ASA/PIX: Ferramenta de segurança a um exemplo de configuração do túnel IPSec de LAN para LAN do IOS Router

Índice

Introdução

Este documento demonstra como configurar um túnel de IPsec da um PIX Security Appliance 7.x ou posterior ou um Adaptive Security Appliance (ASA) com uma única rede interna para o roteador 2611 que executa a imagem crypto. As rotas estáticas são usadas por simplicidade.

Refira configurar o roteador de IPSec ao PIX para obter mais informações sobre de uma configuração de túnel de Rede-para-Rede entre um roteador e o PIX.

Refira o túnel IPSec de LAN para LAN entre o Cisco VPN 3000 Concentrator e o exemplo de configuração do PIX Firewall para obter mais informações sobre de uma configuração de túnel de Rede-para-Rede entre o PIX Firewall e o Cisco VPN 3000 Concentrator.

Refira o túnel de IPsec entre PIX 7.x e exemplo de configuração do VPN 3000 concentrator a fim aprender mais sobre a encenação onde o túnel de LAN para LAN está entre o PIX e o concentrador VPN.

Refira o Spoke-à-cliente aumentado 7.x VPN PIX/ASA com exemplo de configuração da autenticação TACACS+ a fim aprender mais sobre a encenação onde o túnel de LAN para LAN entre as PIXes igualmente permite um cliente VPN alcançar o spoke PIX com o PIX de hub.

Refira o SDM: IPSec local a local VPN entre ASA/PIX e um exemplo de configuração do IOS

Router a fim aprender a encenação mais mais ou menos idêntica onde a ferramenta de segurança PIX/ASA executa a versão de software 8.x.

Refira o profissional da configuração: O IPSec local a local VPN entre ASA/PIX e um exemplo de configuração do IOS Router a fim aprender uma encenação mais mais ou menos idêntica onde a configuração ASA-relacionada seja mostrada usando ASDM GUI e a configuração Roteador-relacionada é mostrado usando Cisco CP GUI.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- PIX-525 com versão de software de PIX 7.0
- Cisco 2611 Router com Software Release 12.2(15)T13 de Cisco IOS®

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

No PIX, os comandos access-list e nat 0 trabalham juntos. Quando um usuário na rede de 10.1.1.0 vai à rede de 10.2.2.0, a lista de acessos está usada para permitir o tráfego de rede de 10.1.1.0 ser cifrado sem Network Address Translation (NAT). No roteador, os **comandos route-map and access-list** são usados permitir o tráfego de rede de 10.2.2.0 ser cifrado sem NAT. Contudo, quando aqueles mesmos usuários vão em qualquer outro lugar, são traduzidos ao endereço de 172.17.63.230 através da tradução de endereço de porta (PAT).

Estes são os comandos configuration exigidos na ferramenta de segurança PIX para que o tráfego não ser executado através da PANCADINHA sobre o túnel, e tráfego ao Internet a ser executado através da PANCADINHA

```
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

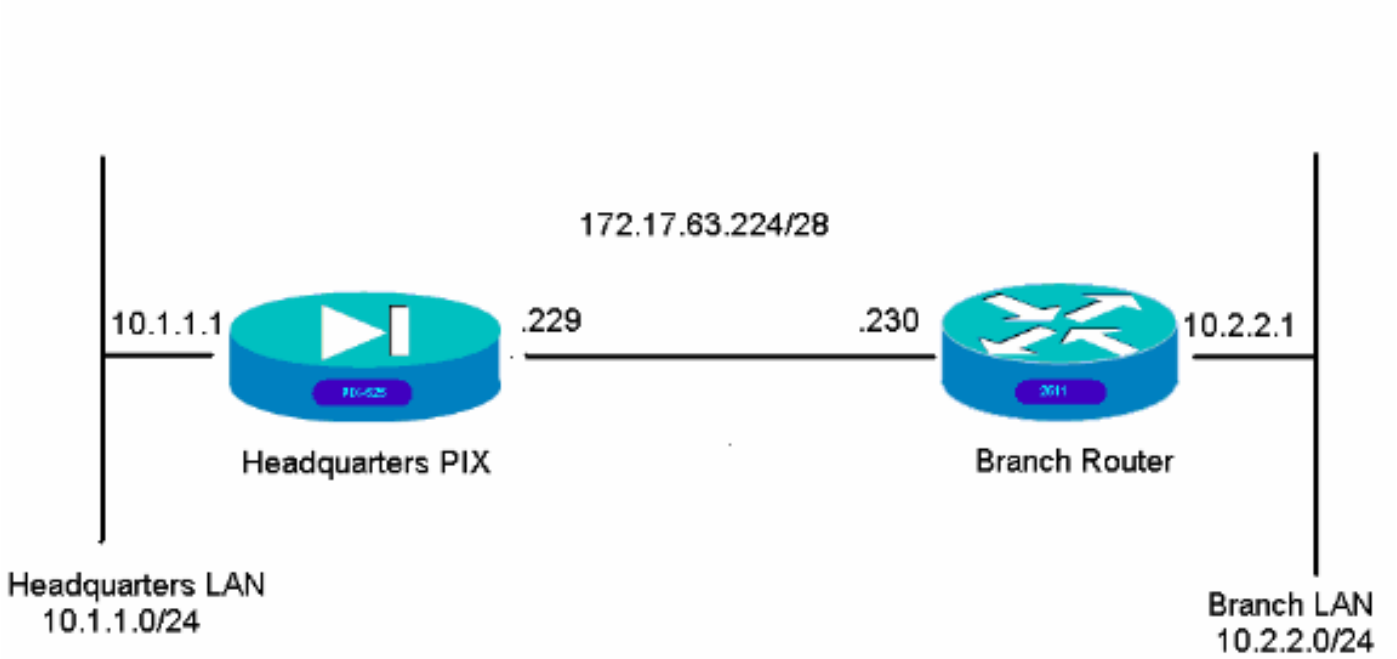
Nesta seção, você encontrará informações para configurar os recursos descritos neste

documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Estes exemplos de configuração são para a interface da linha de comando. Veja a configuração usando a seção adaptável do Security Device Manager (ASDM) deste documento se você prefere configurar usando o ASDM.

- PIX da matriz
- Roteador de filial

PIX da matriz

```
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#
```

Roteador de filial

```
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
```

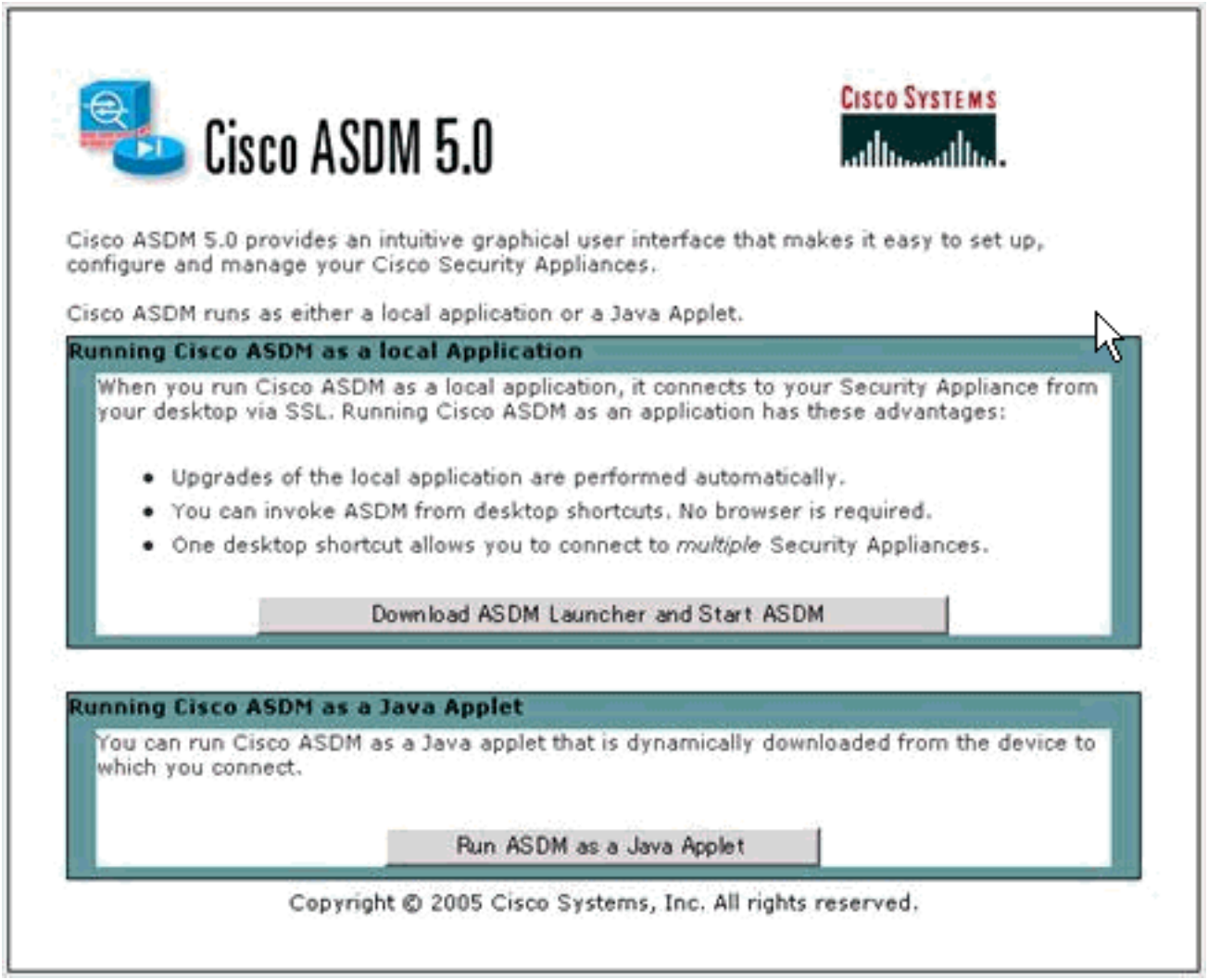
```
transform-set sharks esp-des esp-md5-hmac ! crypto map
nolan 11 ipsec-isakmp set peer 172.17.63.229 set
transform-set sharks match address 120 ! ! ! ! ! ! ! ! !
! no voice hpi capture buffer no voice hpi capture
destination ! ! mta receive maximum-recipients 0 ! ! ! !
interface Ethernet0/0 ip address 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
```

Configuração usando o ASDM

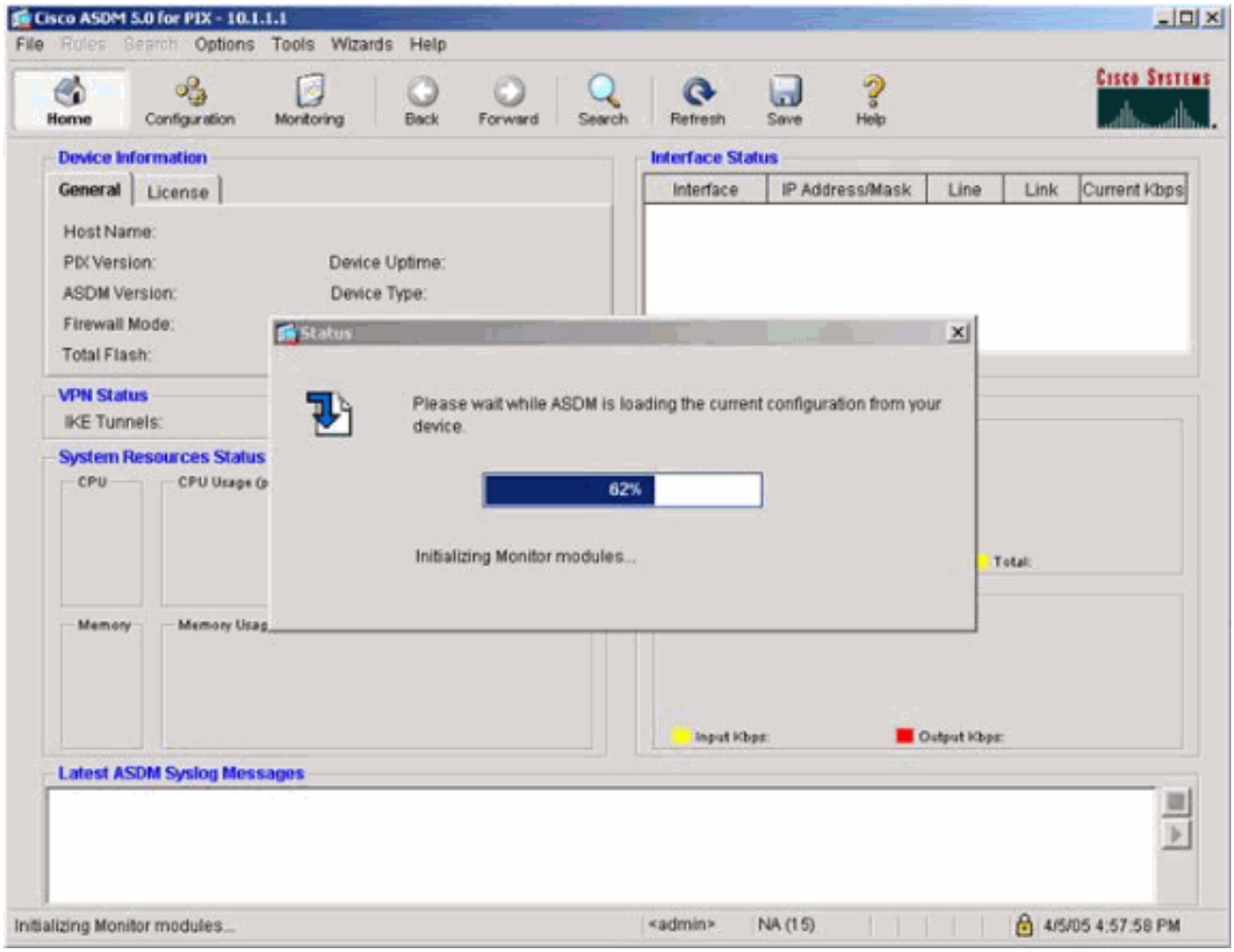
Este exemplo demonstra como configurar o PIX usando o ASDM GUI. Um PC com um navegador e um endereço IP 10.1.1.2 é conectado ao E1 da interface interna do PIX. Assegure-se de que o HTTP esteja permitido no PIX.

Este procedimento ilustra a configuração ASDM das matrizes PIX.

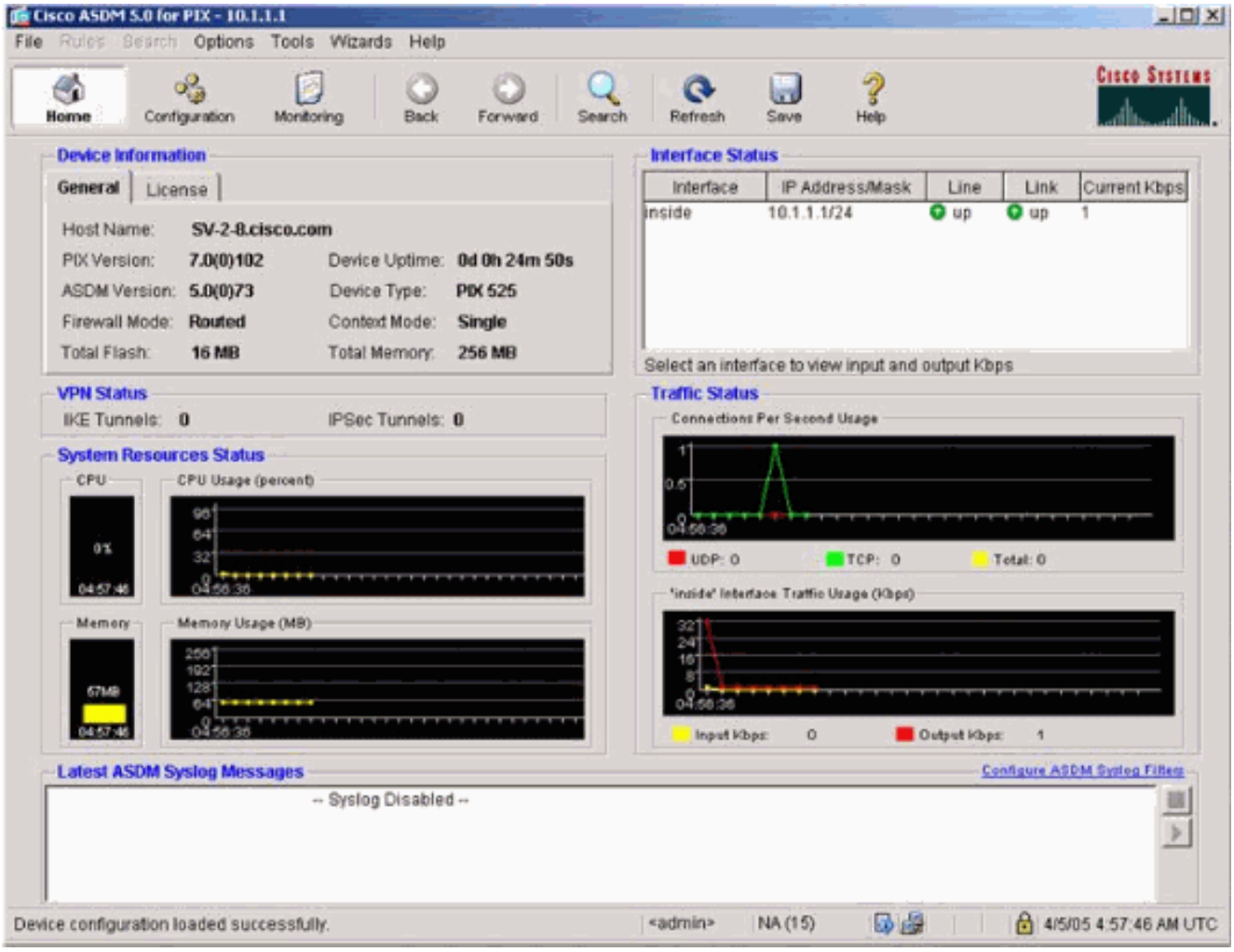
1. Conecte o PC ao PIX e escolha um método da transferência.



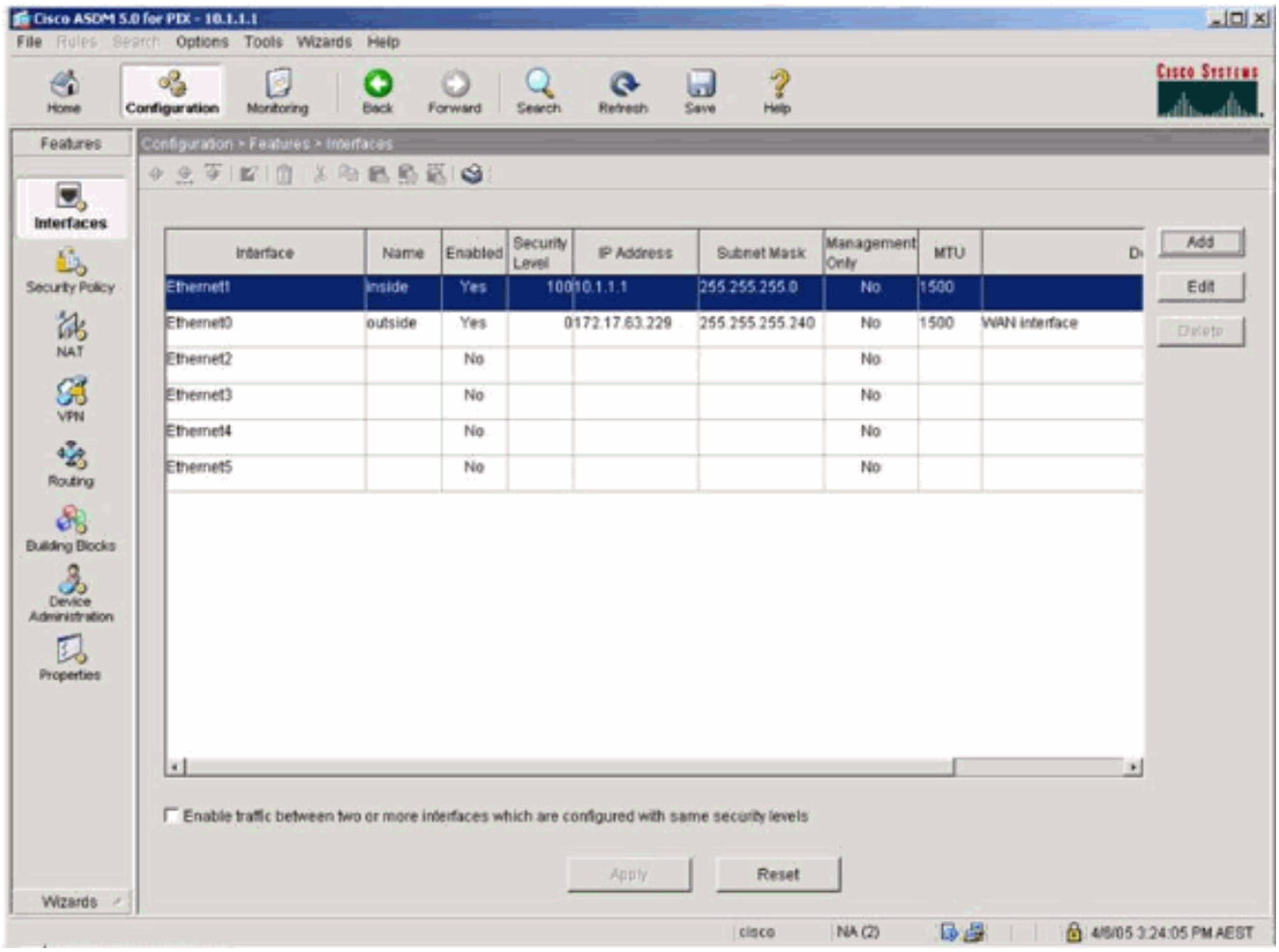
O ASDM carrega a configuração existente do PIX.



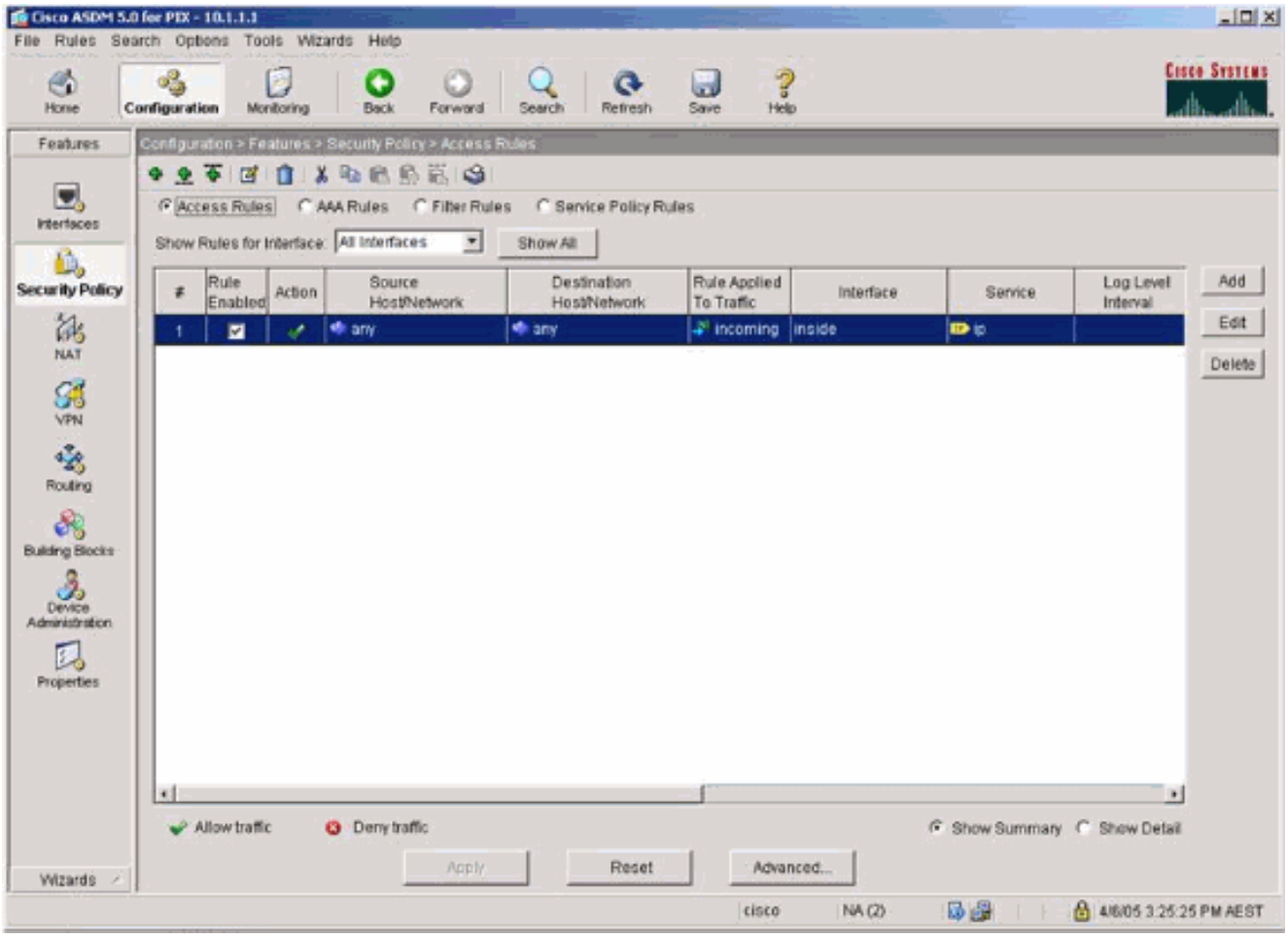
Este indicador fornece instrumentos e menus da monitoração.



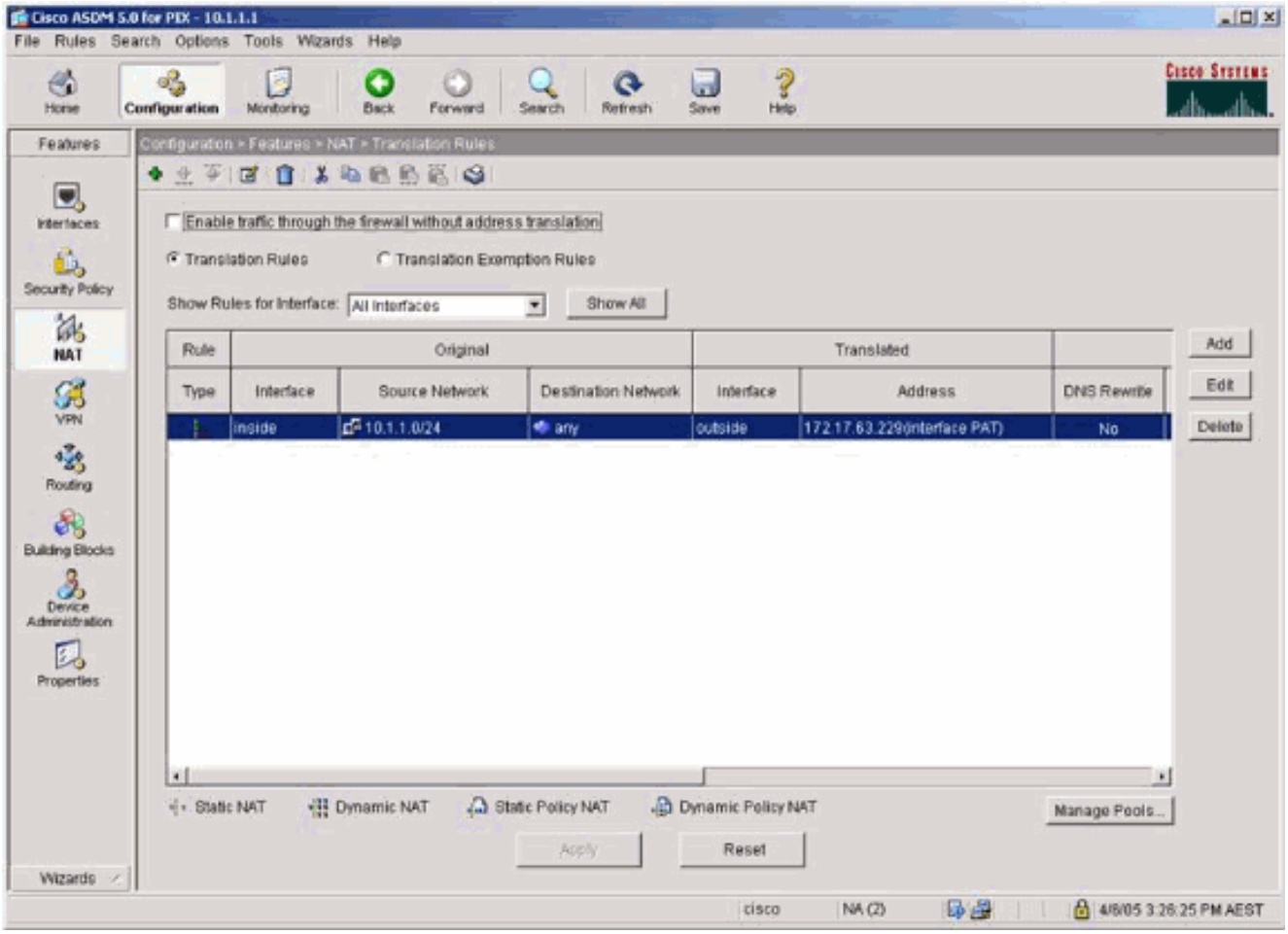
2. Selecione a **configuração > as características > as relações** e seleto **adicionar** para relações novas ou **edite** para uma configuração existente.



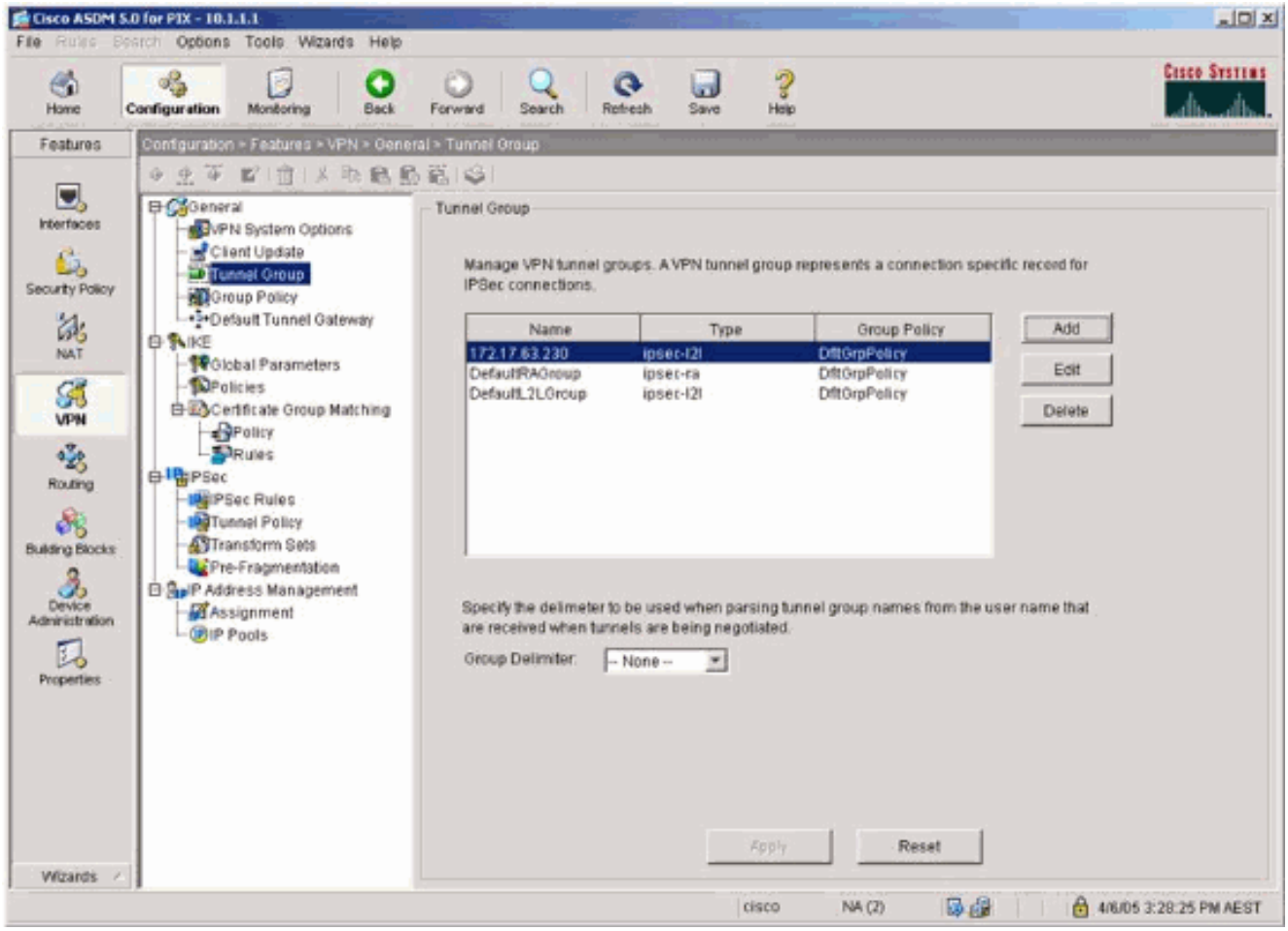
3. Selecione as opções de segurança para a interface interna.



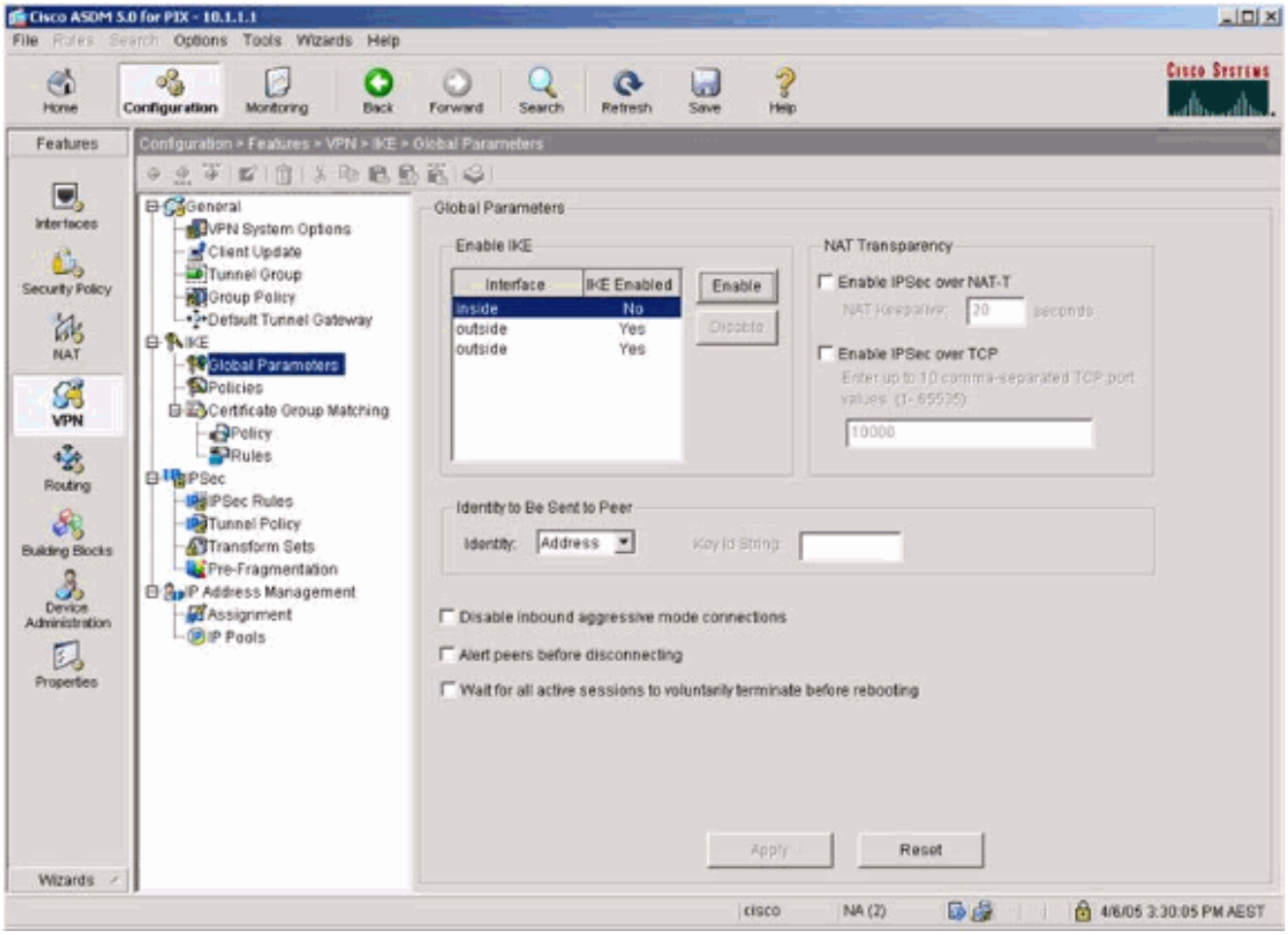
4. Na configuração de NAT, o tráfego criptografado é NAT-isento e todo tráfego restante é NAT/PAT à interface
   externa.



5. Selecione o **VPN >General > grupo de túneis** e permita um grupo de
   túneis

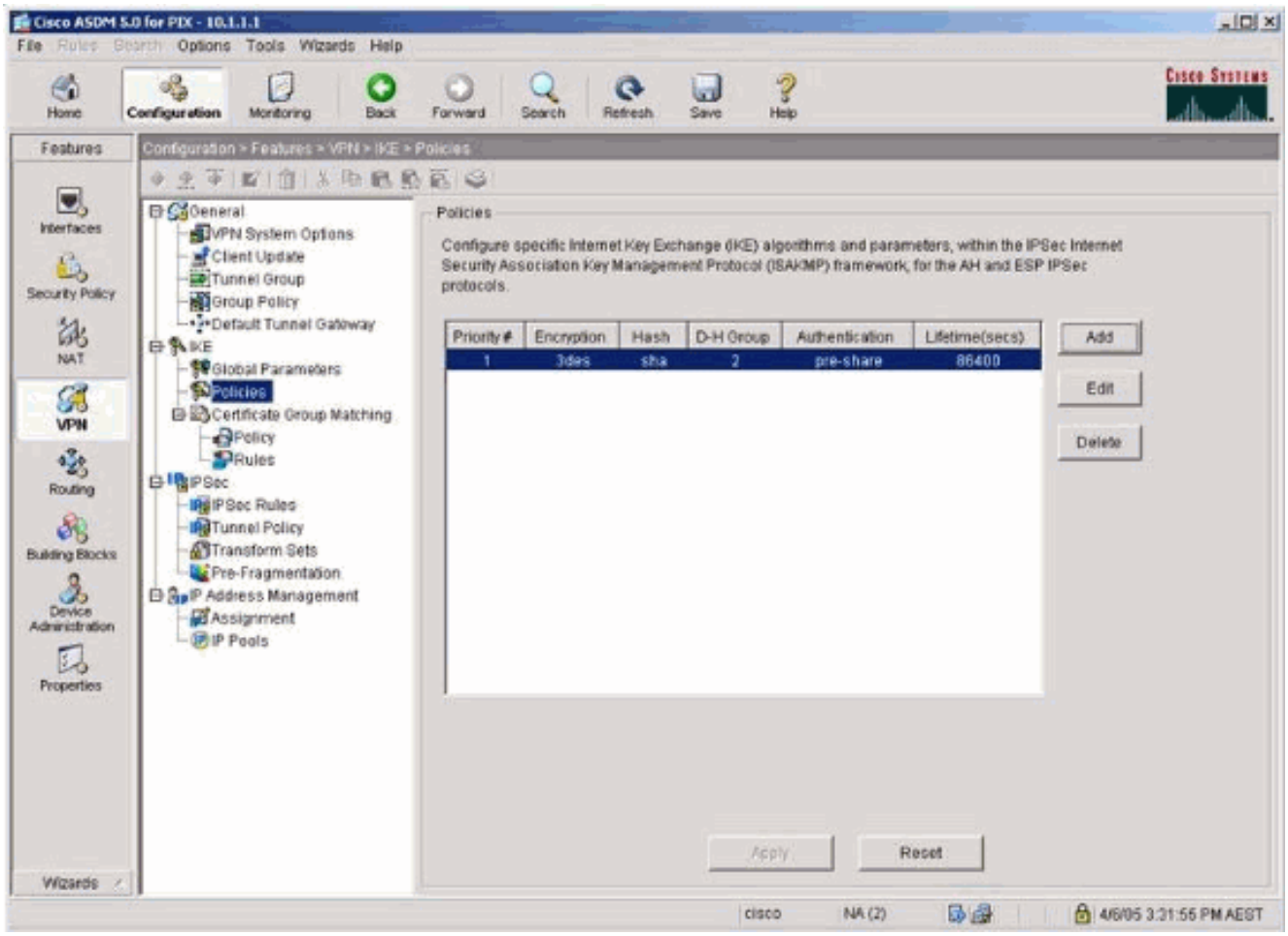


6. Selecione **VPN > IKE > parâmetros globais** e permita o IKE na interface externa.

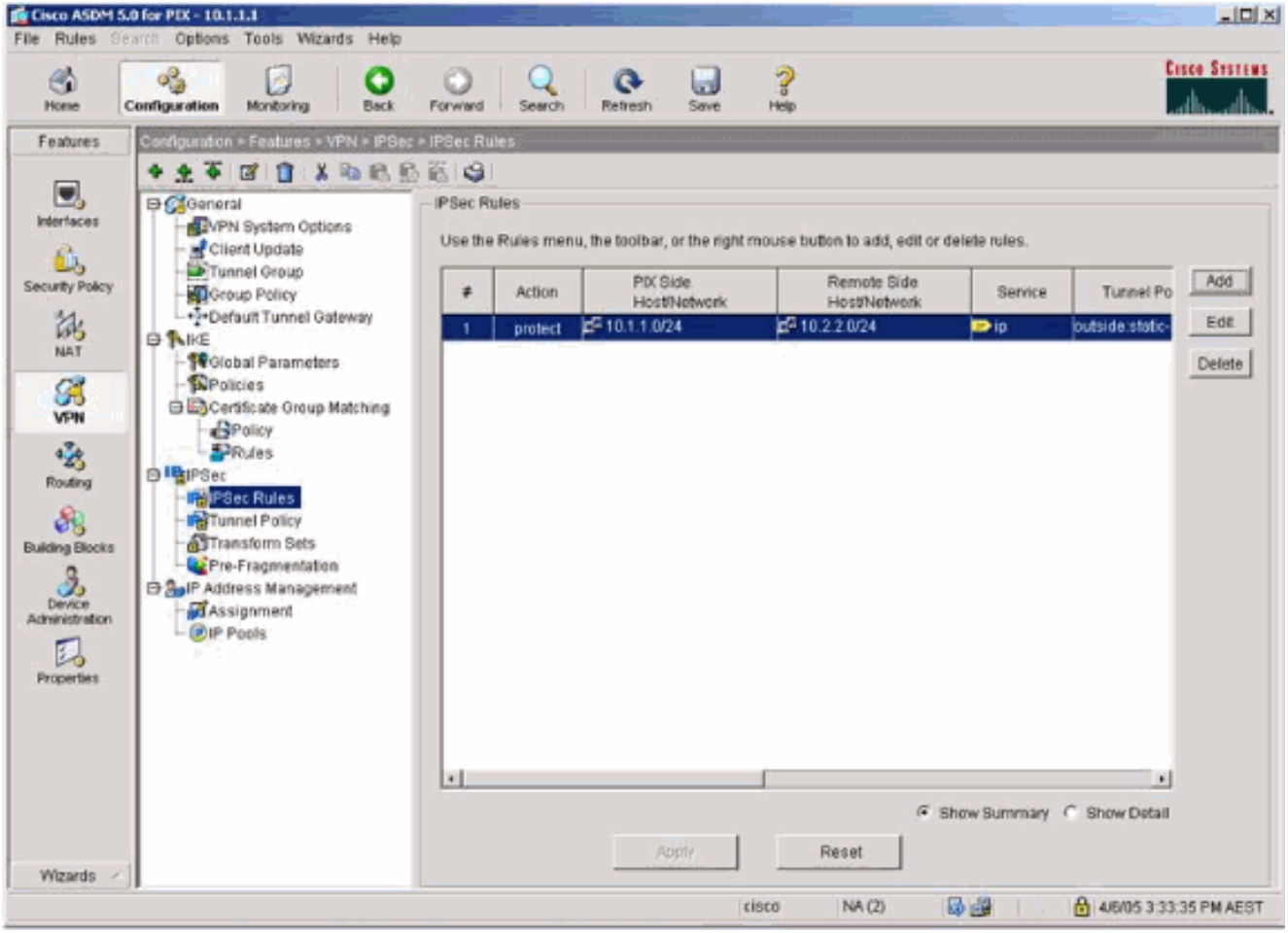


7. Selecione **VPN > IKE > políticas** e escolha as políticas de

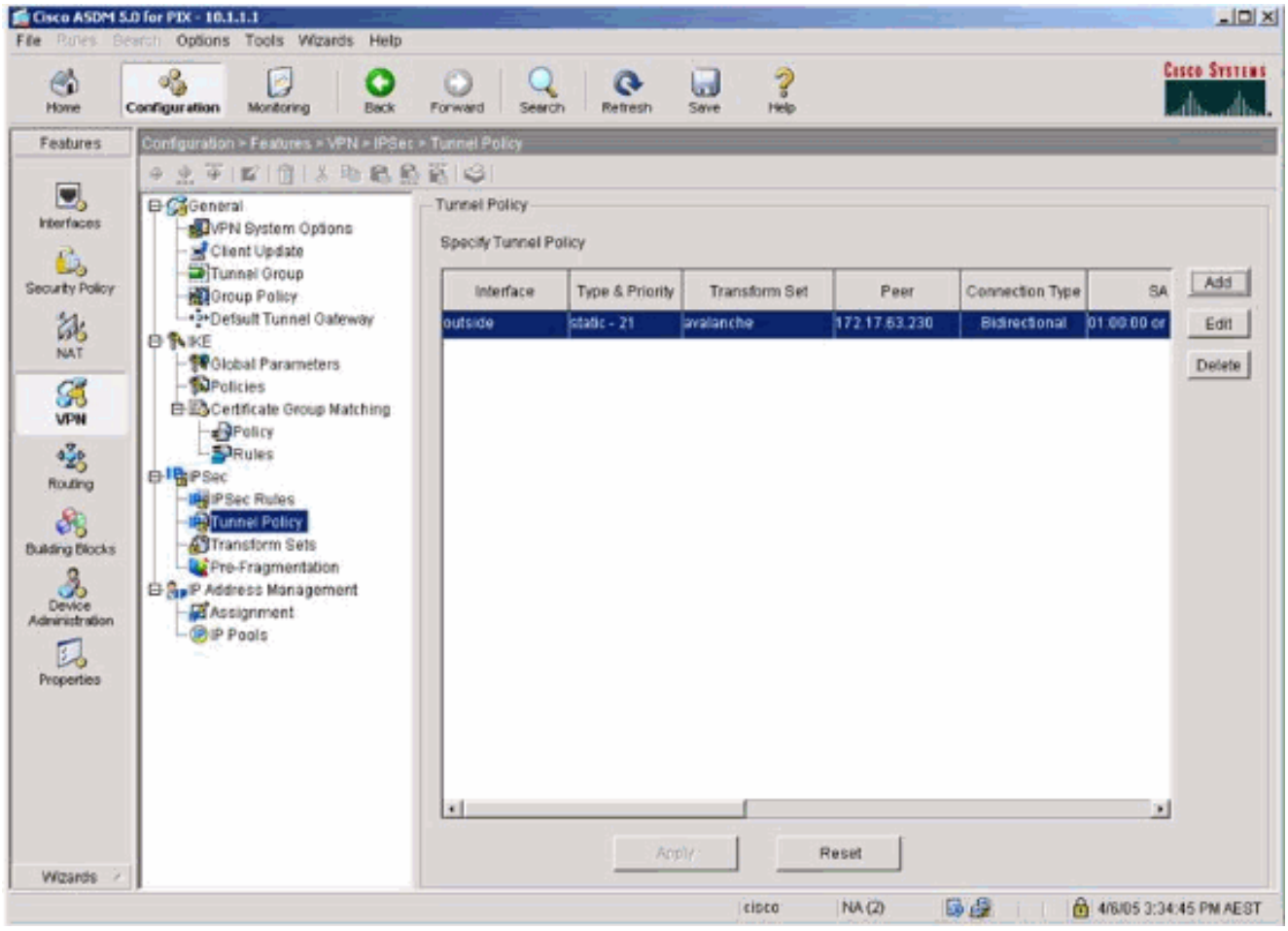
IKE.



8. Selecione **VPN > IPsec > regras do IPsec** e escolha o **IPsec** para o túnel local e o endereçamento
remoto.

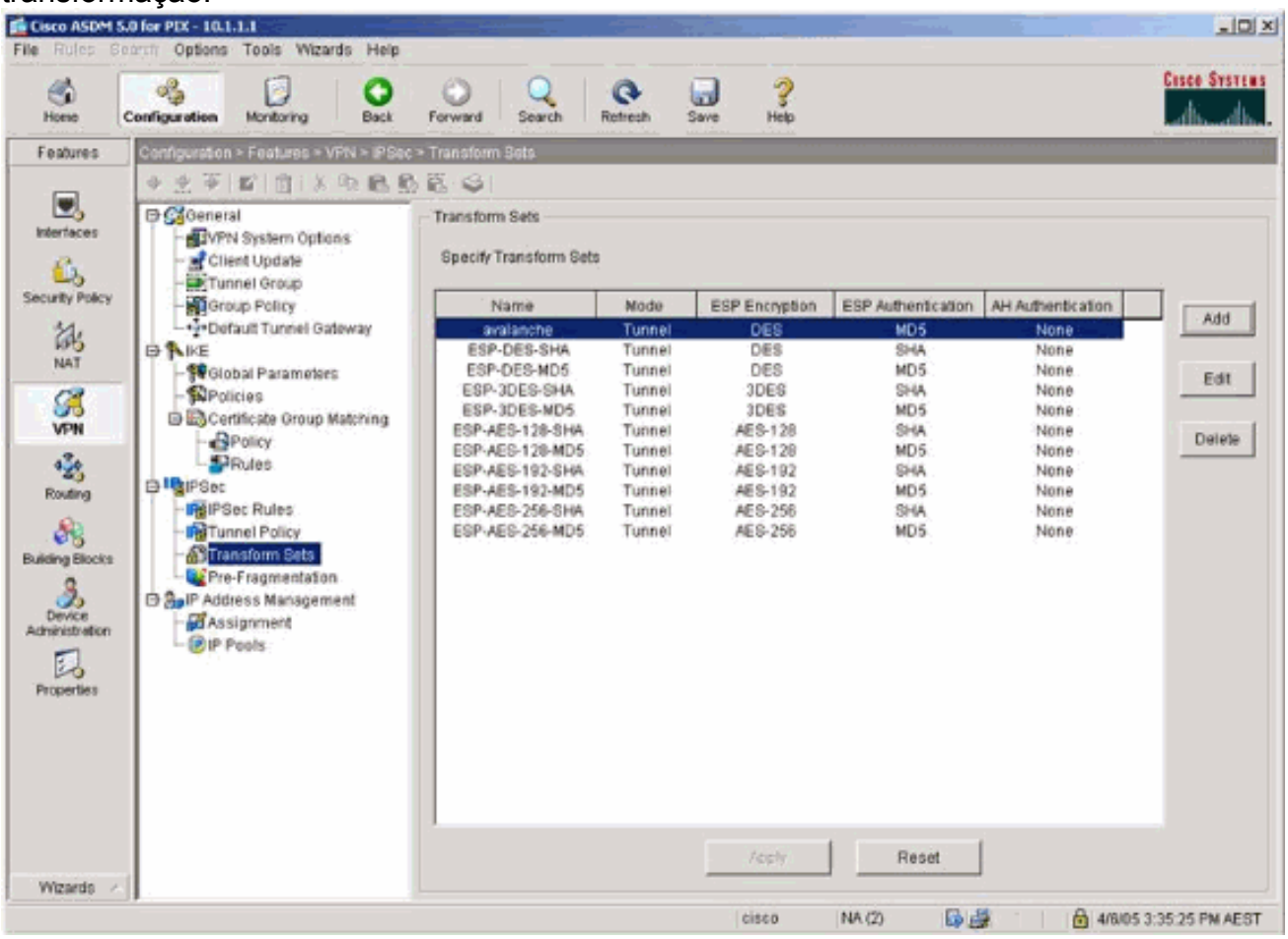


9. Selecione **política VPN > de IPsec > de túnel** e escolha a política do túnel.

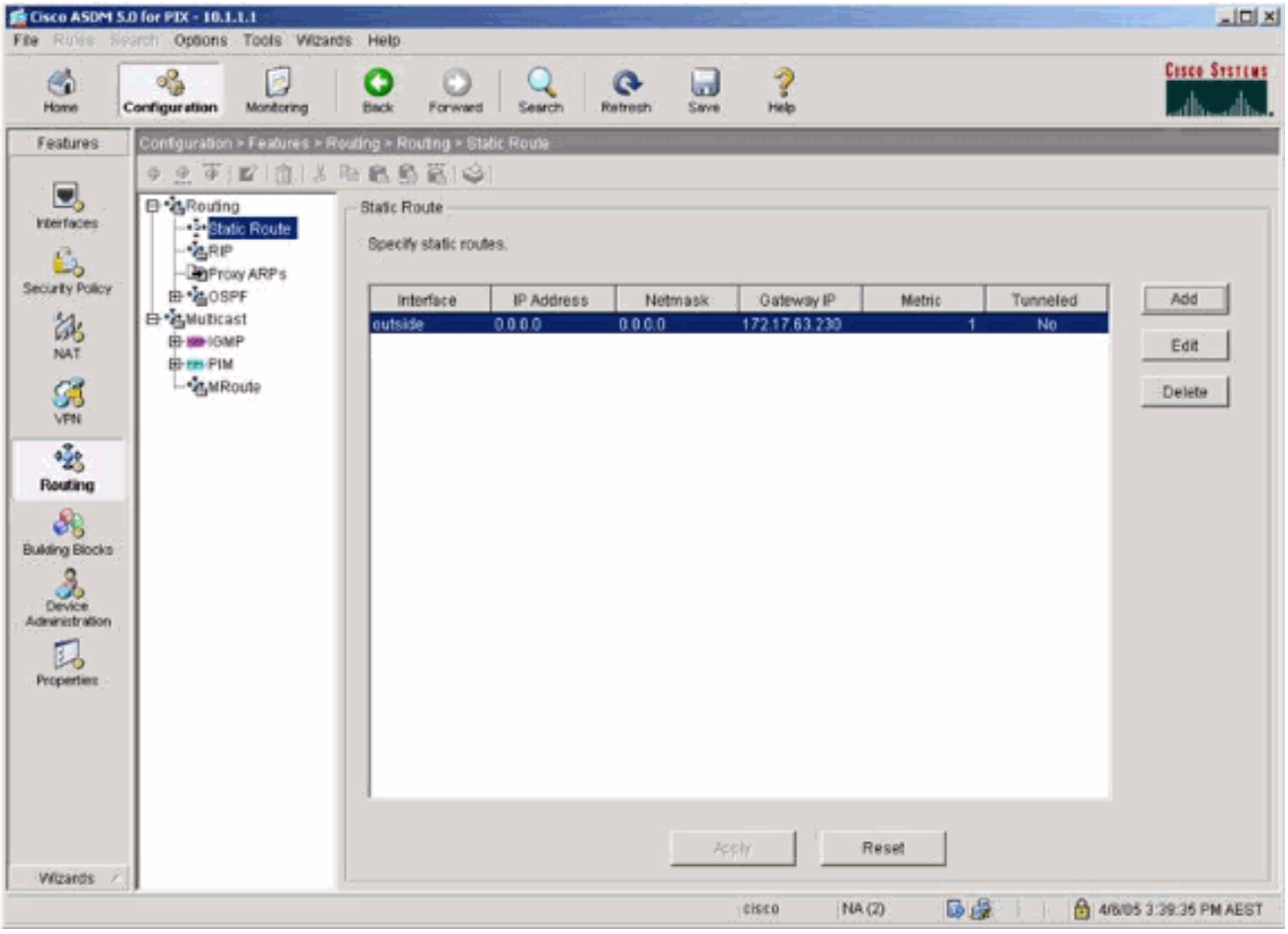


10. Seleto o **VPN > o IPsec > transformam grupos** e escolhem um grupo da

transformação.



11. Selecione o **roteamento > o roteamento > a rota estática** e escolha uma rota estática ao gateway router. Neste exemplo, a rota estática aponta ao par remoto VPN para a simplicidade.



Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- show crypto ipsec sa – Mostra as associações de segurança da fase 2.
- show crypto isakmp sa - Mostra as associações de segurança da fase 1.

Troubleshooting

Você pode usar o ASDM para permitir o registro e para ver os logs.

- Selecione a **configuração > as propriedades > instalação de registro > de registro**, escolha-os **permitem o registro** e o clique **aplica-se** para permitir o registro.
- Selecione a **monitoração > registrando > buffer de registro > no nível de registro**, escolha o **logging buffer**, e clique a **vista** para ver os logs.

Comandos para Troubleshooting

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **IPsec do debug crypto** — Mostra as negociações de IPSEC de fase 2.
- debug crypto ipsec - Exibe as negociações ISAKMP da fase 1.
- **motor do debug crypto** — Mostra o tráfego que é cifrado.
- clear crypto isakmp — Limpa as associações de segurança relacionadas à fase 1.
- clear crypto sa — Limpa as associações de segurança relacionadas à fase 2.
- debug icmp trace - Exibe se as requisições de ICMP dos hosts alcançam o PIX. Você precisa de adicionar o **comando access-list** permitir o ICMP em sua configuração a fim executar este debuga.
- logging buffer debugging - Mostra as conexões estabelecidas e negadas aos hosts que passam pelo PIX. A informação é armazenada no buffer de registro PIX e você pode ver a saída com o **comando show log**.

Informações Relacionadas

- Soluções de Troubleshooting Mais Comuns de VPN IPsec L2L e de Acesso Remoto
- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems