2.0 toe te staan om zonder NAT te worden versleuteld. Maar als deze zelfde gebruikers ook maar ergens anders naartoe gaan, worden ze vertaald naar het 172.17.63.230-adres via Port Address Translation (PAT).

Dit zijn de configuratieopdrachten die op de PIX security applicatie vereist zijn, zodat verkeer *niet* door PAT in de tunnel kan rijden en verkeer naar het internet om door PAT te lopen

```
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
```

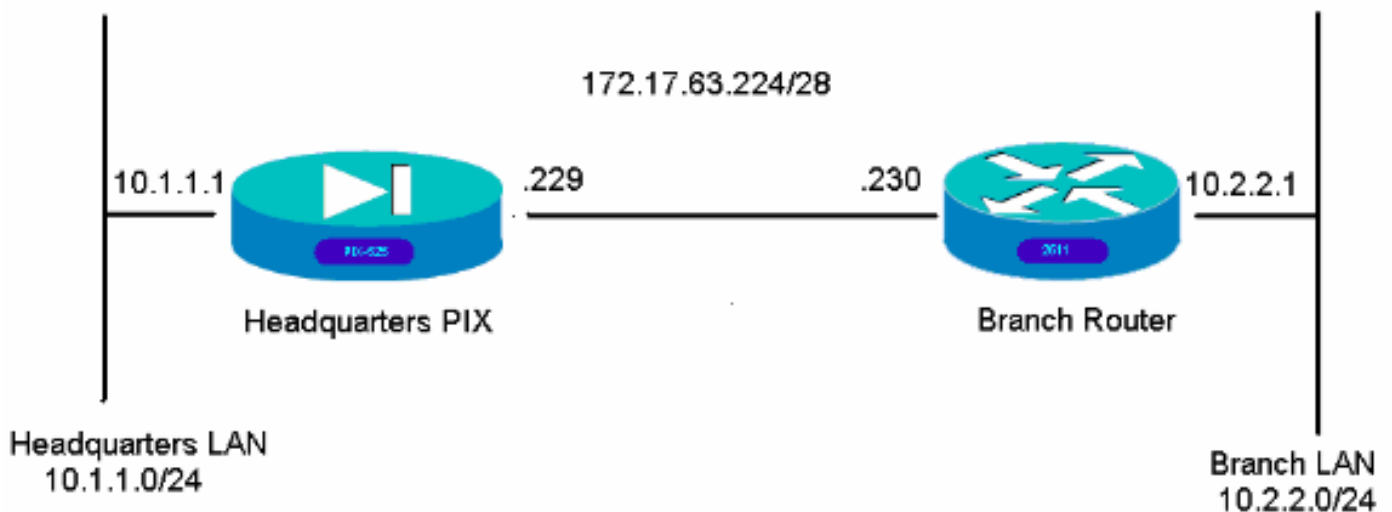
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het [Opname Gereedschap](#) ([alleen geregistreerde](#) klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

[Netwerkdigram](#)

Het netwerk in dit document is als volgt opgebouwd:



[Configuraties](#)

Deze configuratievoorbeelden zijn voor de opdrachtregel interface. Zie het gedeelte [Configuration](#) met [Adaptieve Security Devices Manager \(ASDM\)](#) van dit document als u liever wilt configureren met behulp van ASDM.

- [Hoofdkantoor PIX](#)
- [Vestigingsrouter](#)

Hoofdkantoor 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 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
```

Vestigingsrouter

```
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

```



[Configuratie met ASDM](#)

Dit voorbeeld toont aan hoe te om PIX te vormen met behulp van de ASDM GUI. Een PC met een browser en IP adres 10.1.1.2 wordt aangesloten op de binneninterface e1 van de PIX. Zorg ervoor

dat http is ingeschakeld op de PIX.

Deze procedure illustreert de ASDM-configuratie van het hoofdkwartier PIX.

1. Sluit de PC aan op de PIX en kies een downloadmethode.

 **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](#)

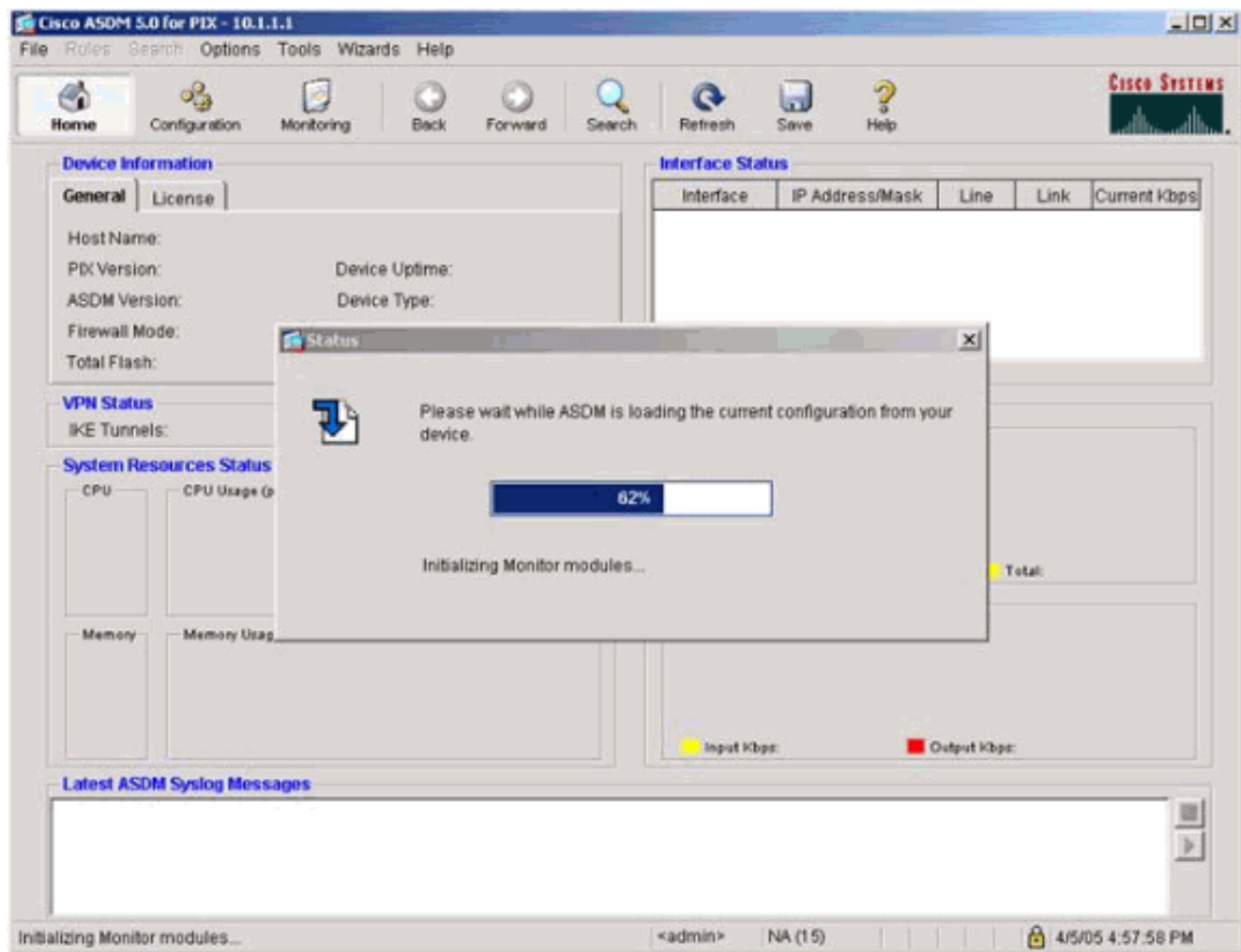
Running Cisco ASDM as a Java Applet

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 laadt de bestaande configuratie uit de PIX.



Dit venster biedt controle-instrumenten en -menu's.

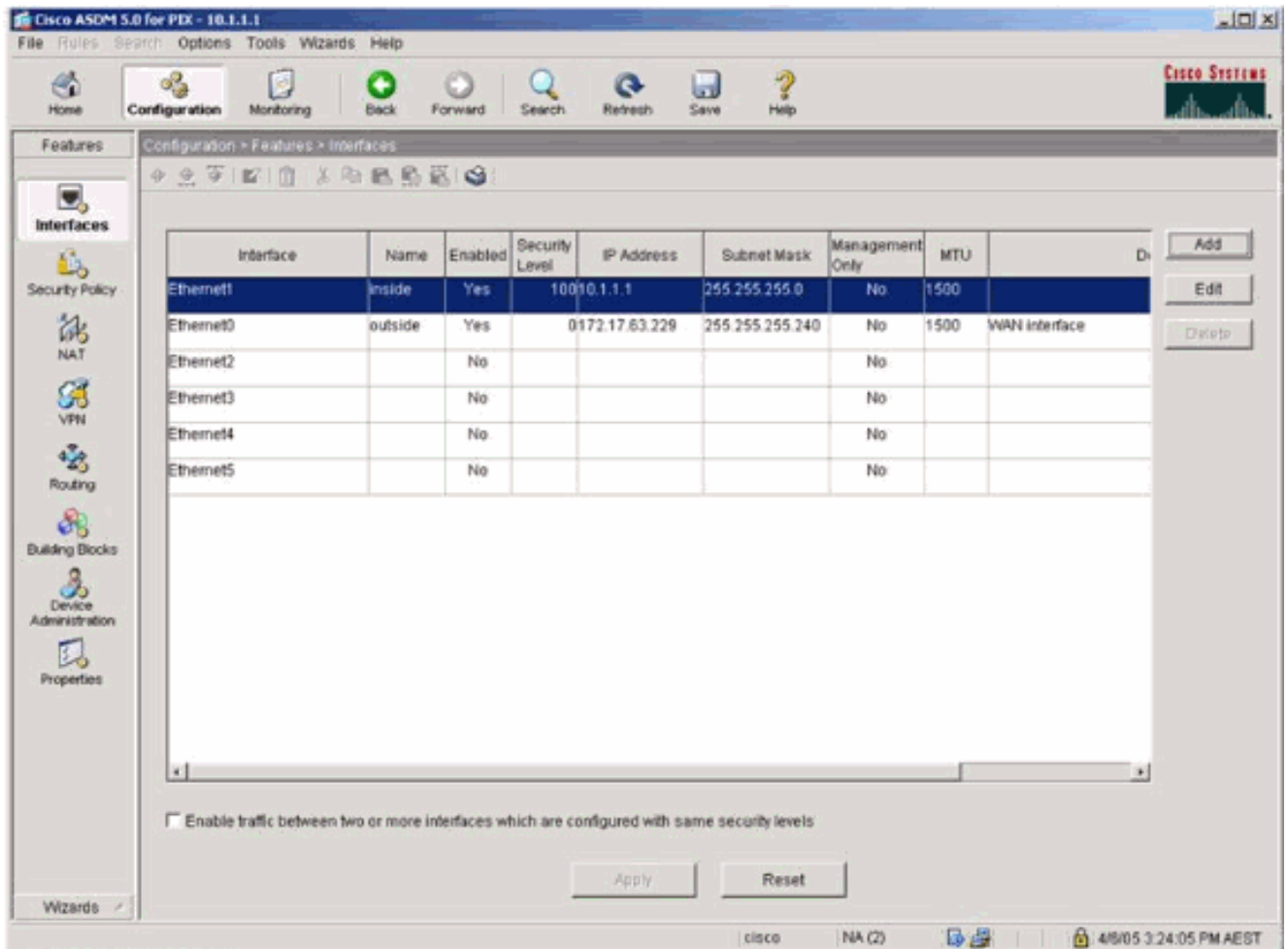
The screenshot displays the Cisco ASDM 5.0 for PIX - 10.1.1.1 interface. The top navigation bar includes Home, Configuration, Monitoring, Back, Forward, Search, Refresh, Save, and Help. The main content area is divided into several sections:

- Device Information:**
 - General: Host Name: SV-2-B.cisco.com, PIX Version: 7.0(0)102, ASDM Version: 5.0(0)73, Firewall Mode: Routed, Total Flash: 16 MB.
 - License: Device Uptime: 0d 0h 24m 50s, Device Type: PIX 525, Context Mode: Single, Total Memory: 256 MB.
- Interface Status:**

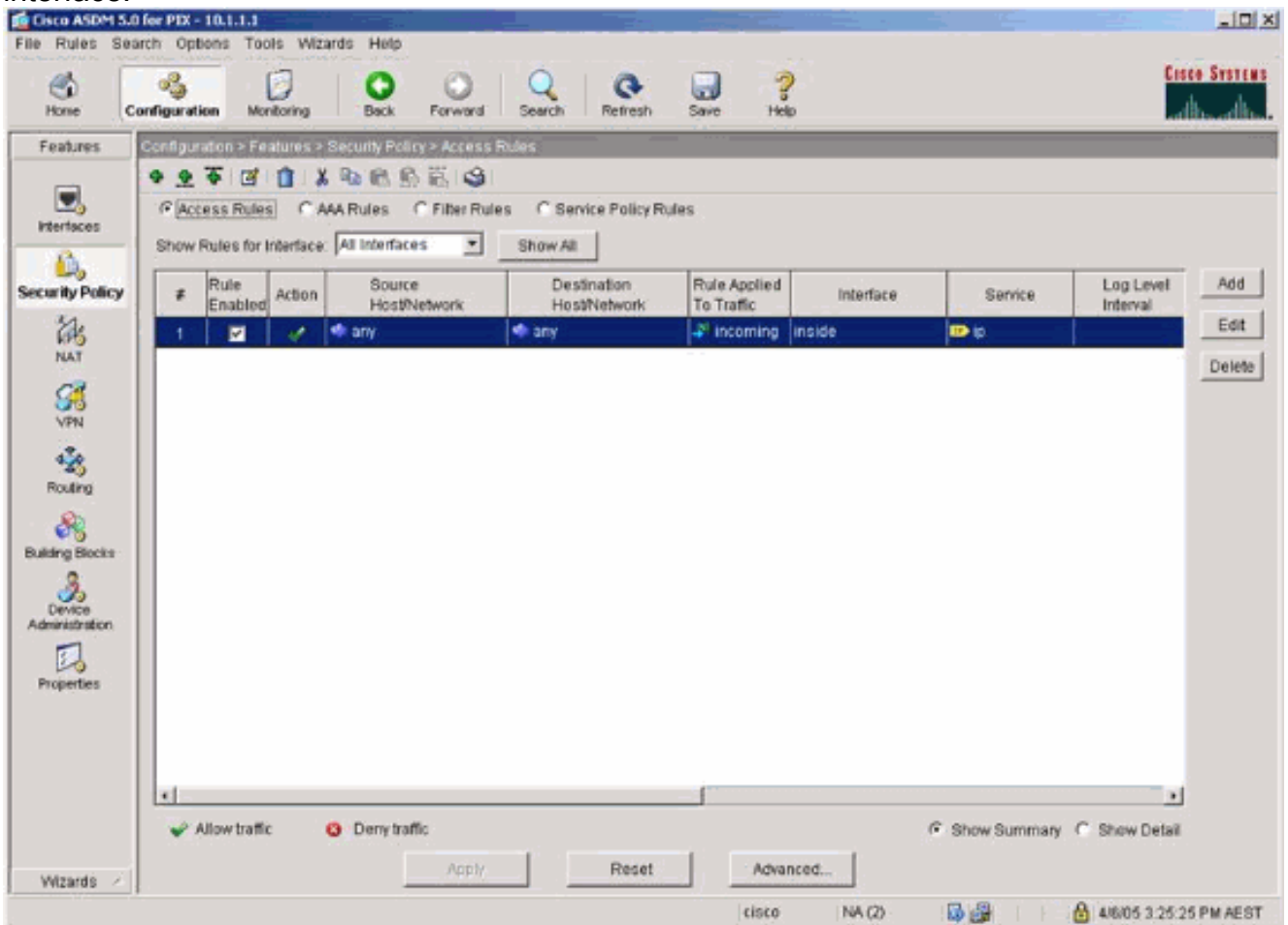
Interface	IP Address/Mask	Line	Link	Current Kbps
inside	10.1.1.1/24	up	up	1
- VPN Status:** IKE Tunnels: 0, IPsec Tunnels: 0.
- System Resources Status:**
 - CPU: 0% (04:57:46), CPU Usage (percent) graph.
 - Memory: 67MB (04:57:46), Memory Usage (MB) graph.
- Traffic Status:**
 - Connections Per Second Usage graph.
 - 'inside' Interface Traffic Usage (Kbps) graph showing Input Kbps: 0 and Output Kbps: 1.
- Latest ASDM Syslog Messages:** -- Syslog Disabled --

The bottom status bar shows: Device configuration loaded successfully, <admin>, NA (15), and 4/5/05 4:57:46 AM UTC.

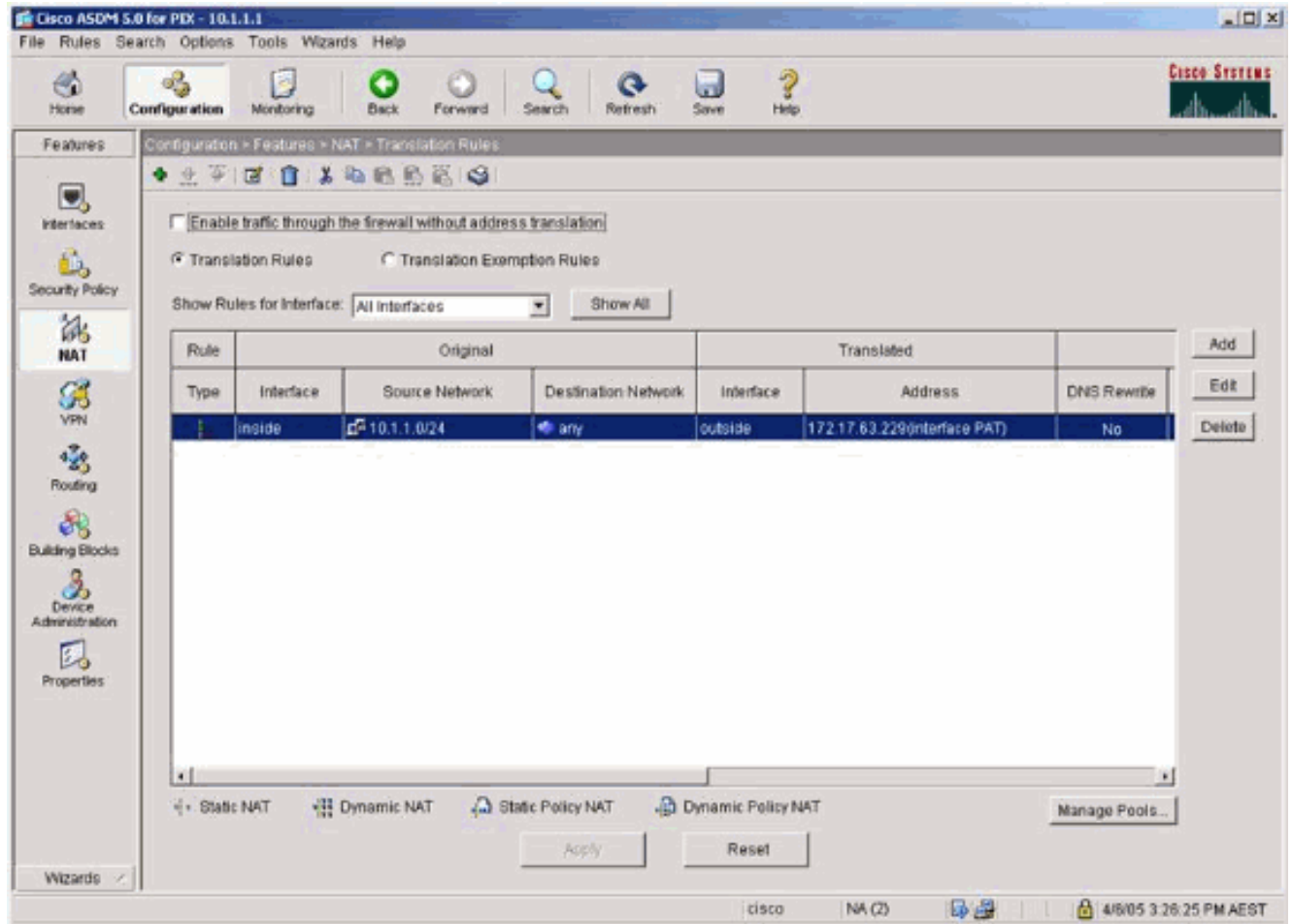
2. Selecteer **Configuratie > Functies > Interfaces** en selecteer **Toevoegen** voor nieuwe interfaces of **Bewerken** voor een bestaande configuratie.



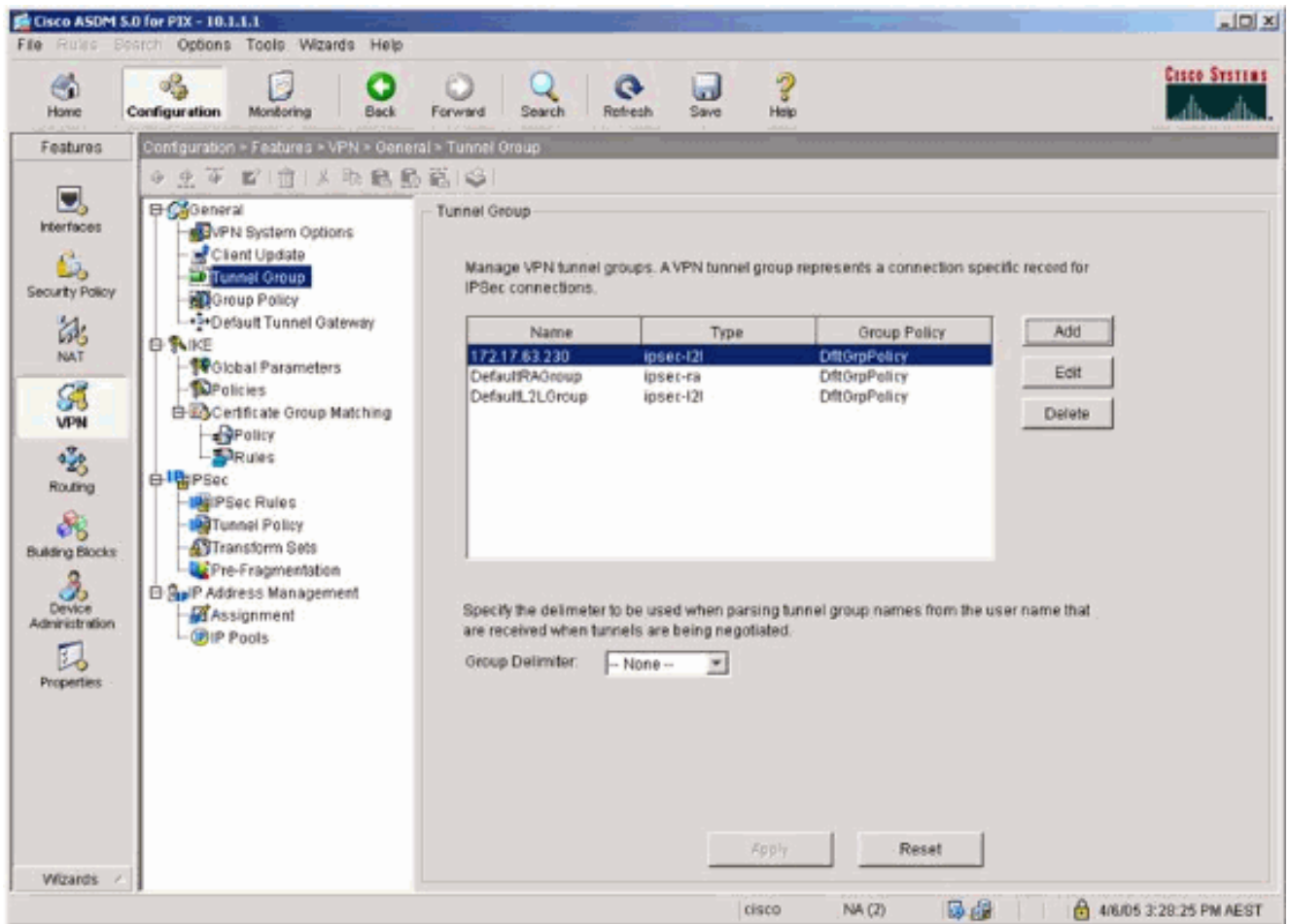
3. Selecteer de beveiligingsopties voor de interne interface.



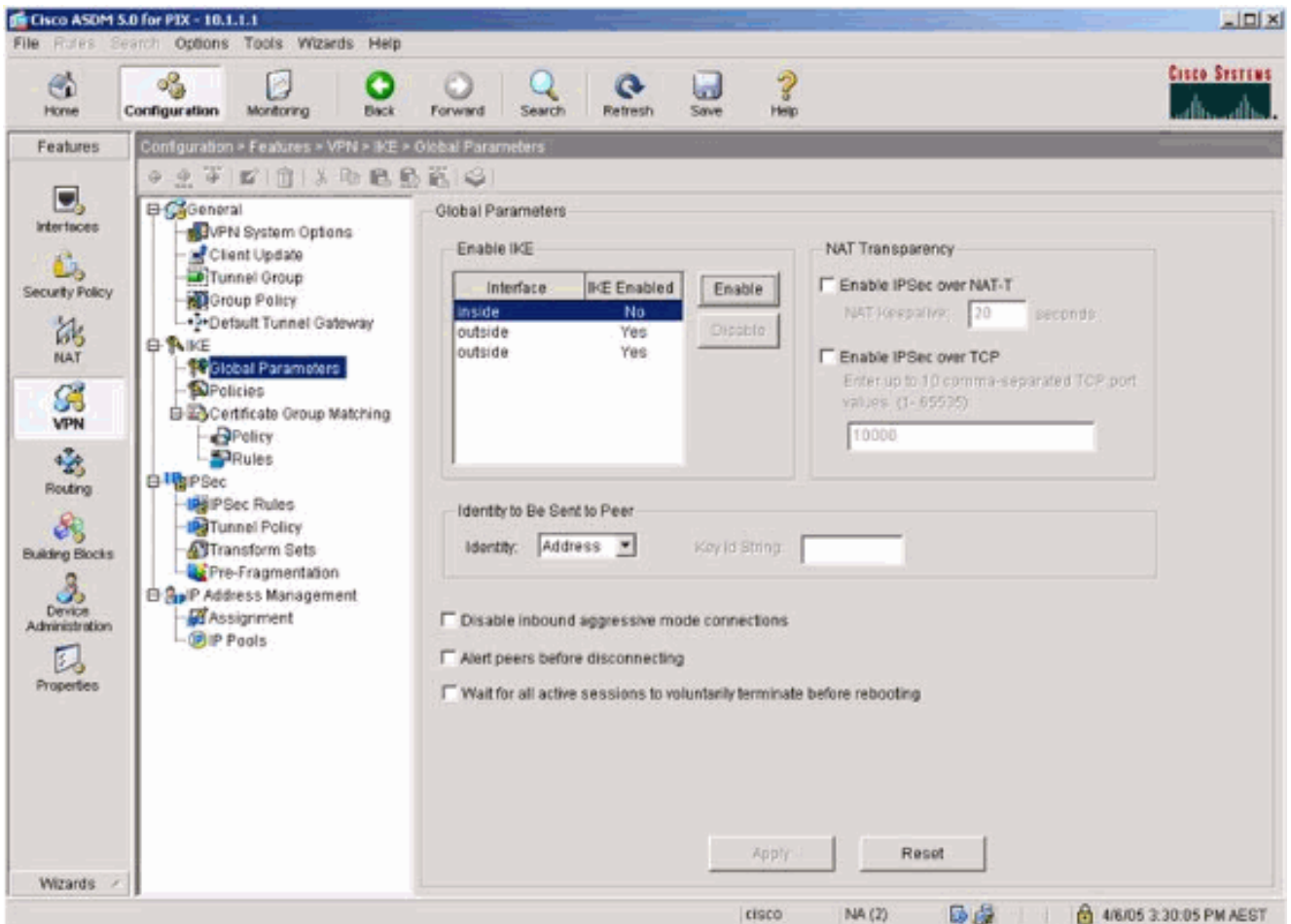
4. In de NAT-configuratie is het gecodeerde verkeer NAT-vrijgesteld en al het andere verkeer NAT/PAT aan de externe interface is.



5. Selecteer VPN >General > Tunnel Group en zet een tunnelgroep in

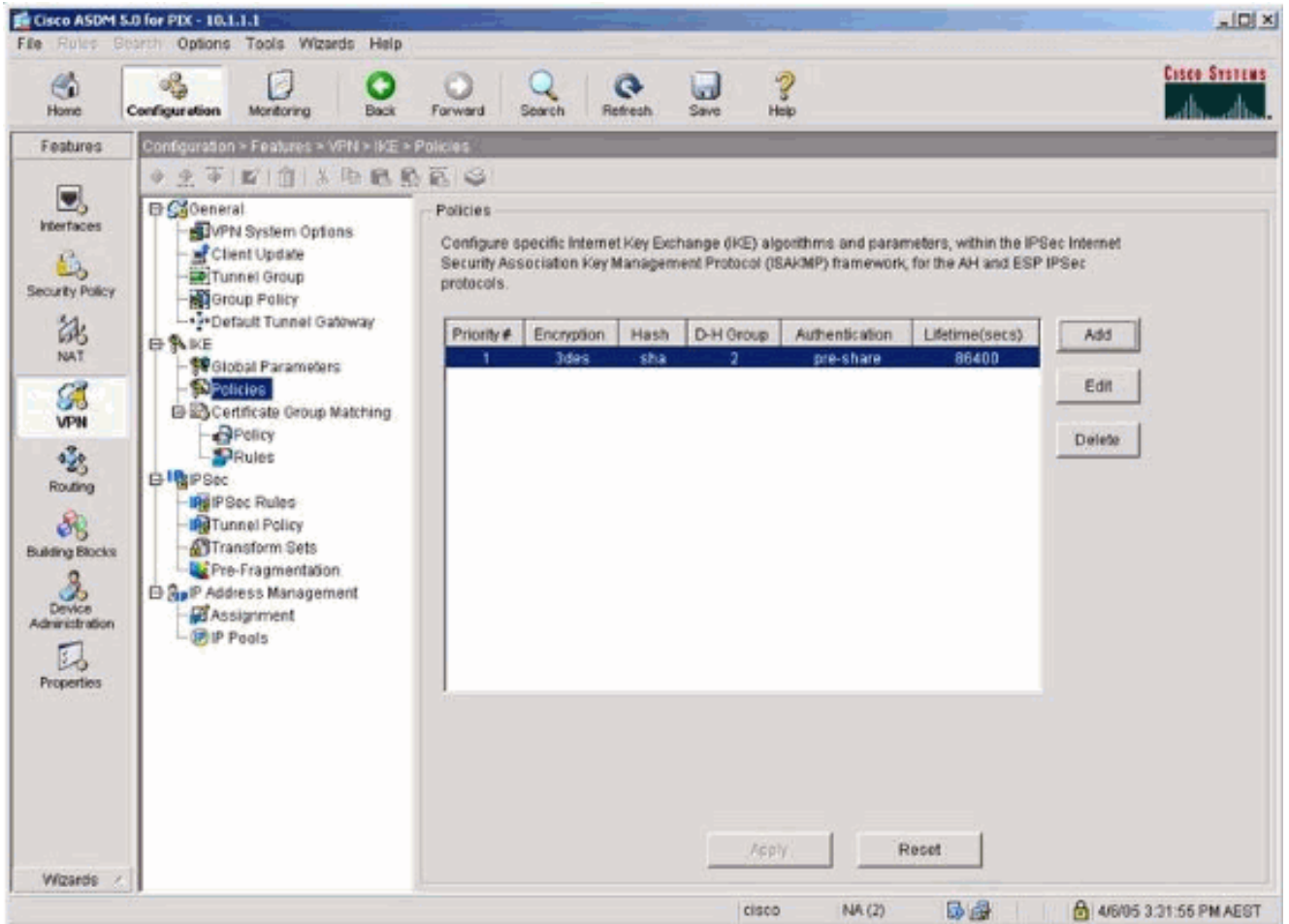


6. Selecteer VPN > IKE > Mondiale parameters en schakel IKE in op de externe interface.

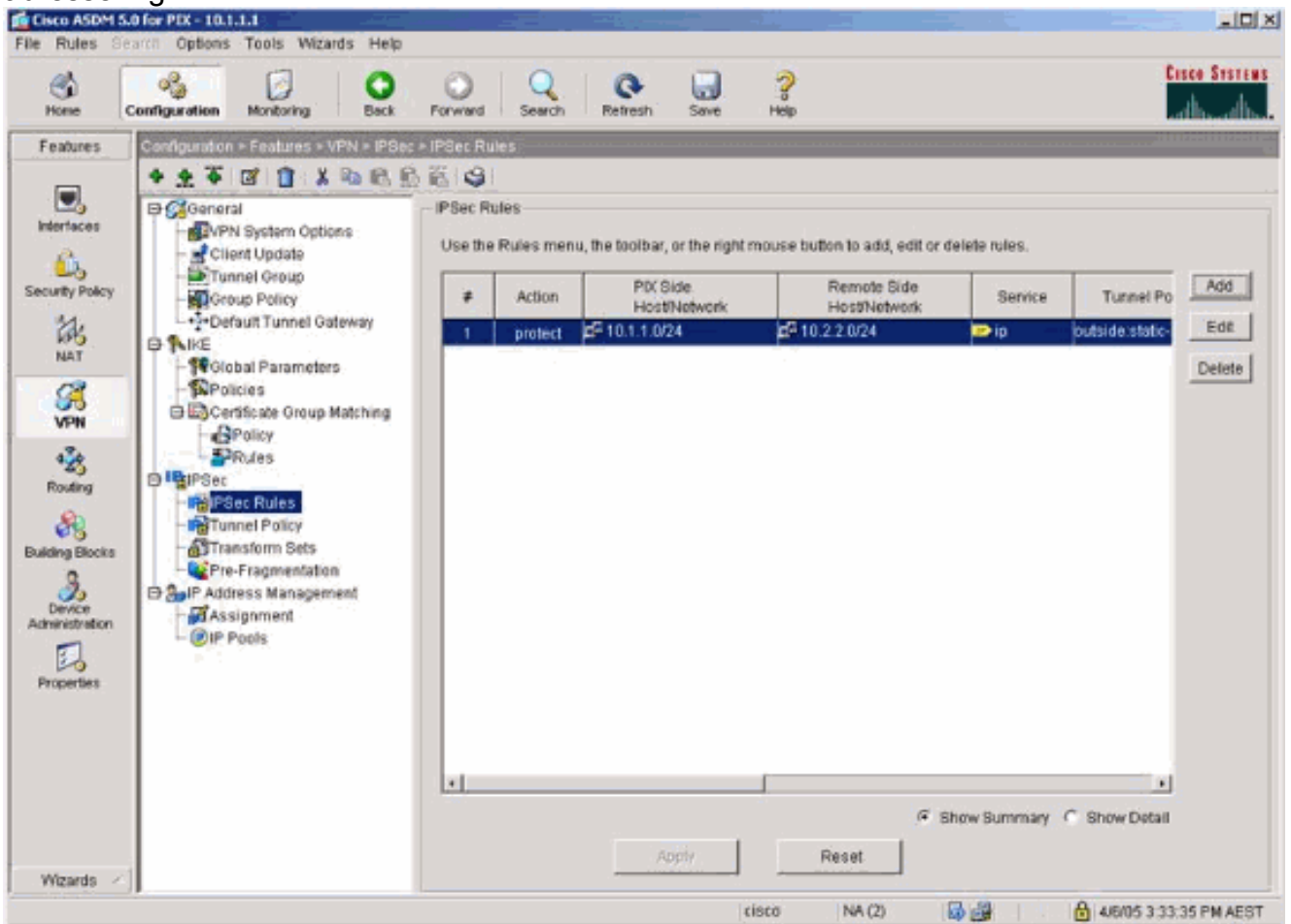


7. Selecteer VPN > IKE > Beleid en kies het IKE-

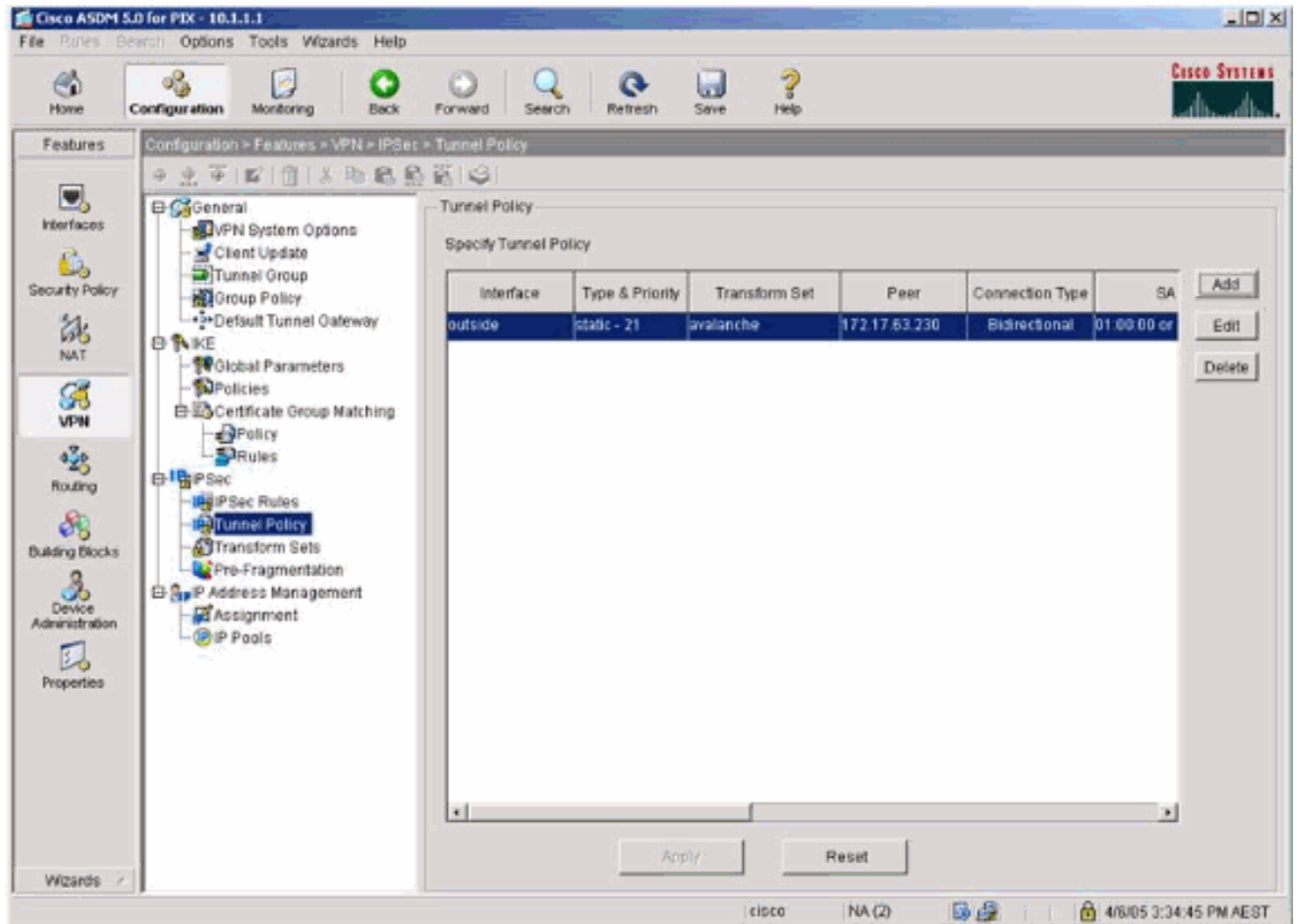
beleid.



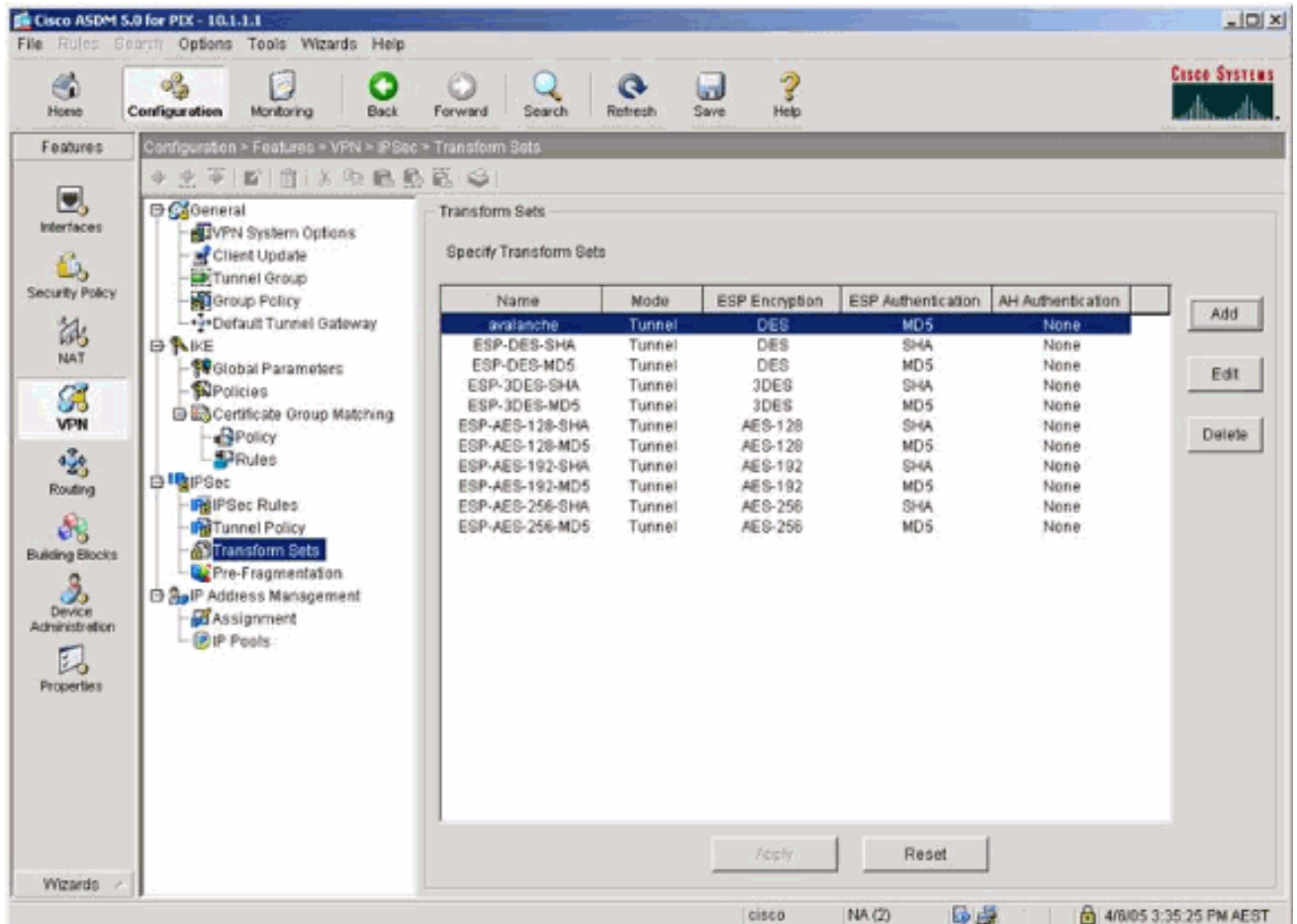
8. Selecteer VPN > IPsec > IPsec Regels en kies IPsec voor de lokale tunnel en externe adressering.



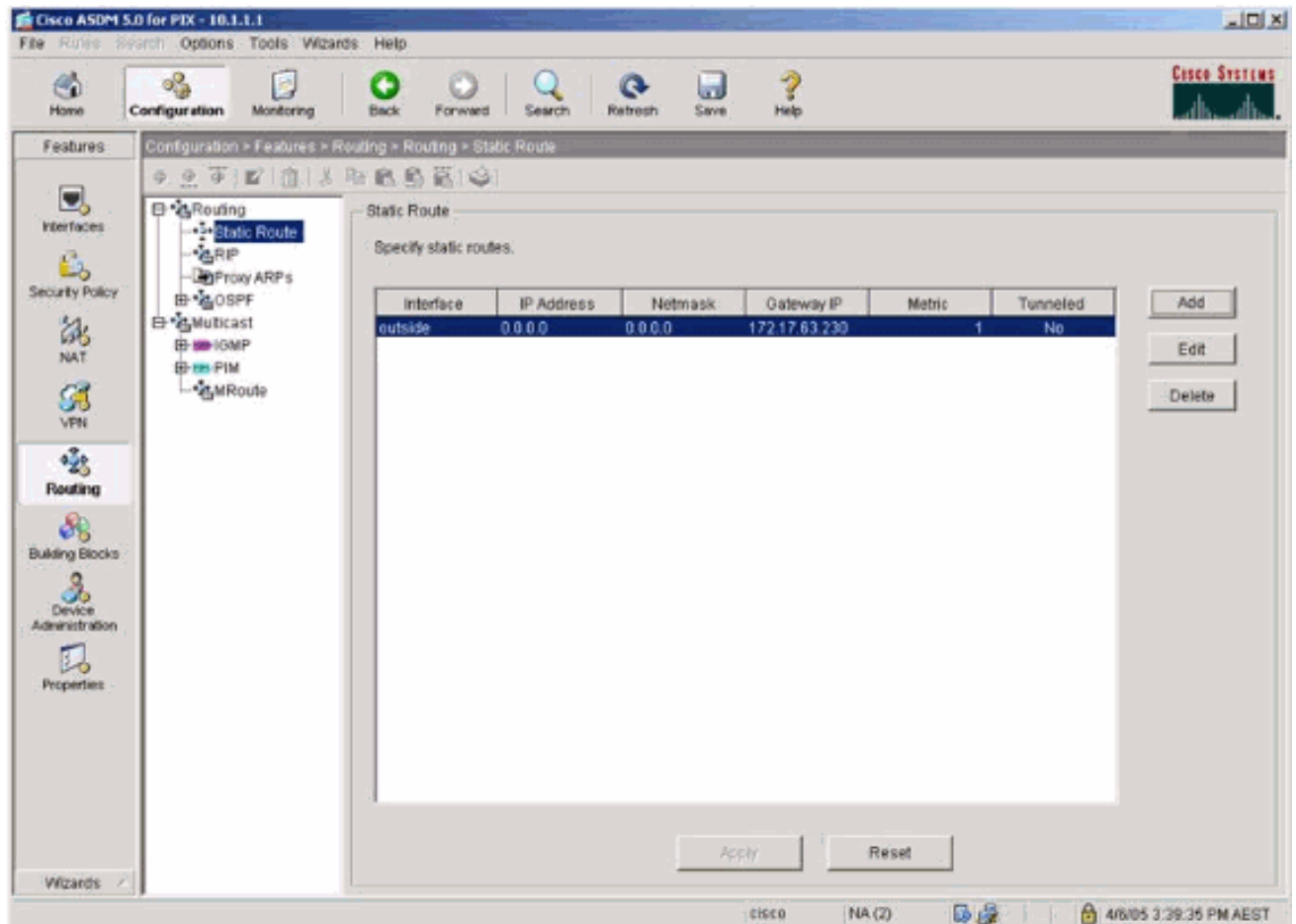
9. Selecteer VPN > IPsec > Tunnelbeleid en kies het tunnelbeleid.



10. Selecteer VPN > IPsec > **Selecteert** transformatiesets en kies een verzameling transformaties.



11. Selecteer **Routing > Routing > Statische route** en kies een statische route naar gateway-router. In dit voorbeeld, wijst de statische route naar de verre VPN peer voor eenvoudig.



Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het [Uitvoer Tolk](#) ([uitsluitend geregistreeerde](#) klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **toon crypto ipsec sa** - shows the fase 2 security associaties.
- **toon crypto isakmp sa** - toont de fase 1 veiligheidsassociaties.

Problemen oplossen

U kunt ASDM gebruiken om houtkap mogelijk te maken en om de logbestanden te bekijken.

- Selecteer **Configuration > Properties > Logging > Logging Setup**, kies **Vastlegging inschakelen** en klik op **Toepassen** om vastlegging mogelijk te maken.
- Selecteer **Monitoring > Vastlegging > Buffer > Op vastlegging niveau**, kies **Logging Buffer** en klik op **Weergeven** om de logbestanden te bekijken.

Opdrachten voor troubleshooting

Het [Uitvoer Tolk](#) ([uitsluitend geregistreeerde](#) klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg [Belangrijke informatie over debug Commands](#) voordat u **debug**-opdrachten gebruikt.

- **debug crypto ipsec** - toont de IPsec onderhandelingen van fase 2.
- **debug crypto isakmp** — toont de ISAKMP-onderhandelingen over fase 1.
- **debug crypto motor** - toont het verkeer dat wordt versleuteld.
- **duidelijke crypto isakmp** — ontslaat de veiligheidsassociaties met betrekking tot fase 1.
- **duidelijke crypto sa** — ontruimt de veiligheidsassociaties met betrekking tot fase 2.
- **bug-overtrekken**: toont aan of de verzoeken van ICMP van de hosts de PIX bereiken. U moet de opdracht **toeganglijst** toevoegen om ICMP in uw configuratie toe te staan om dit debug uit te voeren.
- **het foutoptreden van de houtbuffer** - toont verbindingen die worden gevestigd en ontkend aan hosts die door de PIX gaan. De informatie wordt opgeslagen in de PIX-logbuffer en u kunt de uitvoer zien met de opdracht **Logboek weergeven**.

Gerelateerde informatie

- [Meest gebruikelijke L2L- en IPSec VPN-oplossingen voor probleemoplossing](#)
- [Cisco PIX-firewallsoftware](#)
- [Opdrachtreferenties van Cisco Secure PIX-firewall](#)
- [Security meldingen uit het veld \(inclusief PIX\)](#)
- [Verzoeken om opmerkingen \(RFC's\)](#)