ASA/PIX: Dispositivo de seguridad a un ejemplo de configuración del router IOS túnel ipsec de LAN a LAN

Contenido

Introducción

Este documento demuestra cómo configurar un túnel IPsec de PIX Security Appliance 7.x y posterior o de Adaptive Security Appliance (ASA) con una red interna a un router 2611 que ejecuta una imagen de criptografía. Las rutas estáticas se utilizan para simplificar.

Refiera a configurar el router IPSec al PIX para más información sobre a configuración del túnel de LAN a LAN entre un router y el PIX.

Refiérase túnel ipsec de LAN a LAN entre el Cisco VPN 3000 Concentrator y el ejemplo de configuración del firewall PIX para más información sobre a configuración del túnel de LAN a LAN entre el firewall PIX y el Cisco VPN 3000 Concentrator.

Refiera al túnel IPsec entre PIX 7.x y ejemplo de configuración concentrador VPN 3000 para aprender más sobre el escenario donde está el túnel de LAN a LAN entre el PIX y el concentrador VPN.

Refiera al Spoke-a-cliente aumentado 7.x VPN del PIX/ASA con autenticación de TACACS+ el ejemplo de configuración para aprender más sobre el escenario donde el túnel de LAN a LAN entre el PIXes también permite para que un cliente VPN acceda el spoke PIX a través del eje de conexión PIX.

Refiera al SDM: IPSec sitio a sitio VPN en medio ASA/PIX y un ejemplo de configuración del router IOS para aprender un escenario más casi igual donde el dispositivo de seguridad del PIX/ASA funciona con la versión de software 8.x.

Refiera al profesional de la configuración: IPSec sitio a sitio el VPN en medio ASA/PIX y un ejemplo de configuración del router IOS para aprender un escenario más casi igual donde la configuración ASA-relacionada se muestra usando el ASDM GUI y la configuración Router-relacionada se muestra usando Cisco CP GUI.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- PIX-525 con la versión de software PIX 7.0
- Cisco 2611 Router con el Software Release 12.2(15)T13 de Cisco IOS®

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

En el PIX, los comandos access-list y nat 0 funcionan de manera conjunta. Cuando un usuario en la red de 10.1.1.0 va a la red de 10.2.2.0, la lista de acceso se utiliza para permitir que el tráfico de la red de 10.1.1.0 sea cifrado sin el Network Address Translation (NAT). En el router, utilizan a los **comandos route-map and access-list** de permitir que el tráfico de la red de 10.2.2.0 sea cifrado sin el NAT. Sin embargo, cuando van esos mismos usuarios en cualquier parte, los traducen al direccionamiento de 172.17.63.230 con el Port Address Translation (PAT).

Éstos son los comandos configuration requeridos en el dispositivo de seguridad PIX para que el tráfico no ejecutarse a través de la PALMADITA sobre el túnel, y tráfico a Internet a ejecutarse a través de la PALMADITA

```
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
```

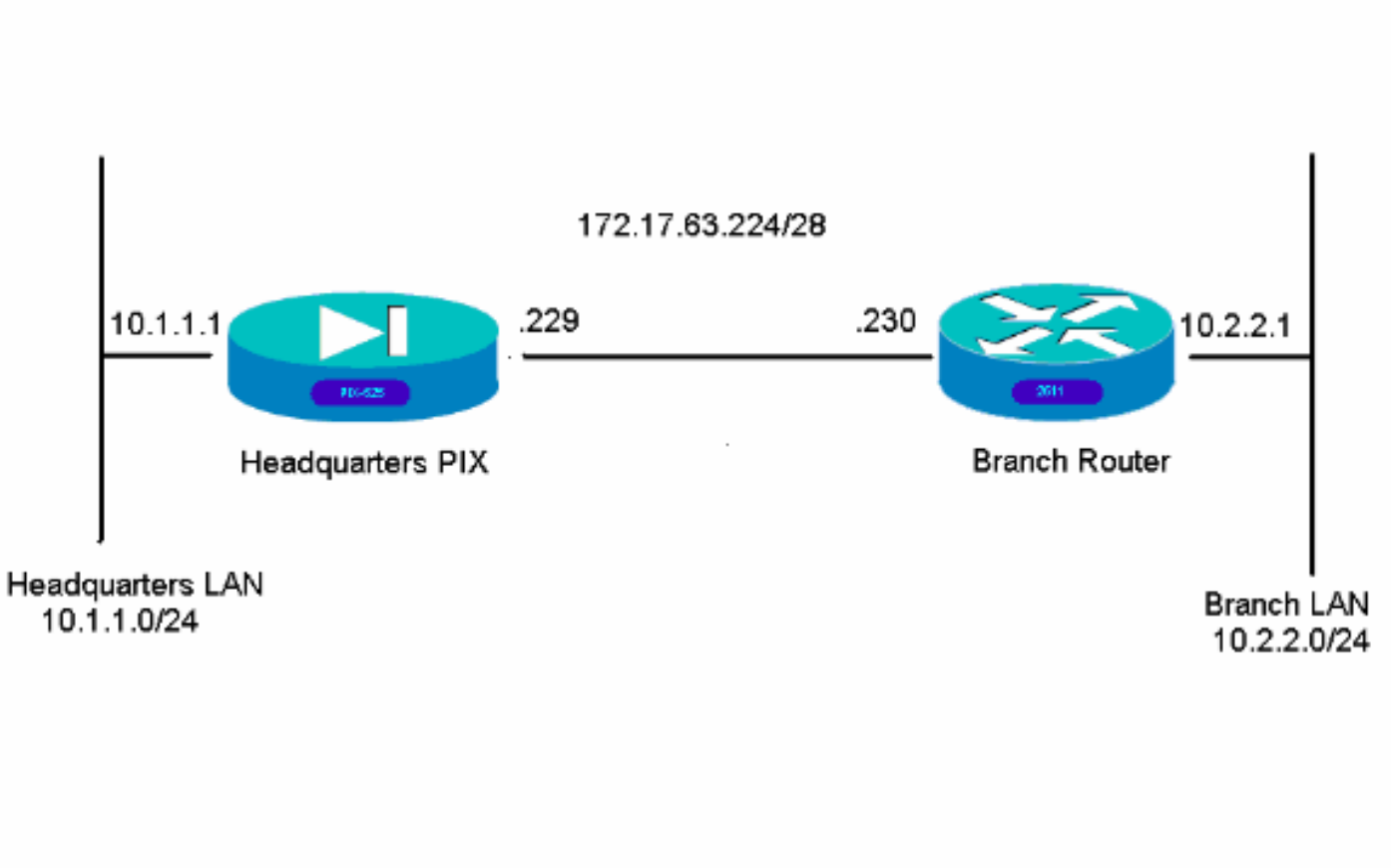
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

Estos ejemplos de configuración están para la interfaz de línea de comando. Vea la configuración usando la sección adaptante del Administrador de dispositivos de seguridad (ASDM) de este documento si usted prefiere configurar usando el ASDM.

- PIX principal
- Router de rama

PIX principal

```
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#
```

Router de rama

```
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
!
!
!
!
!
!
!
!
!
```

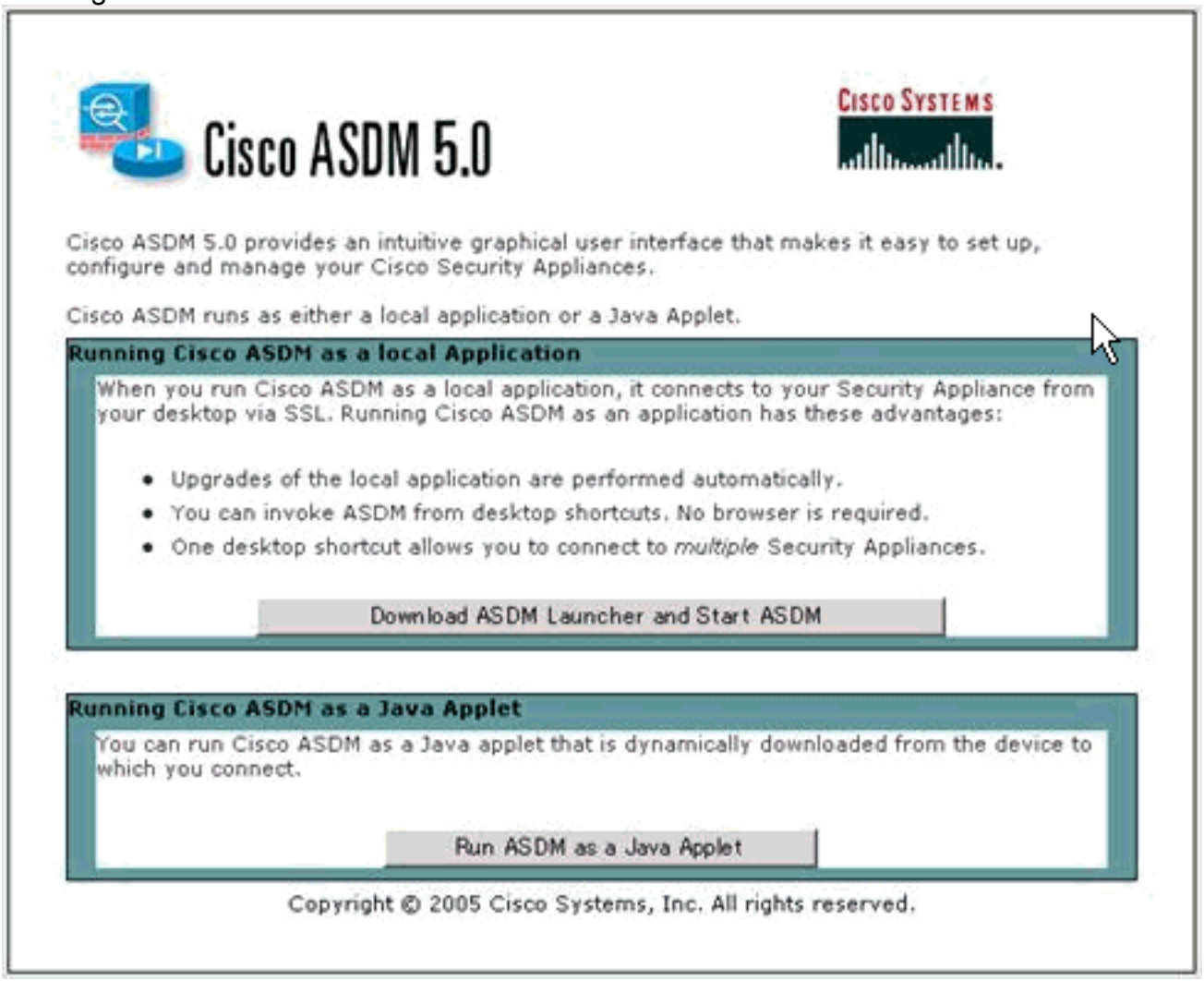
```
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
mta receive maximum-recipients 0
!
!
!
!
interface Ethernet0/0
ip address 172.17.63.230 255.255.255.240
ip nat outside
no ip route-cache
no ip mroute-cache
half-duplex
crypto map nolan
!
interface Ethernet0/1
ip address 10.2.2.1 255.255.255.0
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
```

Configuración usando el ASDM

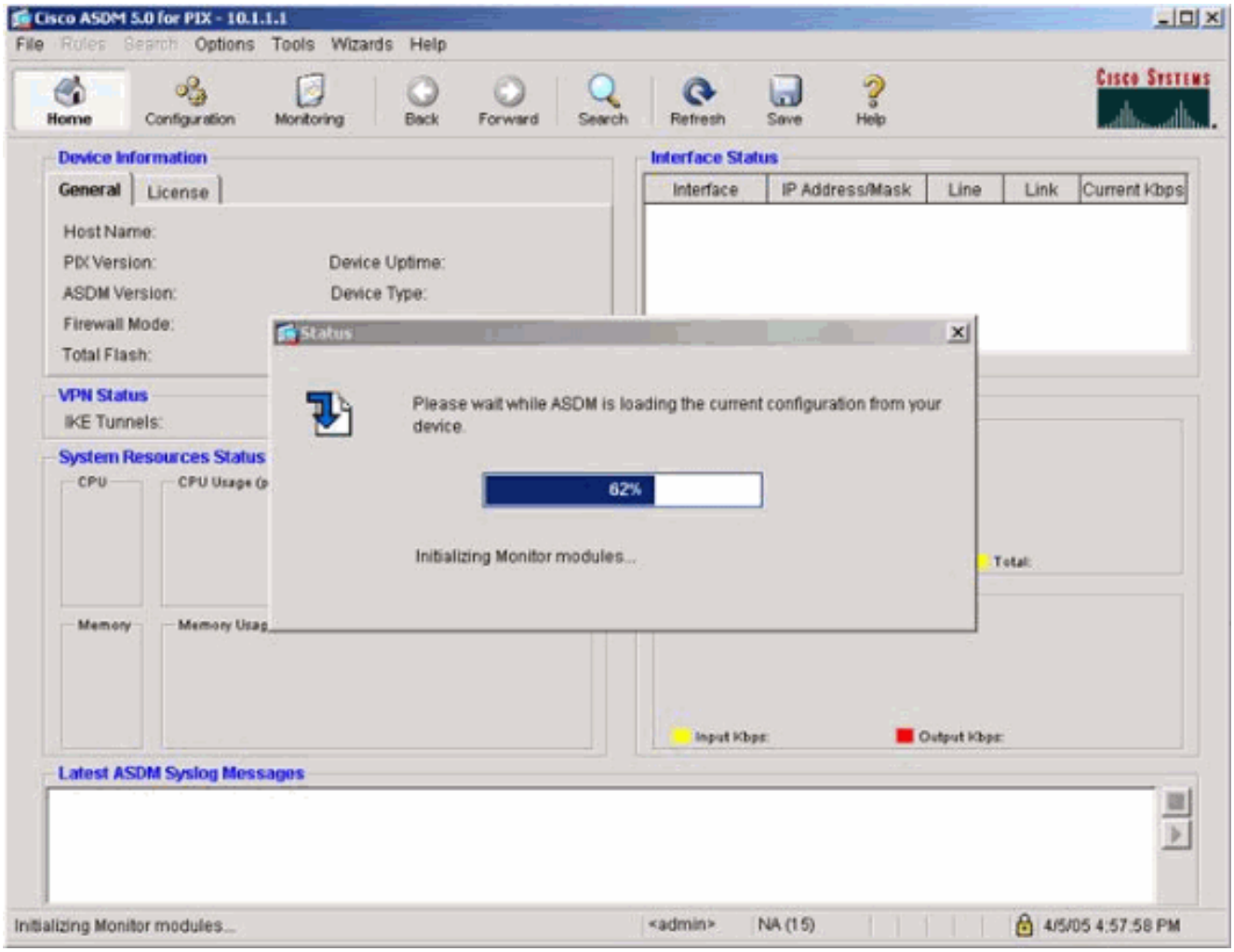
Este ejemplo demuestra cómo configurar el PIX usando el ASDM GUI. Un PC con un navegador y una dirección IP 10.1.1.2 está conectado con el e1 de la interfaz interior del PIX. Asegúrese que el HTTP esté habilitado en el PIX.

Este procedimiento ilustra la Configuración de ASDM de las jefaturas PIX.

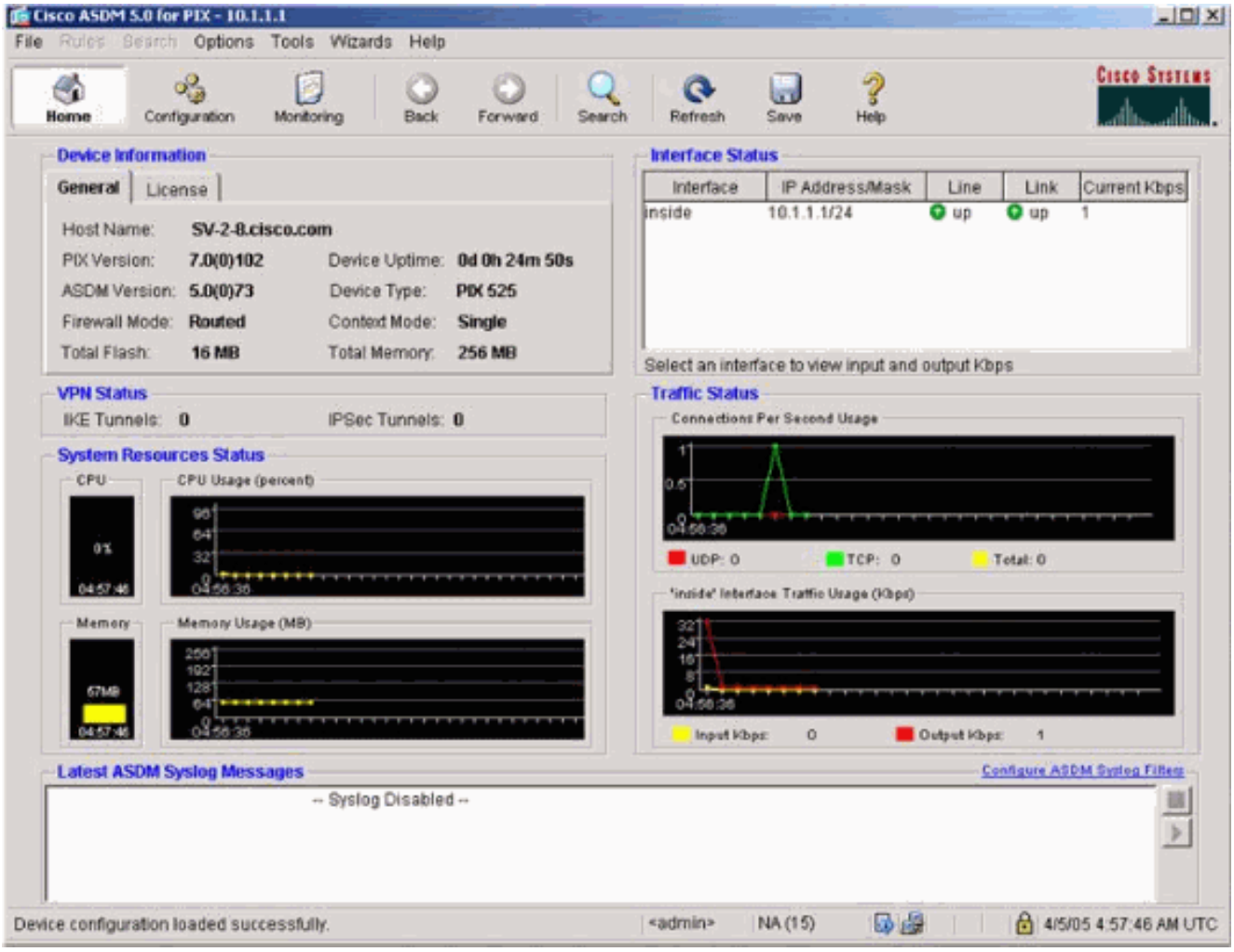
1. Conecte el PC con el PIX y elija un método de la descarga.



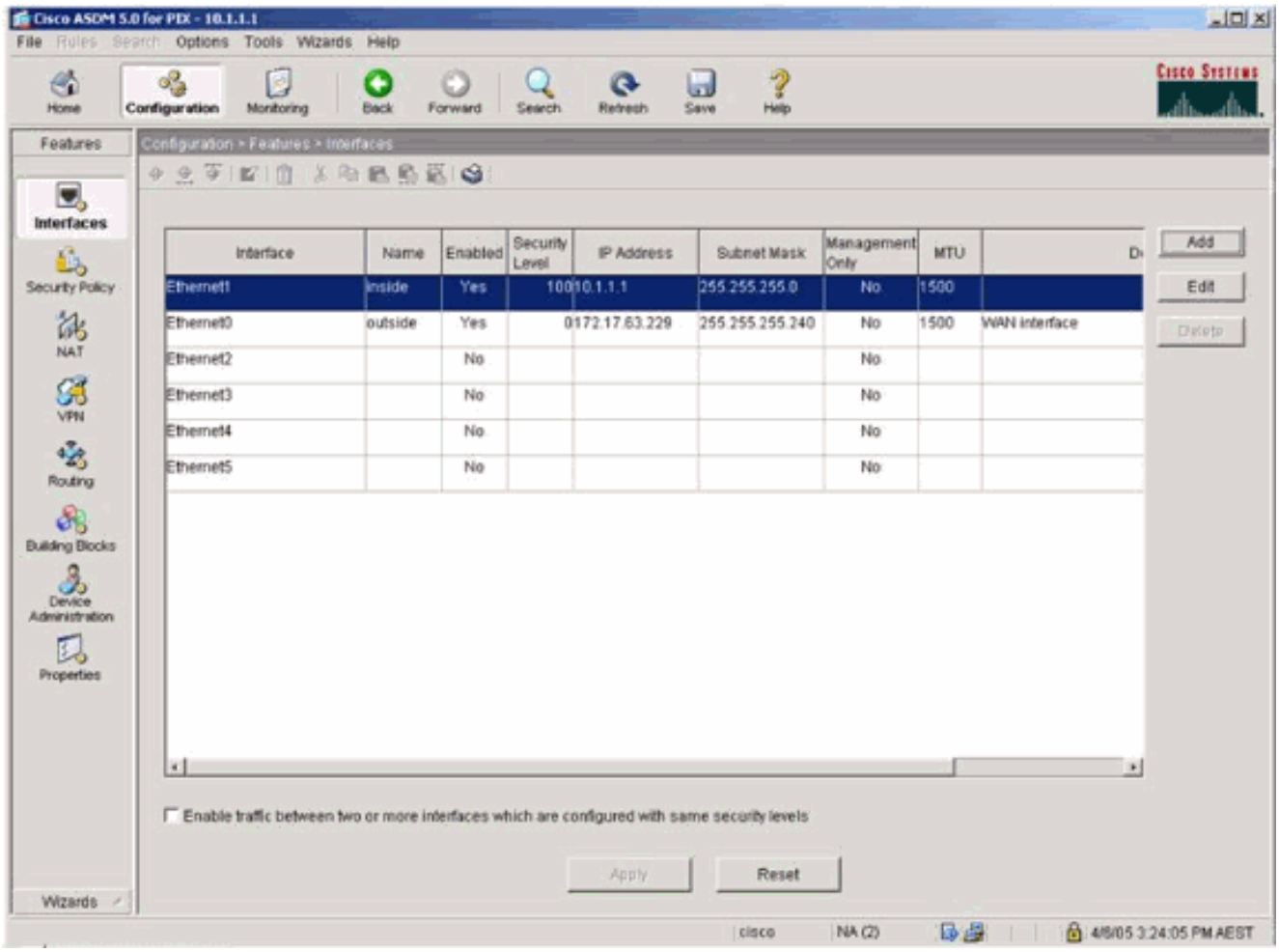
El ASDM carga la configuración existente del PIX.



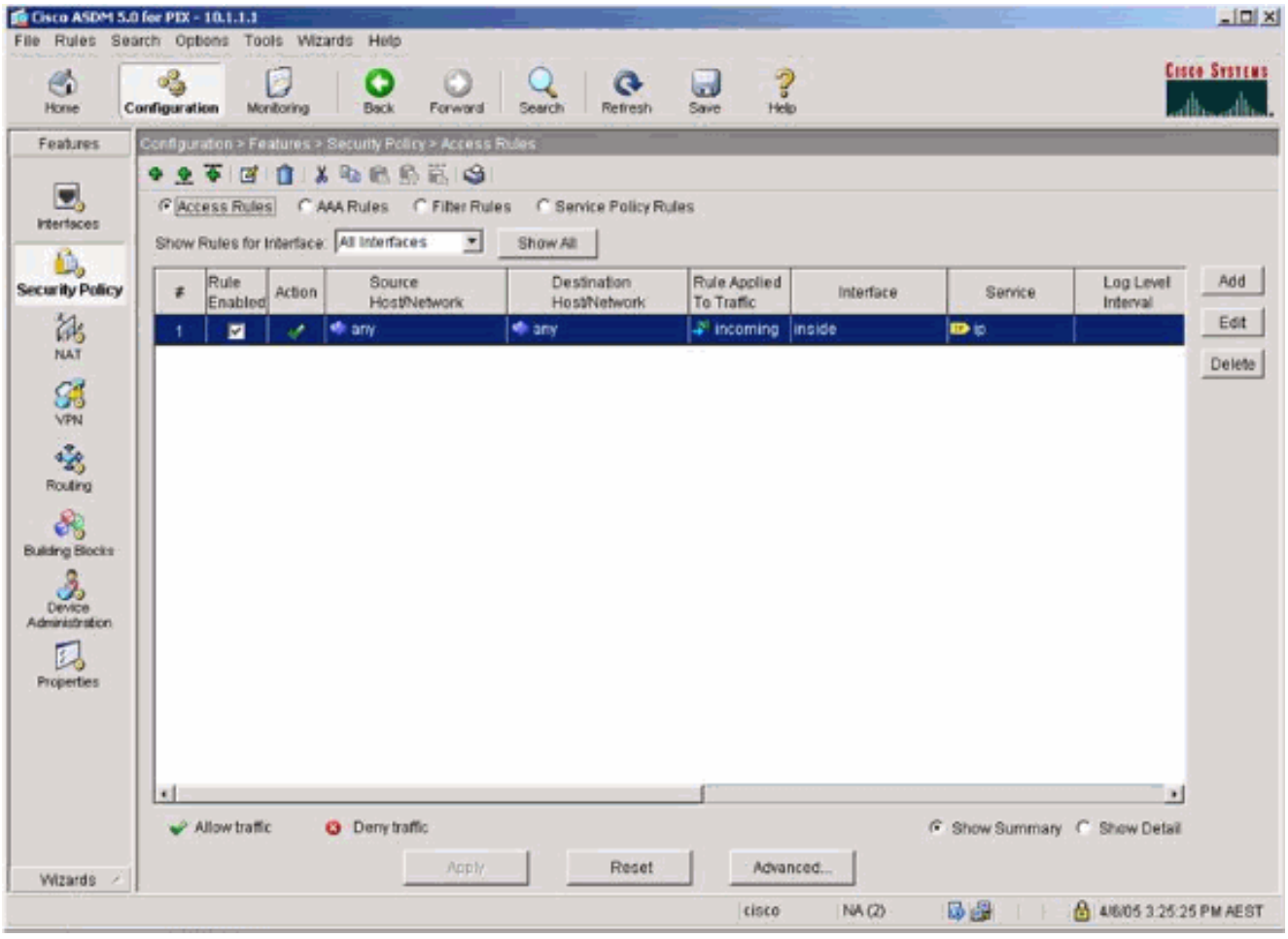
Esta ventana proporciona los instrumentos y los menús de la supervisión.



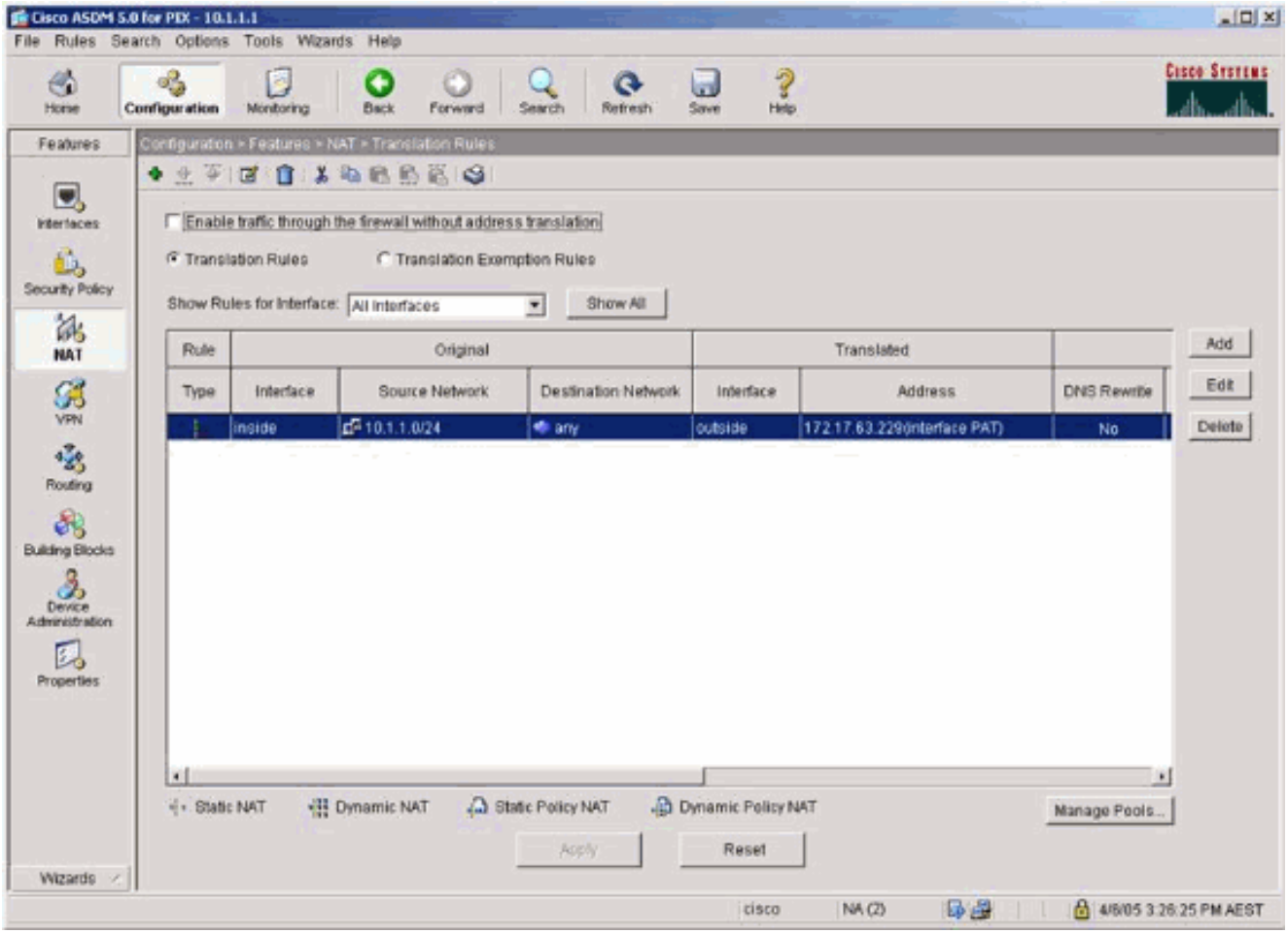
2. Seleccione la **configuración > las características > las interfaces** y selecto **agregue** para las nuevas interfaces o **edite** para una configuración existente.



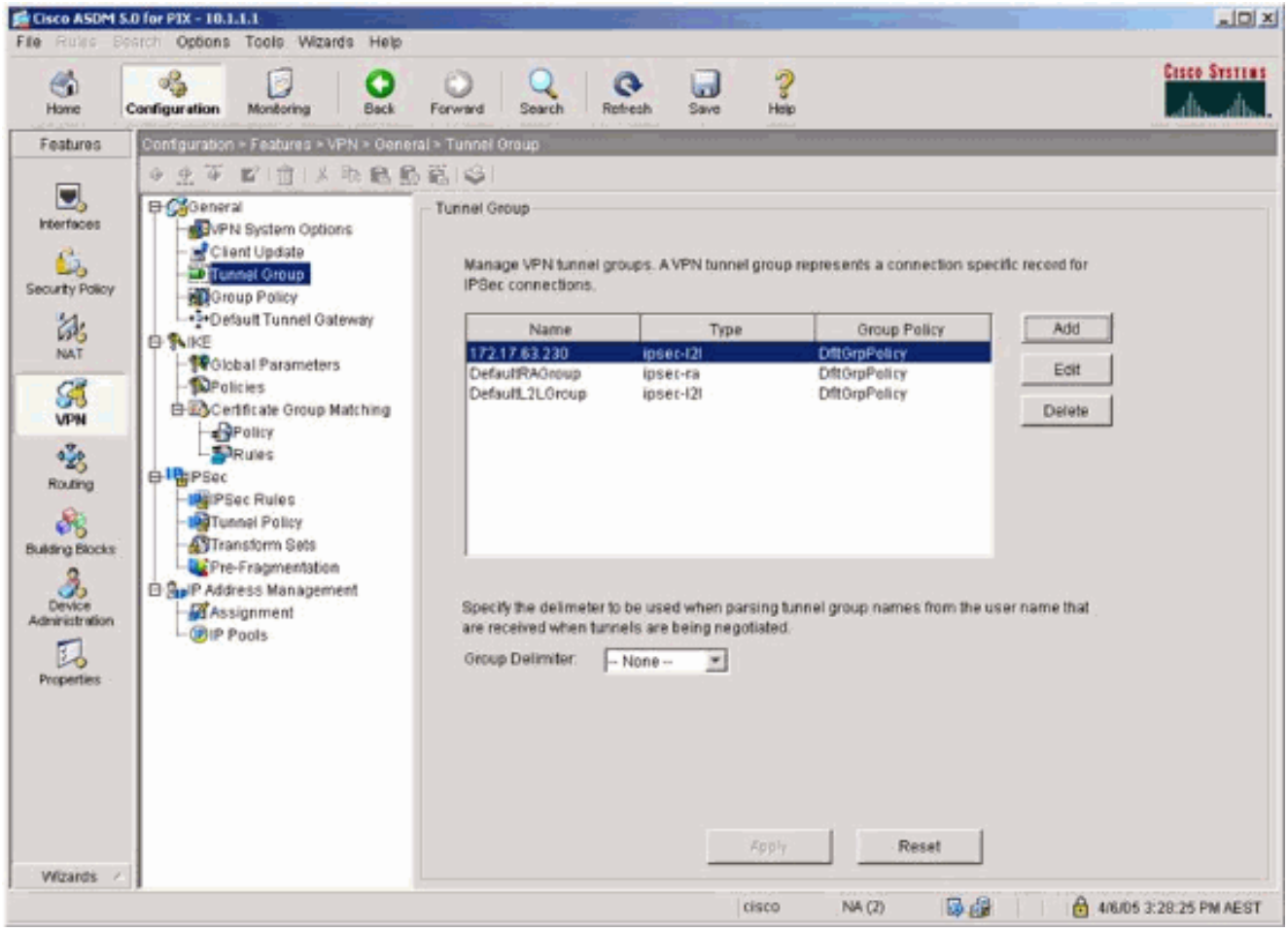
3. Seleccione las opciones de seguridad para la interfaz interior.



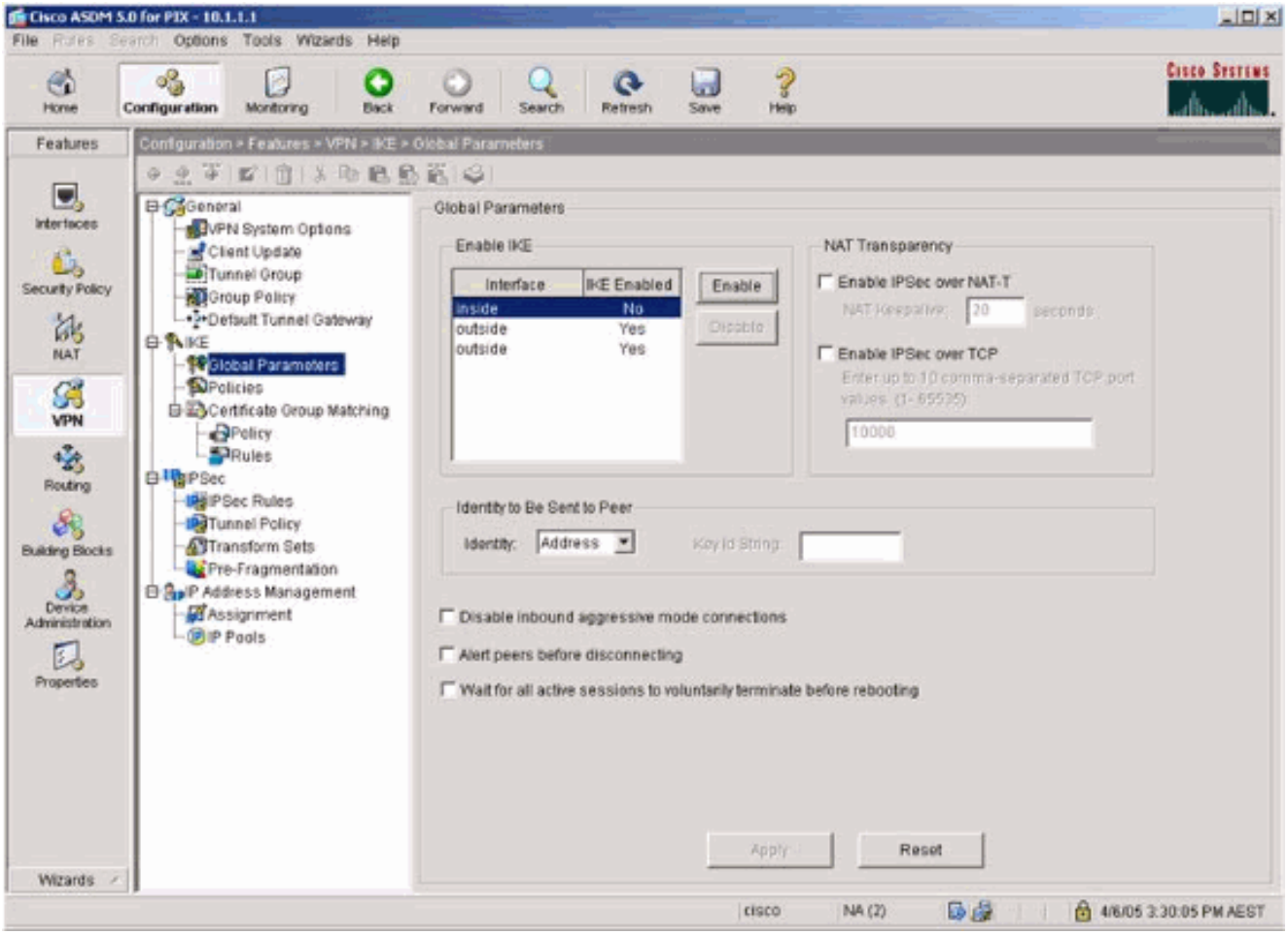
4. En la configuración del NAT, el tráfico encriptado está NAT-exento y el resto del tráfico es NAT/PAT a la interfaz
   exterior.



5. Seleccione el **VPN >General > grupo de túnel** y habilite a un grupo de
   túnel

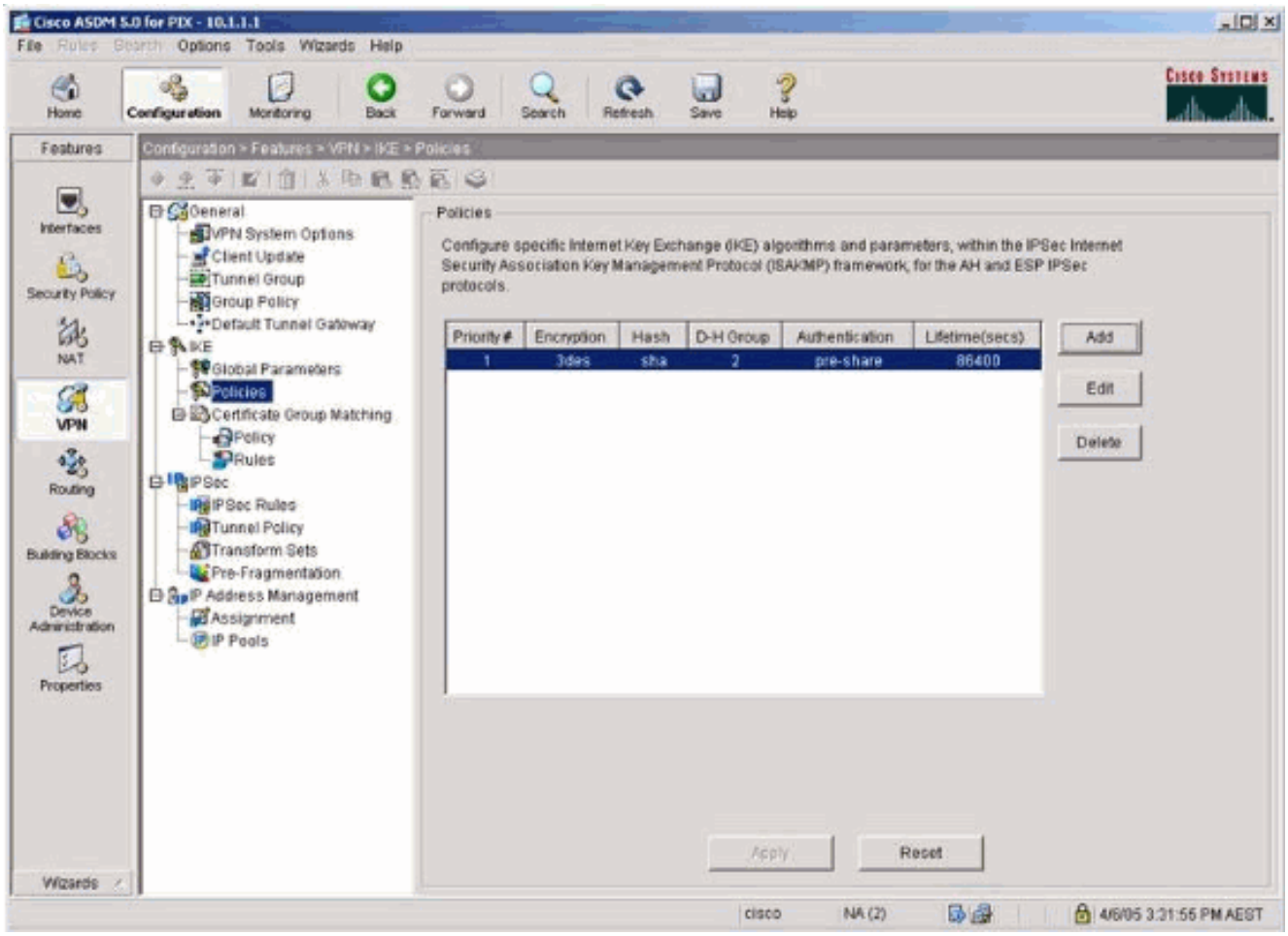


6. Seleccione **VPN > IKE > los Parámetros globales** y habilite el IKE en la interfaz exterior.

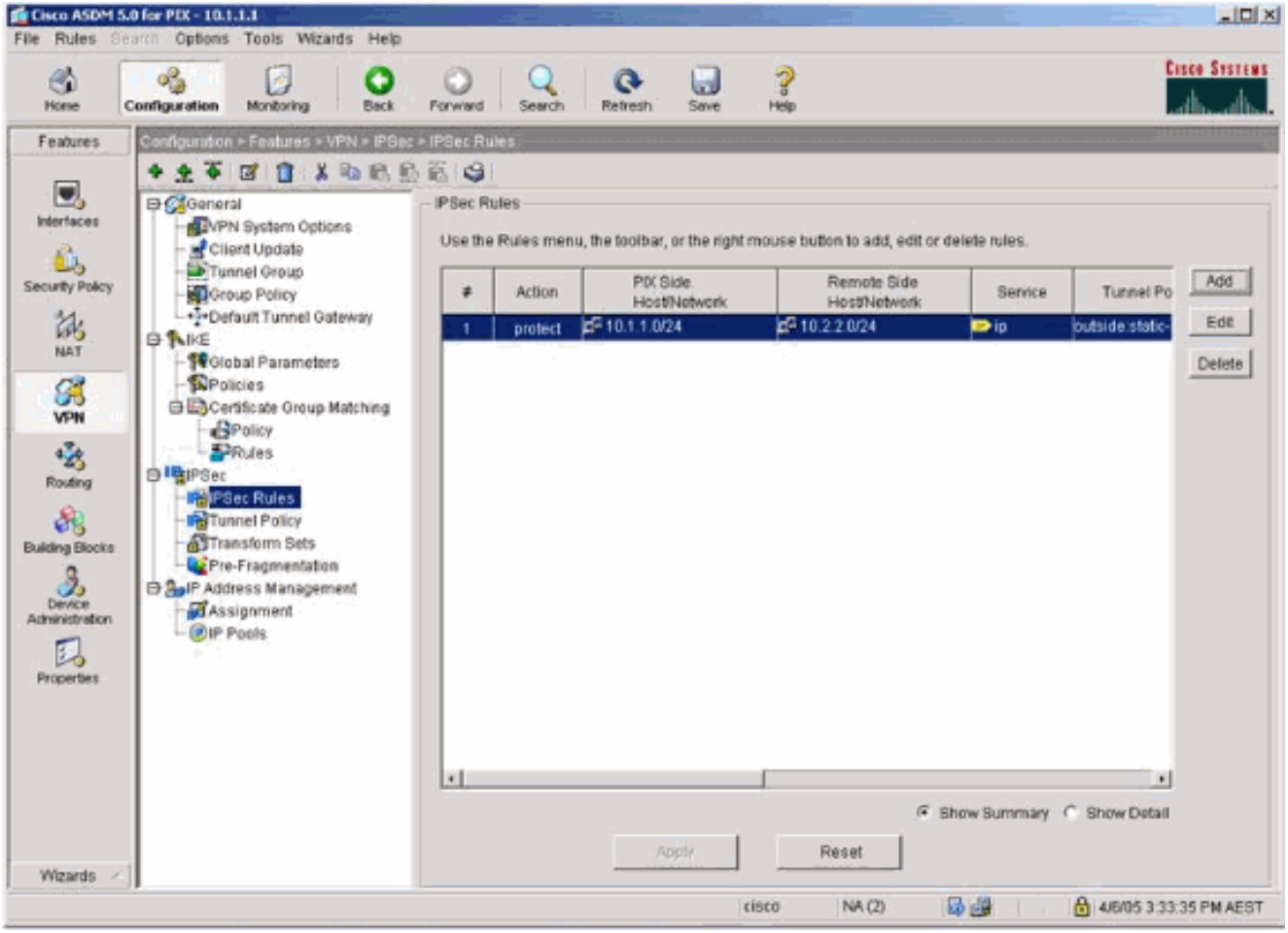


7. Seleccione **VPN > IKE > las directivas** y elija las políticas

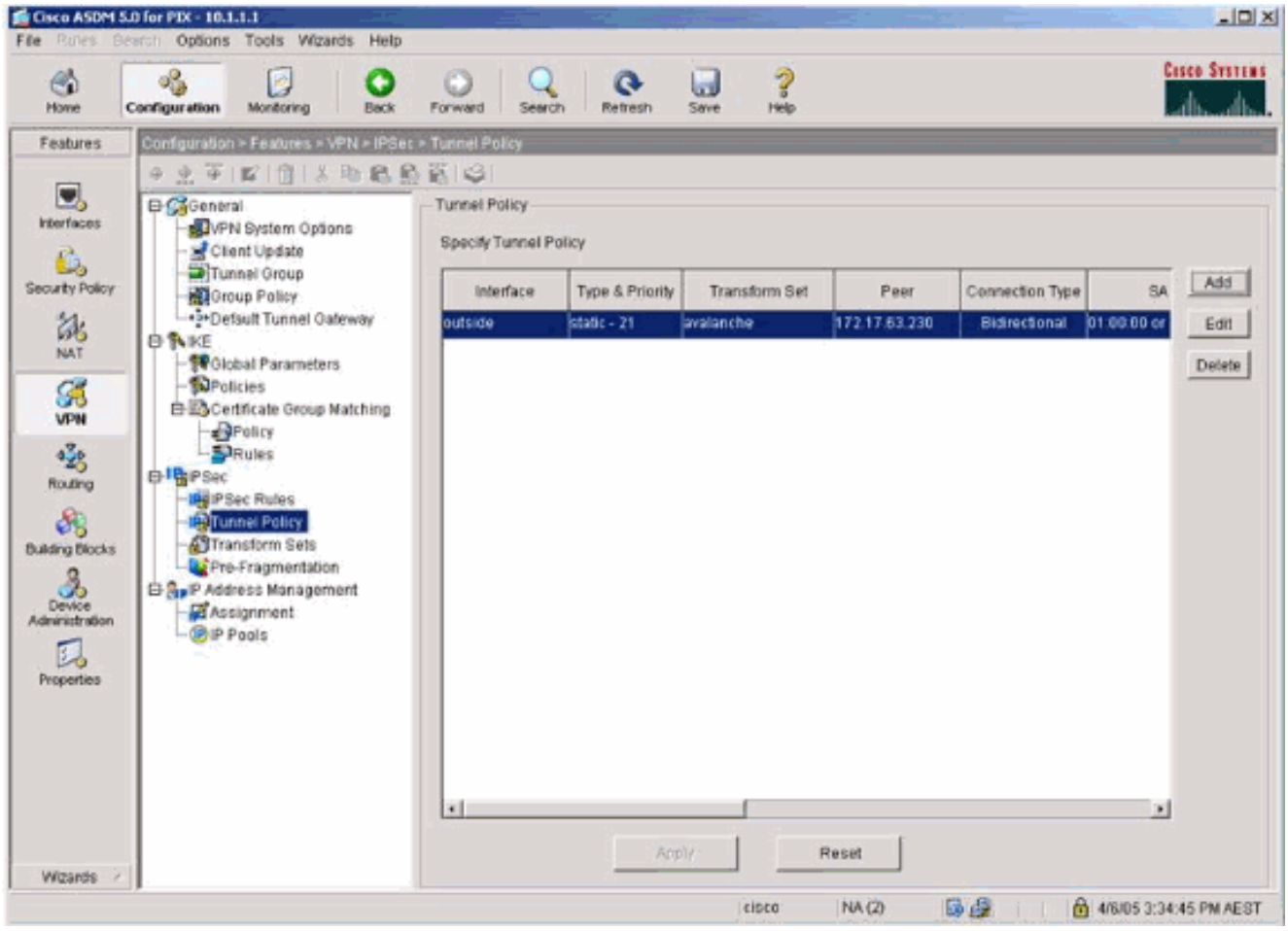
IKE.



8. Seleccione **VPN > IPSec > las reglas del IPSec** y elija el **IPSec** para el túnel local y la dirección
remota.

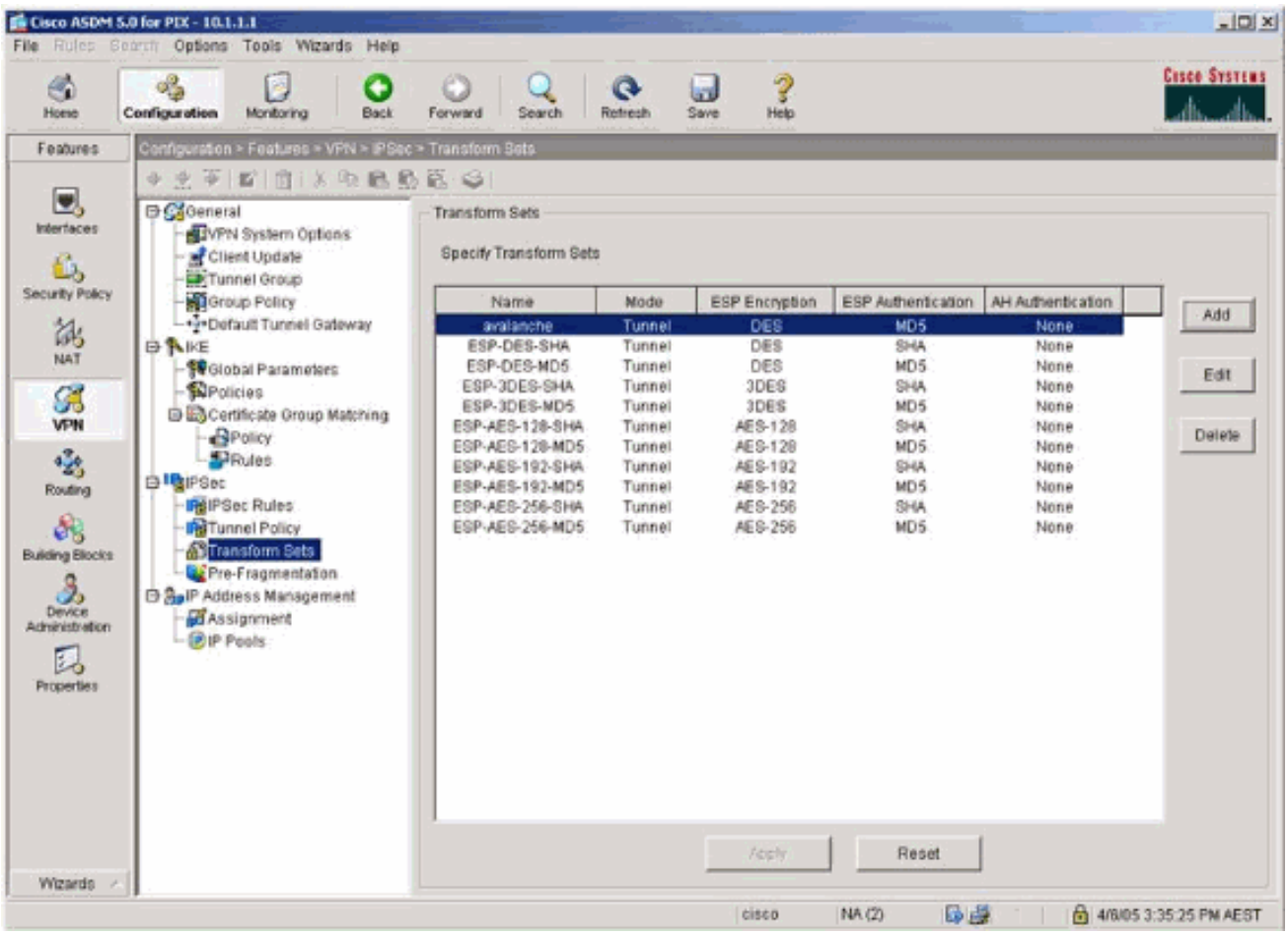


9. Seleccione **VPN > IPSec > directiva del túnel** y elija la directiva del túnel.

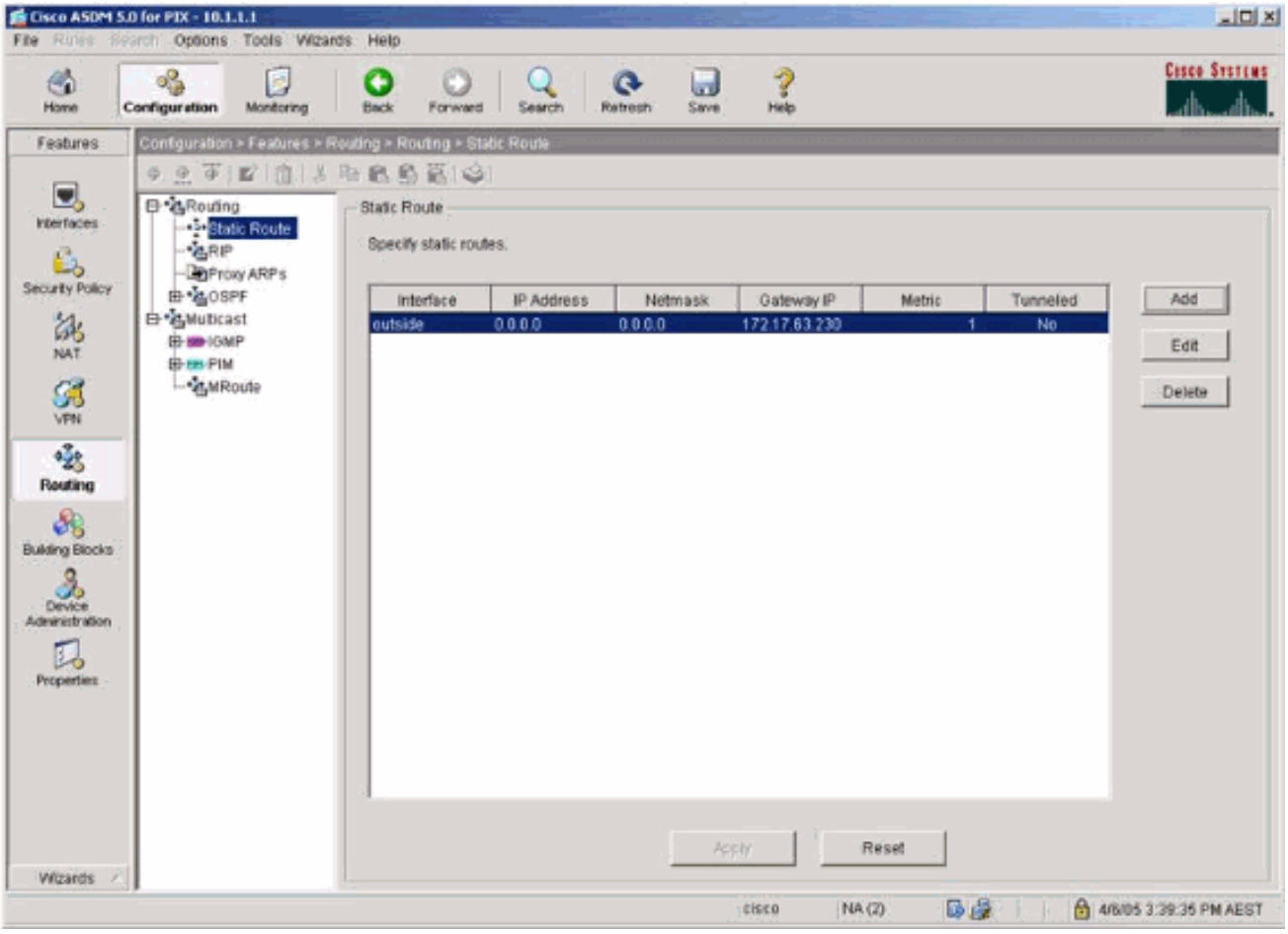


10. Selecto el **VPN > el IPSec > transforman los conjuntos** y eligen un conjunto de la

transformación.



11. Seleccione la **encaminamiento > la encaminamiento > la Static ruta** y elija una Static ruta al router de gateway. En este ejemplo, la Static ruta señala al peer de VPN remoto para simplicidad.



Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- show crypto ipsec sa - Muestra las asociaciones de seguridad de la fase 2.
- show crypto isakmp sa — Muestra las asociaciones de seguridad de la fase 1.

Troubleshooting

Usted puede utilizar el ASDM para habilitar el registro y para ver los registros.

- Seleccione la **configuración > las propiedades > el registro > la configuración del registro**, elija el **registro del permiso** y el tecleo **se aplica** para habilitar el registro.
- Seleccione la **supervisión > el registro > el búfer del registro > en el nivel de registro**, elija **memoria intermedia de registro**, y haga clic la **visión** para ver los registros.

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **IPSec del debug crypto** — Muestra los IPSec Negotiations de la fase 2.
- debug crypto isakmp — muestra las negociaciones ISAKMP para la fase 1.
- debug crypto engine — muestra el tráfico codificado.
- clear crypto isakmp â€" Borra las asociaciones de seguridad relacionadas con la fase 1.
- **borre el sa crypto** — Borra las asociaciones de seguridad relacionadas con la fase 2.
- debug icmp trace – Muestra si las solicitudes ICMP desde los hosts alcanzan al PIX. Usted necesita agregar el **comando access-list** de permitir el ICMP en su configuración para ejecutar este debug.
- logging buffer debugging—Muestra las conexiones que se establecen y las que se deniegan a los hosts que atraviesan el PIX. La información se salva en el búfer del registro PIX y usted puede ver la salida con el **comando show log**.

Información Relacionada

- Soluciones a los Problemas más frecuentes de IPSec VPN L2L y de Acceso Remoto
- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)