

# ASA/PIX - Configurar um túnel IPsec LAN a LAN do roteador Cisco IOS

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configuração usando ASDM](#)

[Verificar](#)

[Troubleshoot](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

## Introduction

Este documento demonstra como configurar um túnel de IPsec de 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.

Consulte [Configurando IPSec - Roteador para PIX](#) para obter mais informações sobre a configuração de um túnel LAN para LAN entre um roteador e o PIX.

Consulte [Túnel IPSec LAN a LAN entre o Cisco VPN 3000 Concentrator e o PIX Firewall Exemplo](#) para obter mais informações sobre a configuração de um túnel LAN a LAN entre o PIX Firewall e o Cisco VPN 3000 Concentrator.

Consulte o [Exemplo de Configuração de Túnel IPsec Entre PIX 7.x e VPN 3000 Concentrator](#) para saber mais sobre o cenário em que o túnel de LAN para LAN está entre o PIX e o VPN Concentrator.

Consulte o [Exemplo de Configuração de PIX/ASA 7.x Enhanced Spoke-to-Client VPN com Autenticação TACACS+](#) para saber mais sobre o cenário em que o túnel de LAN para LAN entre os PIXes também permite que um VPN Client acesse o PIX do spoke através do PIX do hub.

Consulte a [SDM: Exemplo de Configuração de VPN IPsec Site-to-Site entre ASA/PIX e um IOS Router](#) para saber mais sobre o mesmo cenário em que o PIX/ASA Security Appliance executa a versão de software 8.x.

Consulte o [Configuration Professional: Exemplo de Configuração de VPN IPsec Site-to-Site entre ASA/PIX e um IOS Router](#) para saber mais sobre o mesmo cenário em que a configuração relacionada ao ASA é mostrada usando a GUI do ASDM e a configuração relacionada ao roteador é mostrada usando a GUI do Cisco CP.

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

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

- PIX-525 com software PIX versão 7.0
- Roteador Cisco 2611 com Software Cisco IOS® versão 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

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 10.1.1.0 vai para a rede 10.2.2.0, a lista de acesso é usada para permitir que o tráfego da rede 10.1.1.0 seja criptografado sem a Tradução de Endereço de Rede (NAT). No roteador, os comandos **`route-map`** e **`access-list`** são usados para permitir que o tráfego de rede 10.2.2.0 seja criptografado sem NAT. No entanto, quando alguns desses usuários vão para algum outro lugar, eles são convertidos no endereço 172.17.63.230 por meio de Conversão de Endereço de Porta (PAT).

Estes são os comandos de configuração necessários no PIX Security Appliance para que o tráfego *não* seja executado através do PAT pelo túnel e o tráfego para a Internet seja executado através do 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
```

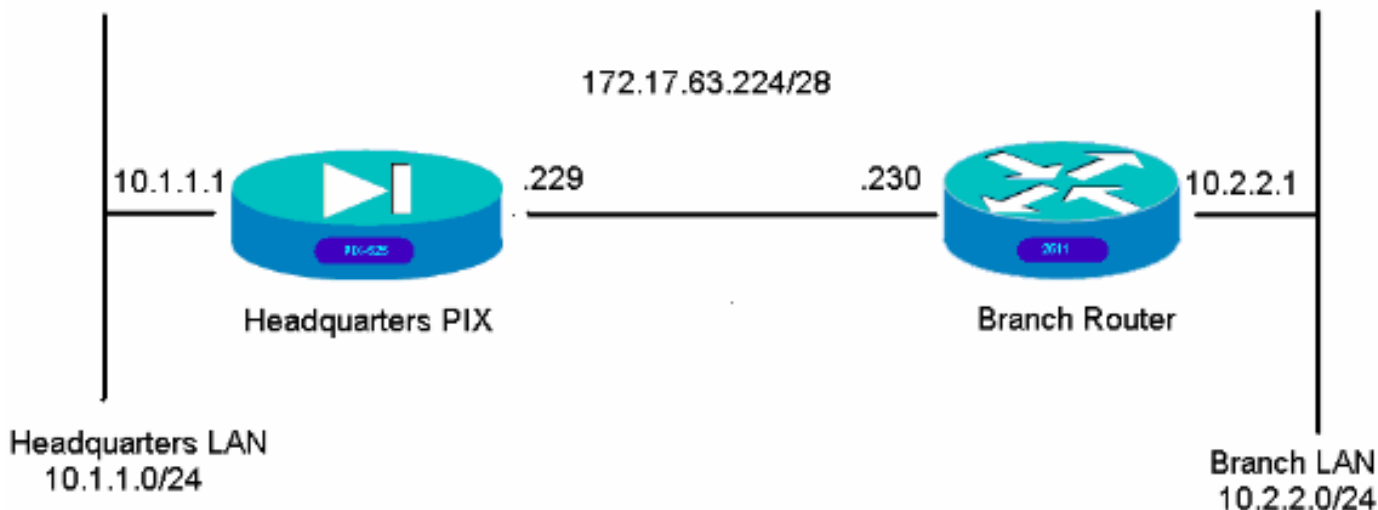
## Configurar

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

Esses exemplos de configuração são para a interface de linha de comando. Consulte a [seção Configuração usando o Adaptive Security Device Manager \(ASDM\)](#) deste documento se preferir configurar usando o ASDM.

- [PIX da matriz](#)
- [Roteador da 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 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
SV-2-8#

```

**Roteador da 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

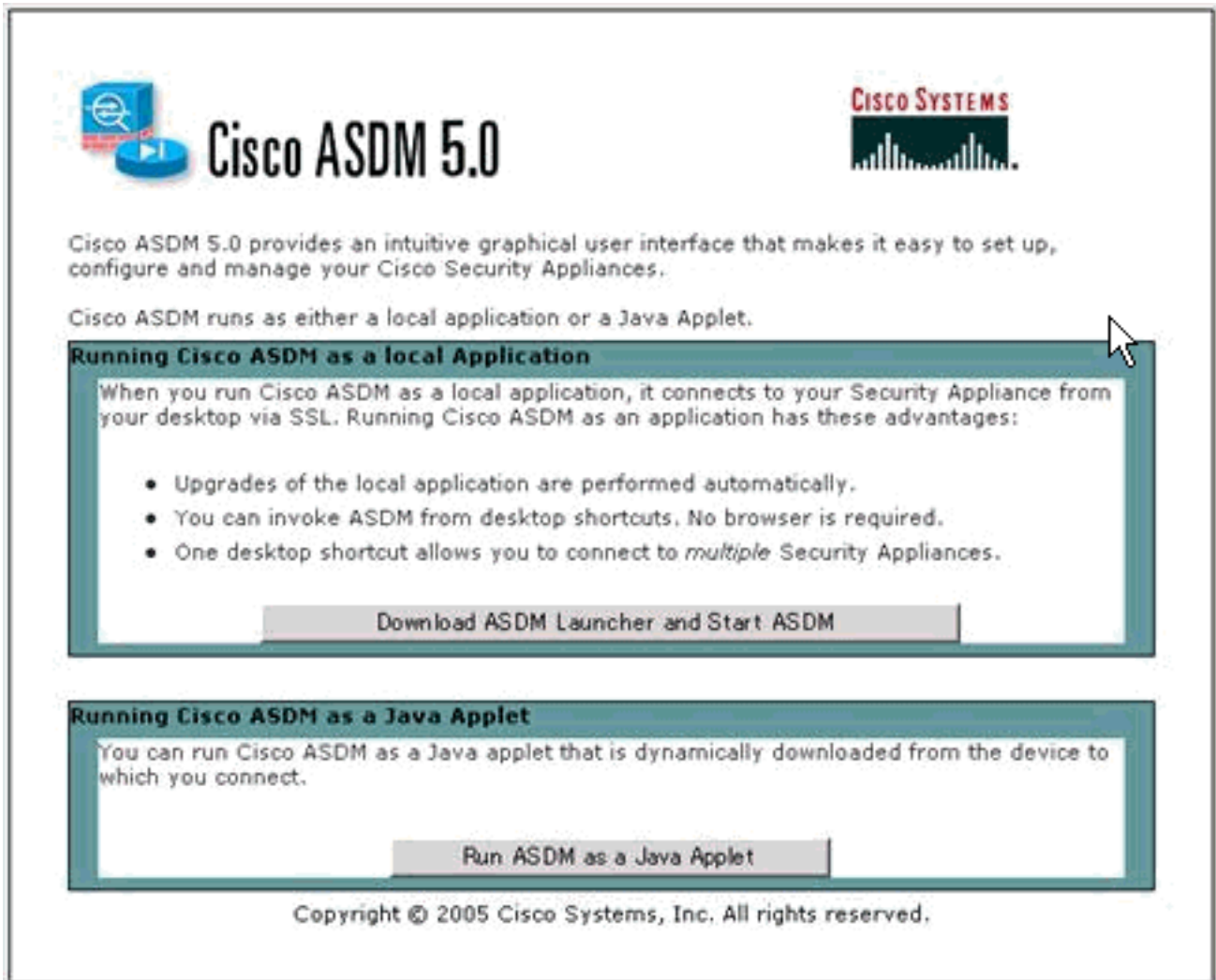
```



## [Configuração usando ASDM](#)

Este exemplo demonstra como configurar o PIX usando a GUI do ASDM. Um PC com um navegador e o endereço IP 10.1.1.2 está conectado à interface interna e1 do PIX. Verifique se http está habilitado no PIX.

Este procedimento ilustra a configuração ASDM do PIX da matriz.

1. Conecte o PC ao PIX e escolha um método de download.



 **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**

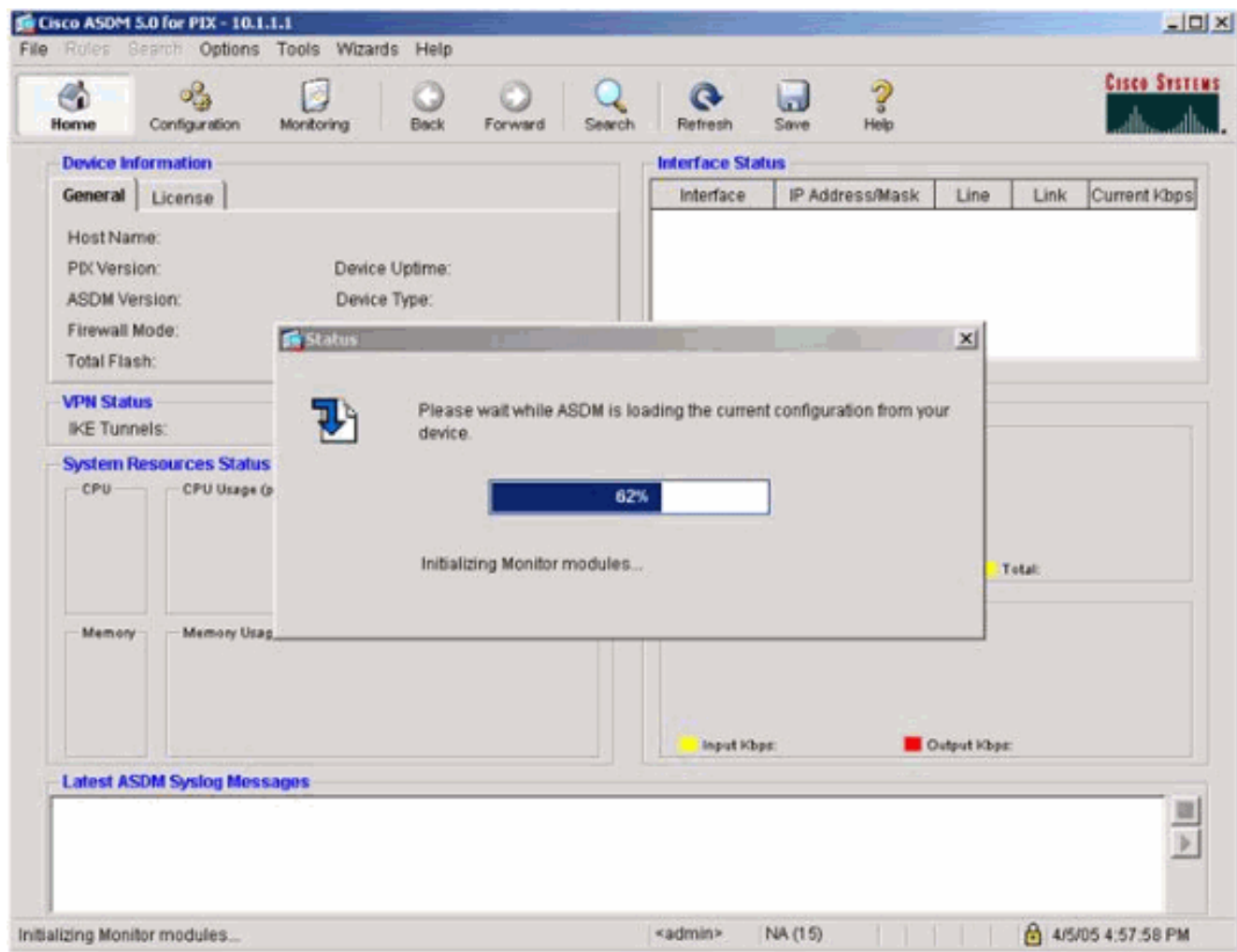
You can run Cisco ASDM as a Java applet that is dynamically downloaded from the device to which you connect.

[Run ASDM as a Java Applet](#)

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

O ASDM carrega a configuração existente do PIX.





Essa janela fornece instrumentos e menus de monitoramento.

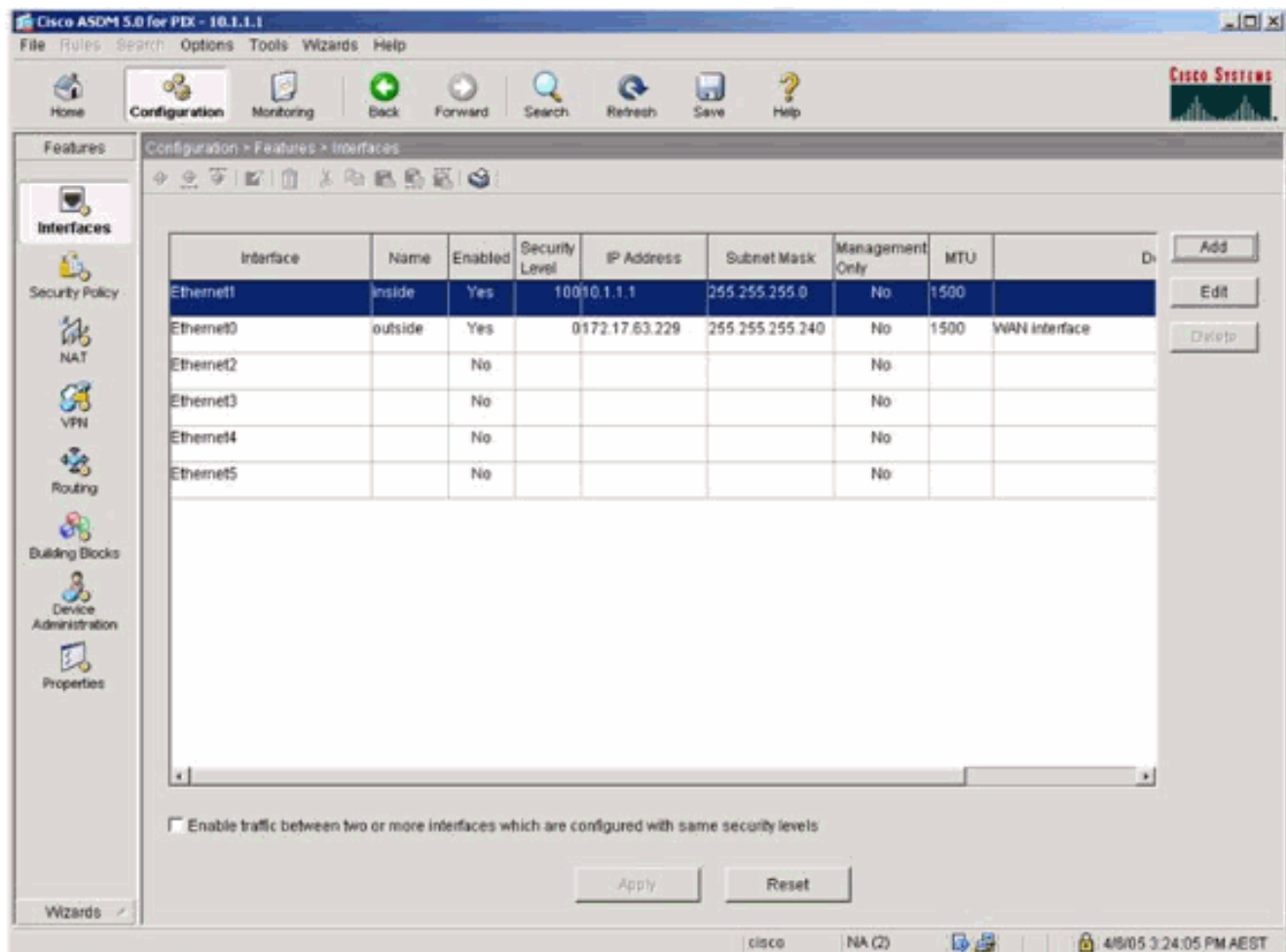
The screenshot displays the Cisco ASDM 5.0 for PIX - 10.1.1.1 interface. The top navigation bar includes Home, Configuration, Monitoring, Back, Forward, Search, Refresh, Save, and Help. The main content area is divided into several sections:

- 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:**

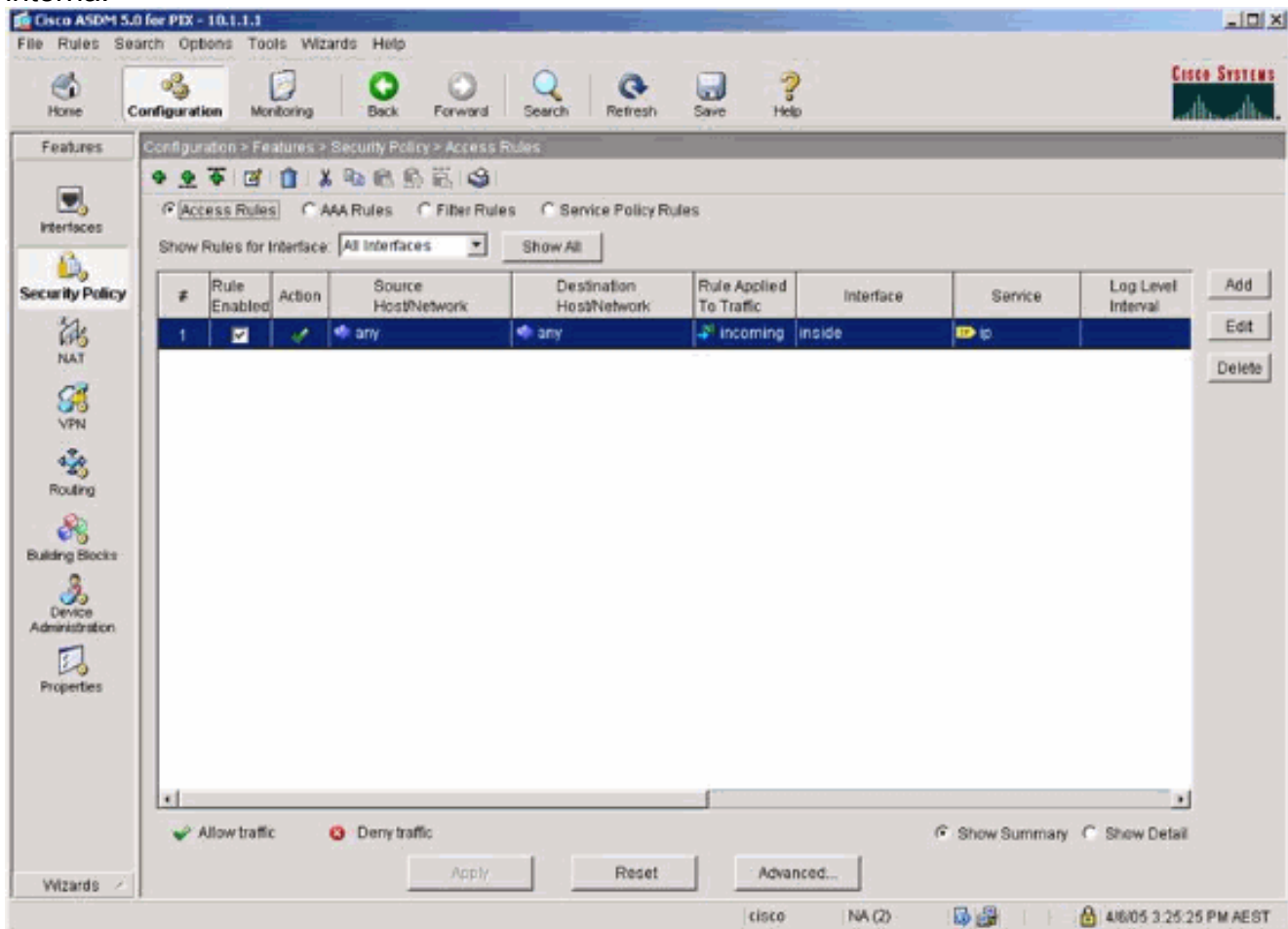
Interface	IP Address/Mask	Line	Link	Current Kbps
inside	10.1.1.1/24	up	up	1
- VPN Status:** IKE Tunnels: 0, IPsec Tunnels: 0.
- System Resources Status:**
  - CPU: 0% (04:57:46), CPU Usage (percent) graph showing 0% usage.
  - Memory: 67MB (04:57:46), Memory Usage (MB) graph showing 67MB usage.
- Traffic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

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

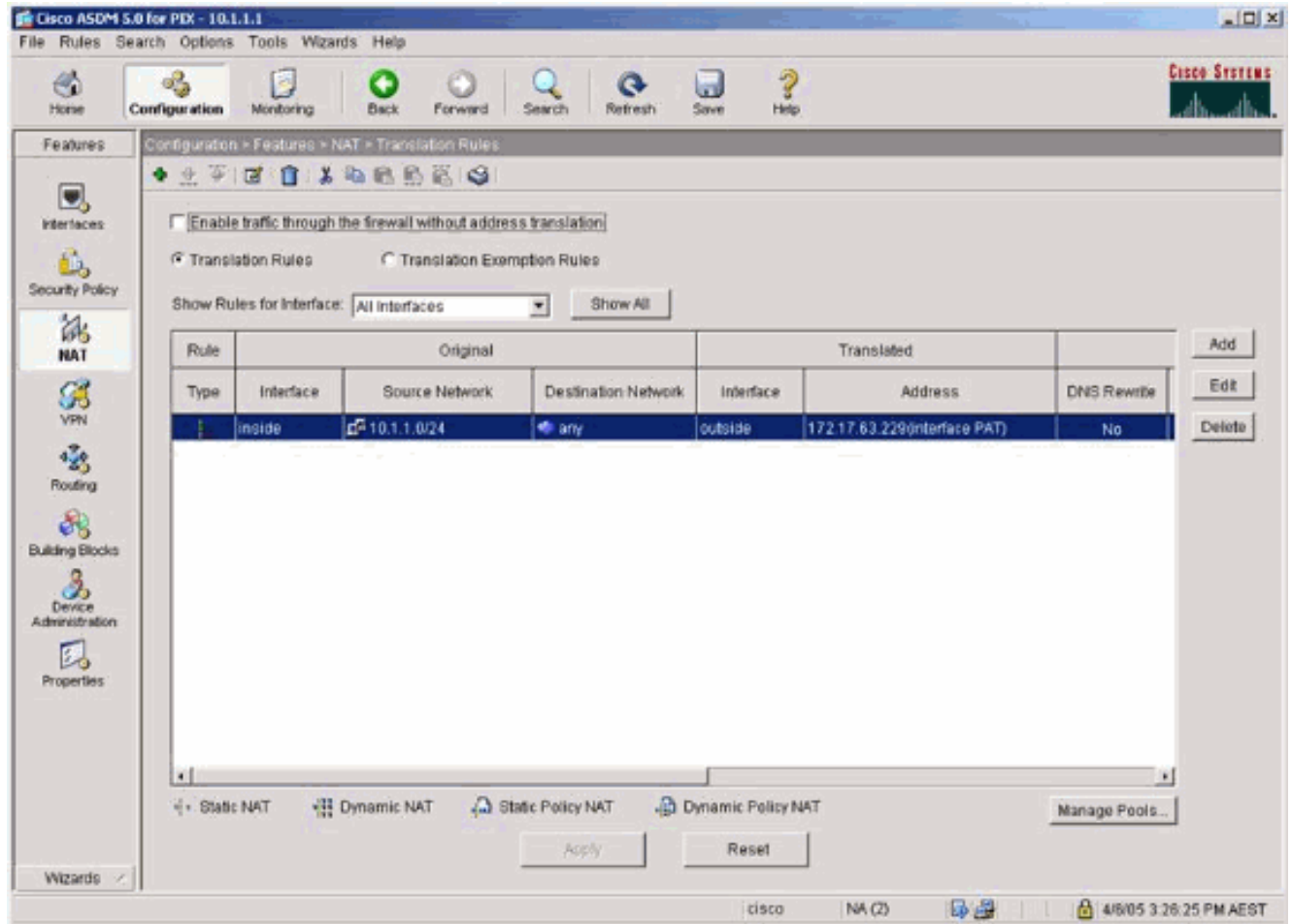
2. Selecione **Configuration > Features > Interfaces** e selecione **Add** para novas interfaces ou **Edit** para uma configuração existente.



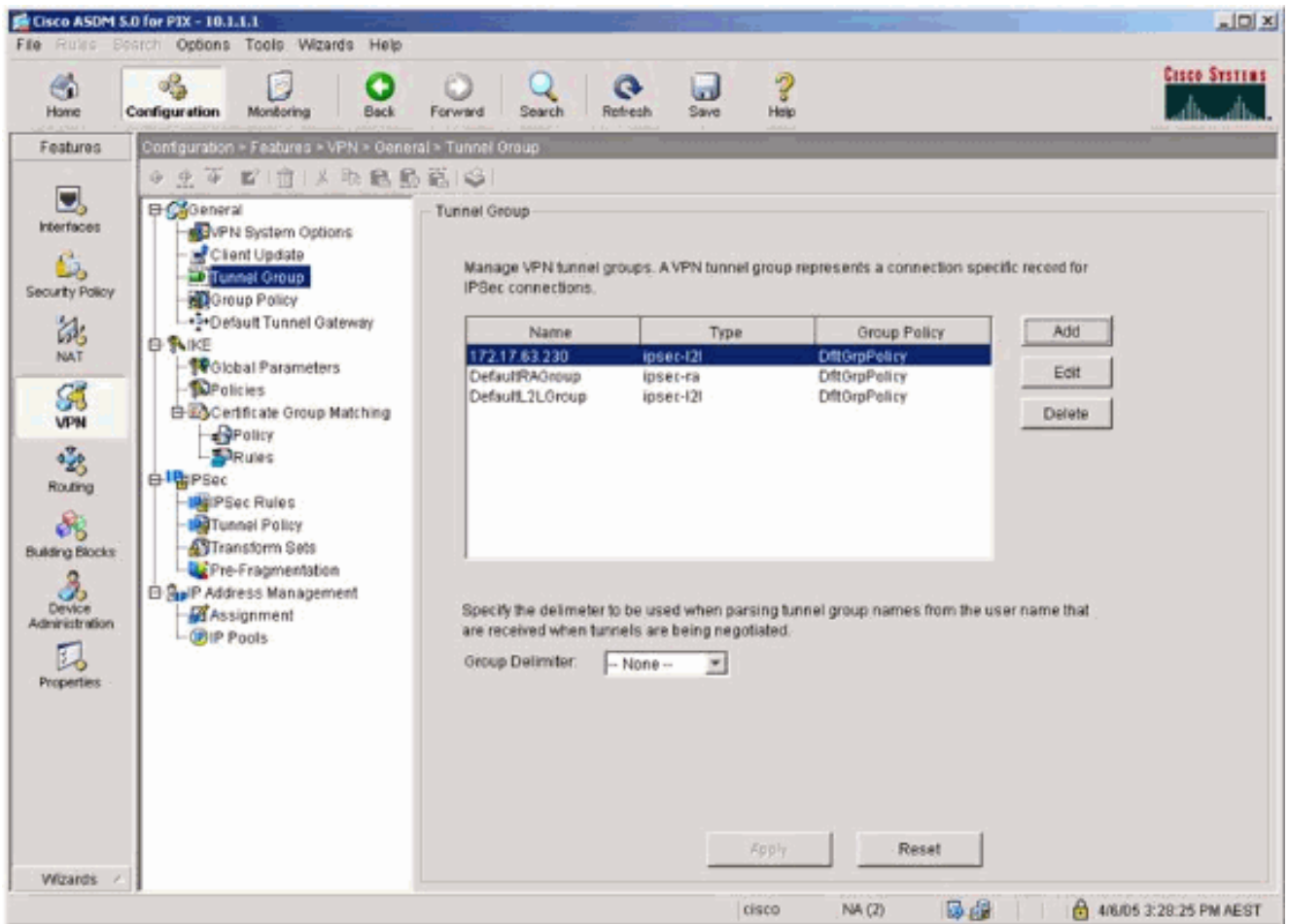
3. Selecione as opções de segurança para a interface interna.



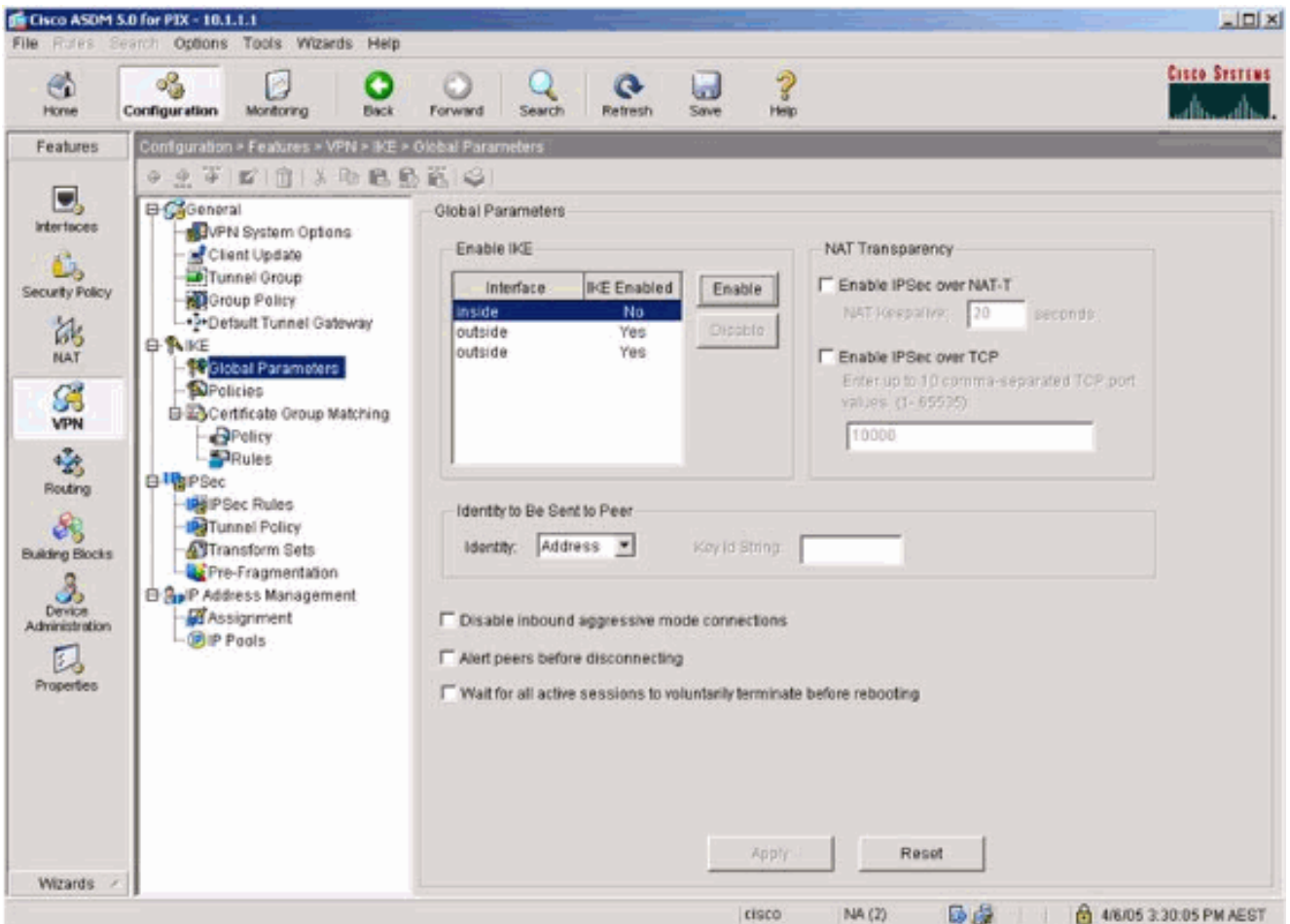
4. Na configuração de NAT, o tráfego criptografado é isento de NAT e todos os outros tráfegos são NAT/PAT para a interface externa.



5. Selecione VPN > Geral > Grupo de Túneis e habilite um Grupo de Túneis



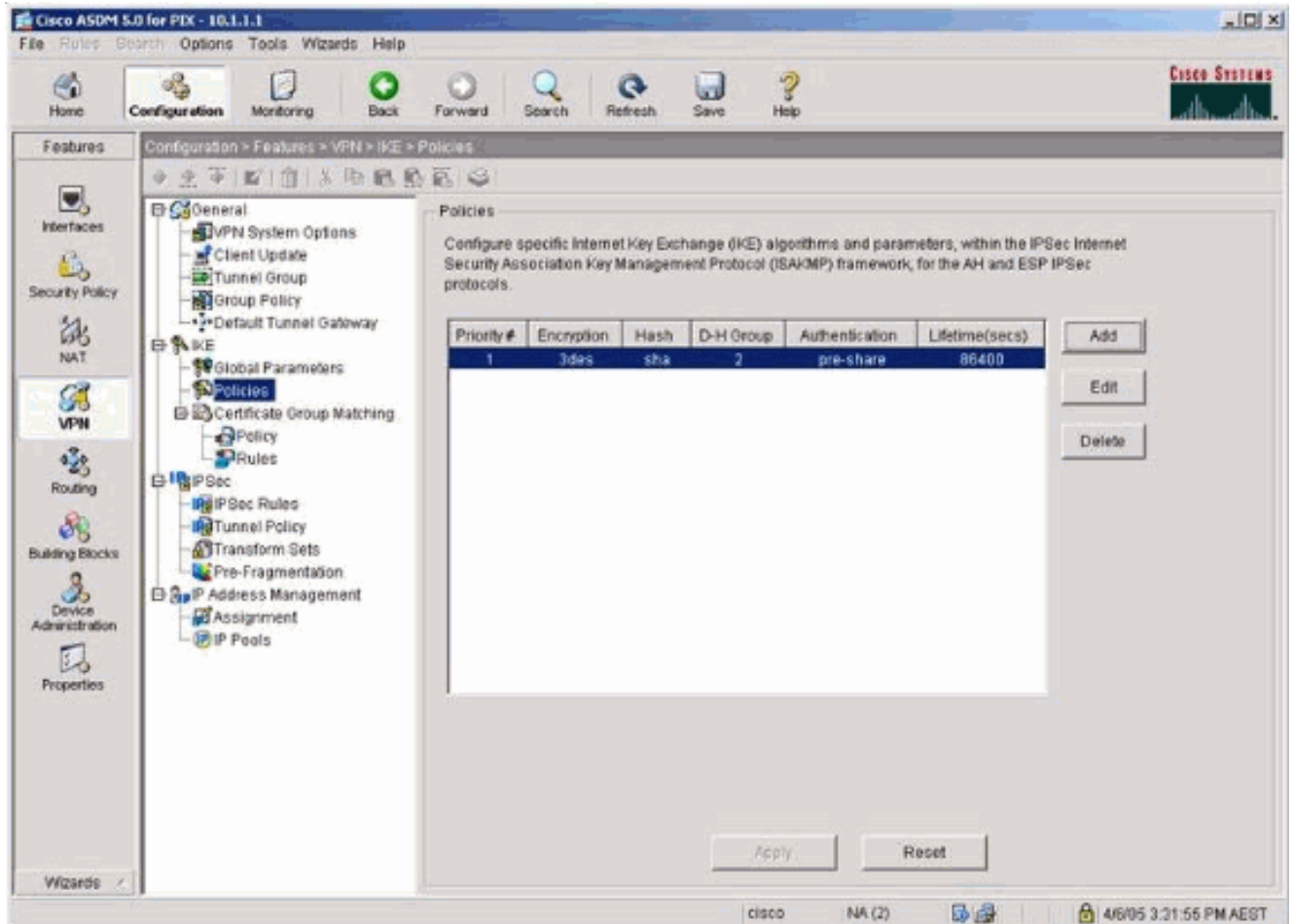
6. Selecione VPN > IKE > Parâmetros globais e ative IKE na interface externa.



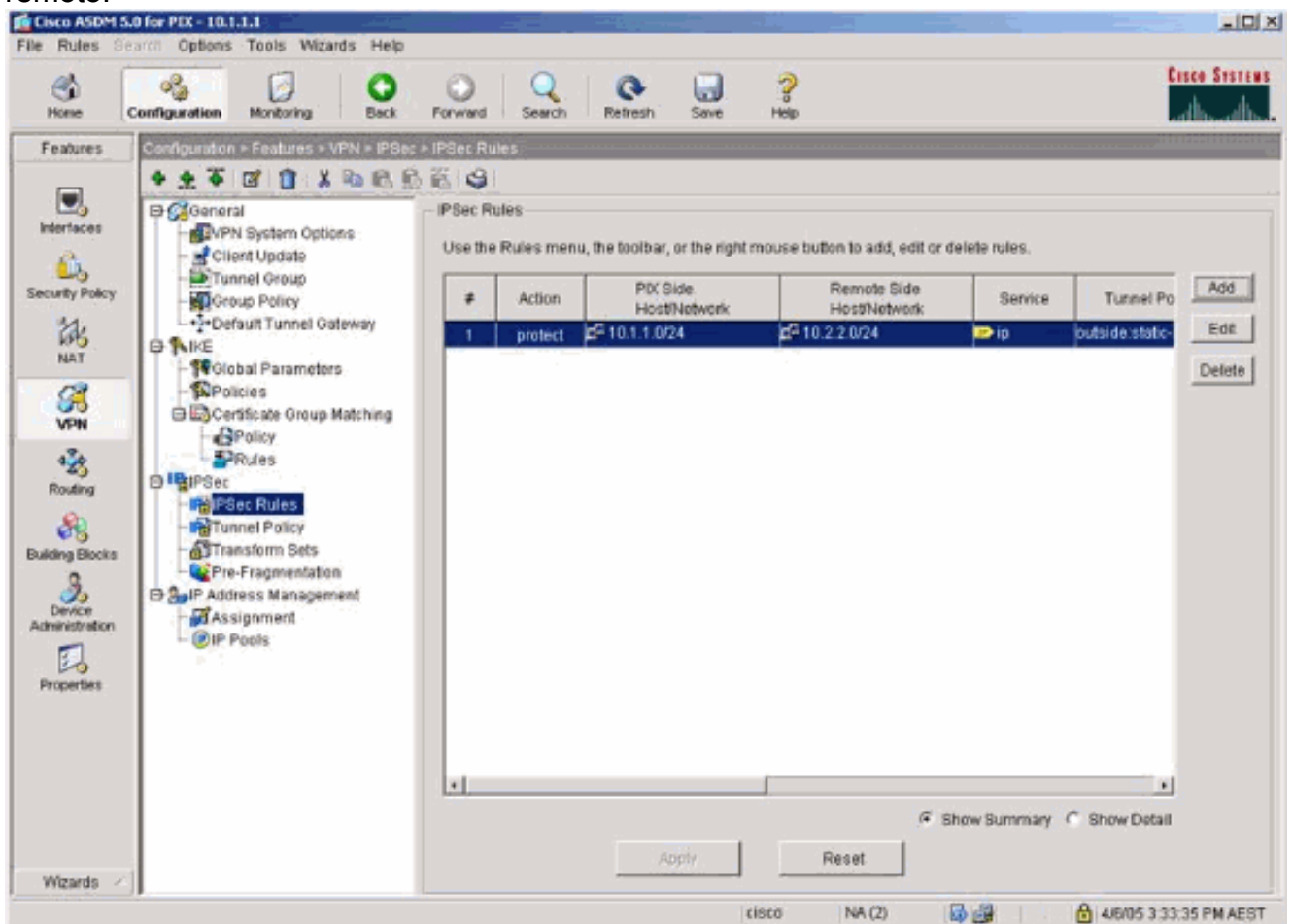
7. Selecione VPN > IKE > Políticas e escolha as políticas de



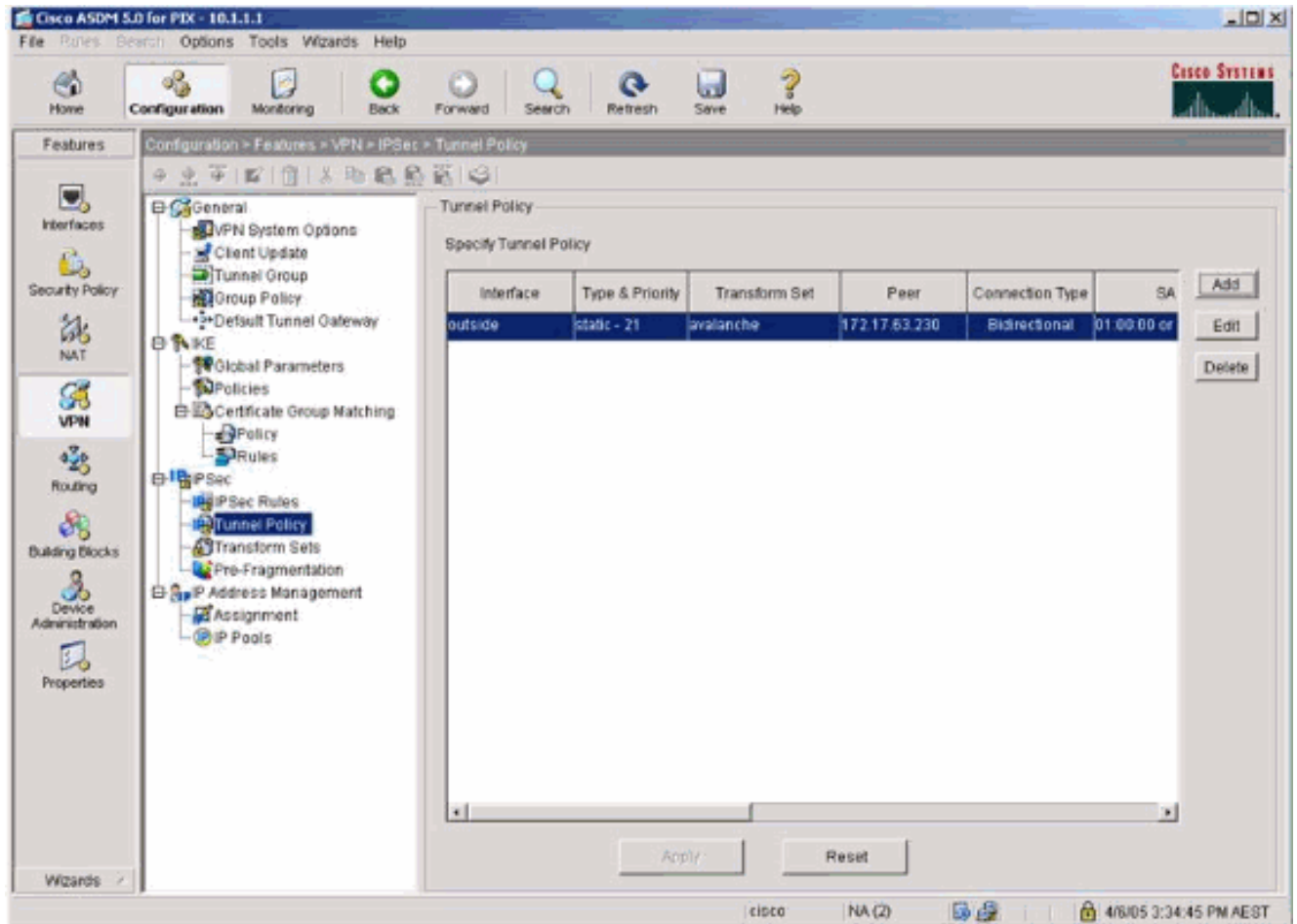
# IKE.



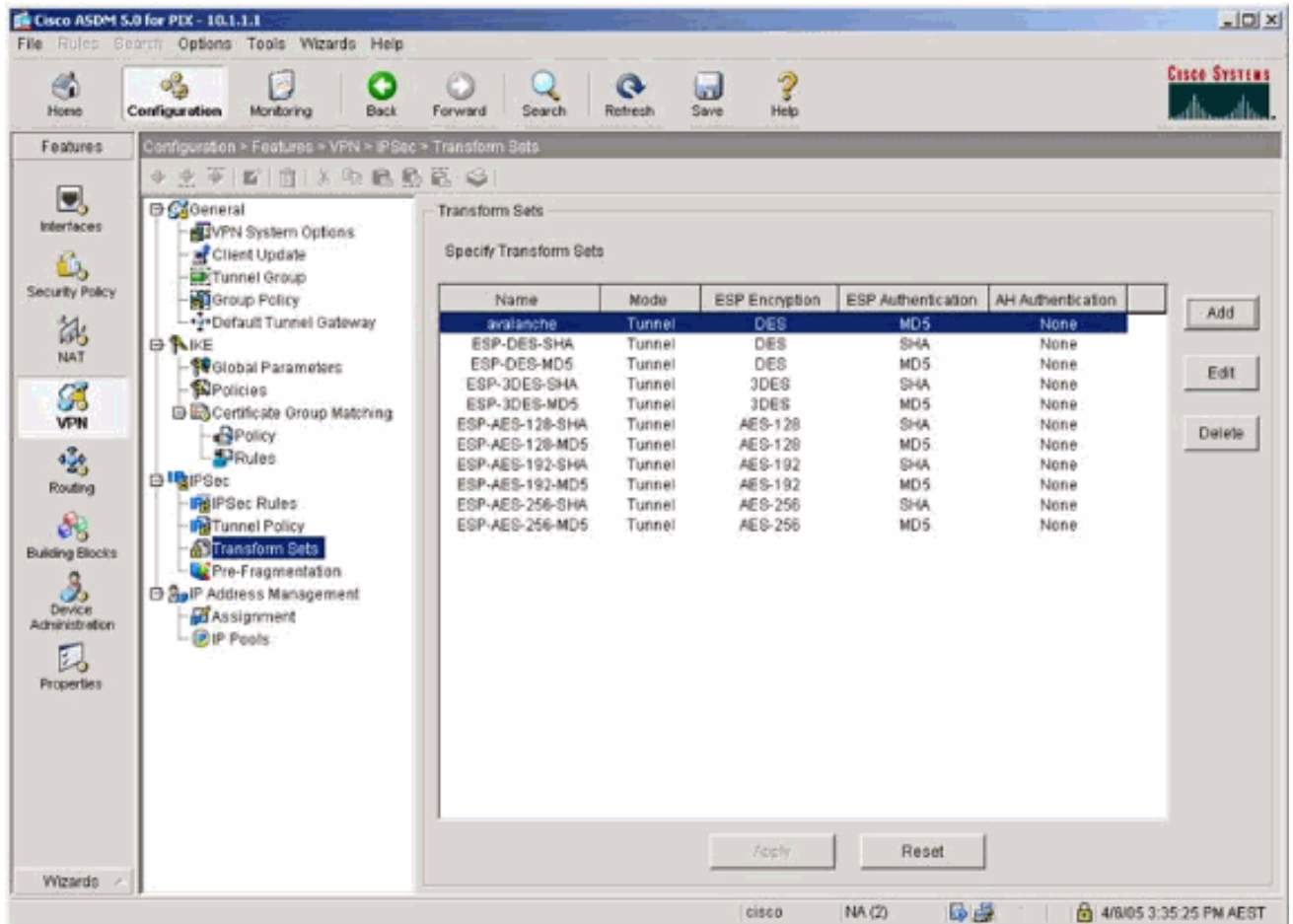
8. Selecione VPN > IPsec > IPsec Rules e escolha IPsec para o túnel local e o endereçamento remoto.



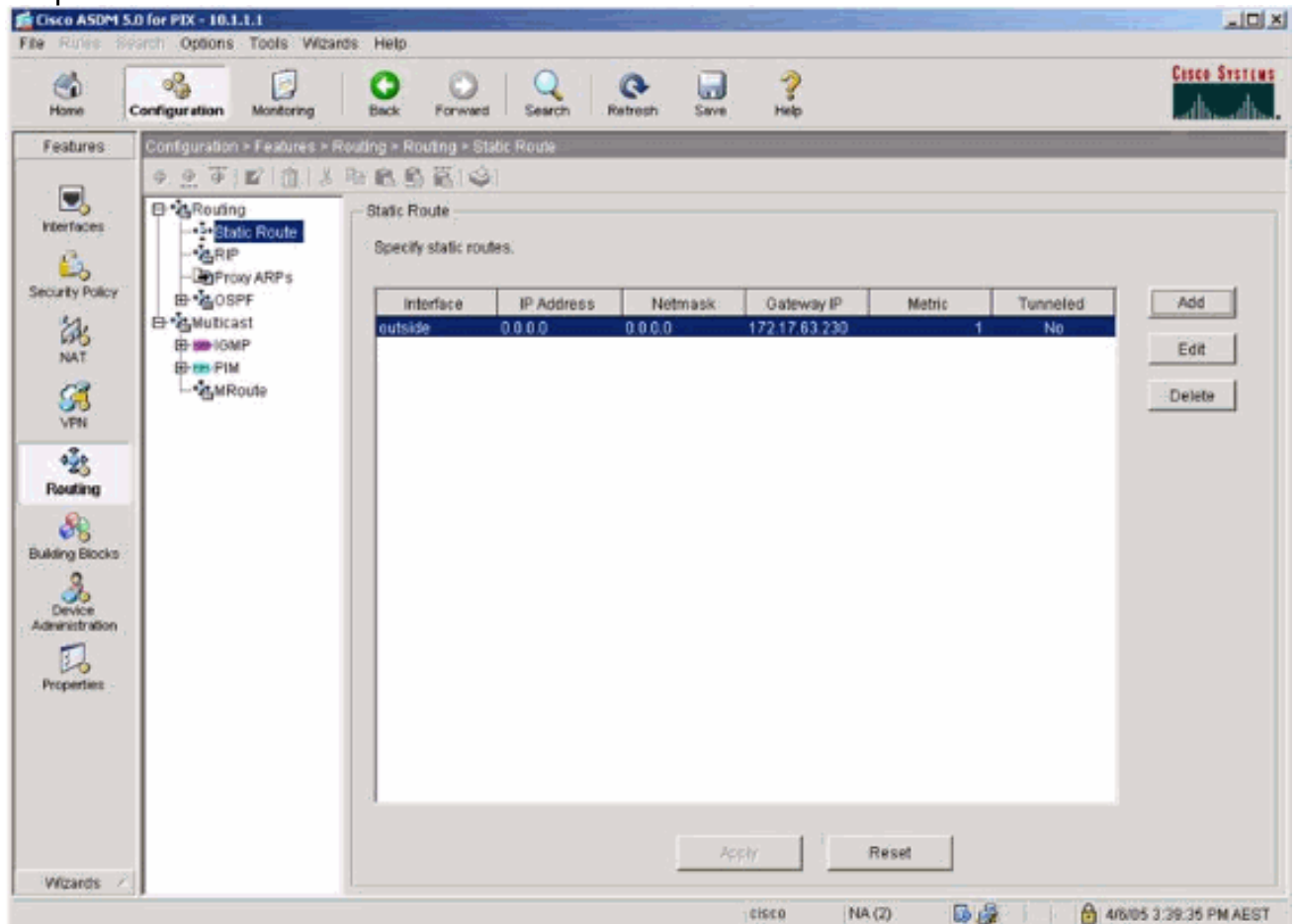
9. Selecione **VPN > IPsec > Tunnel Policy** e escolha a política de túnel.



10. Selecione **VPN > IPsec > Transform Sets** e escolha um Transform Set.



11. Selecione **Routing > Routing > Static Route** e escolha uma rota estática para o roteador do gateway. Neste exemplo, a rota estática aponta para o peer VPN remoto para simplificar.





## Verificar

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

A [Output Interpreter Tool \( somente clientes registrados\) \(OIT\) oferece suporte a 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.

## Troubleshoot

Você pode usar o ASDM para ativar o registro e exibir os registros.

- Selecione **Configuration > Properties > Logging > Logging Setup**, escolha **Enable Logging** e clique em **Apply** para ativar o registro.
- Selecione **Monitoring > Logging > Log Buffer > On Logging Level**, escolha **Logging Buffer** e clique em **View** para exibir os logs.

## Comandos para Troubleshooting

A [Output Interpreter Tool \( somente clientes registrados\) \(OIT\) oferece suporte a 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**.

- **debug crypto ipsec** — Mostra as negociações de IPsec da fase 2.
- **debug crypto ipsec - Exibe as negociações ISAKMP da fase 1.**
- **debug crypto engine** — Mostra o tráfego que está criptografado.
- **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** — Mostra se as solicitações ICMP dos hosts acessam o PIX. Você precisa adicionar o comando **access-list** para permitir o ICMP em sua configuração para executar essa depuração.
- **logging buffer debugging - Mostra as conexões estabelecidas e negadas aos hosts que passam pelo PIX.** As informações são armazenadas no buffer de log 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 \(RFCs\)](#)