

ASA/PIX - Konfigurieren eines Cisco IOS-Router-LAN-to-LAN-IPsec-Tunnels

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfigurationen](#)

[Konfiguration mit ASDM](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Befehle zur Fehlerbehebung](#)

[Zugehörige Informationen](#)

[Einleitung](#)

In diesem Dokument wird veranschaulicht, wie ein IPsec-Tunnel von der PIX Security Appliance 7.x und höher oder der Adaptive Security Appliance (ASA) mit einem internen Netzwerk zu einem 2611-Router konfiguriert wird, der ein Krypto-Image ausführt. Zur Vereinfachung werden statische Routen verwendet.

Weitere Informationen über eine LAN-zu-LAN-Tunnelkonfiguration zwischen einem Router und dem PIX finden Sie unter [Konfigurieren von IPSec - Router zu PIX](#).

Weitere Informationen zur Konfiguration eines LAN-to-LAN-Tunnels zwischen dem Cisco VPN 3000 Concentrator und der PIX-Firewall-[Konfiguration](#) zwischen der PIX-Firewall und dem Cisco VPN 3000-Concentrator finden Sie im [Konfigurationsbeispiel](#) für einen LAN-zu-LAN-Tunnel.

Weitere Informationen zum Szenario, in dem sich der LAN-zu-LAN-Tunnel zwischen dem PIX [7.x und dem VPN](#) 3000 Concentrator befindet, finden Sie im Konfigurationsbeispiel für den [IPsec-Tunnel zwischen PIX und VPN Concentrator](#).

Unter [Konfigurationsbeispiel für PIX/ASA 7.x Enhanced Spoke-to-Client VPN mit TACACS+-Authentifizierung](#) erfahren Sie mehr über das Szenario, in dem der LAN-zu-LAN-Tunnel zwischen den PIXs auch einem VPN-Client den Zugriff auf die Spoke-PIX über den Hub-PIX ermöglicht.

Weitere Informationen finden Sie unter [SDM: Site-to-Site-IPsec-VPN zwischen ASA/PIX und einem IOS-Router - Konfigurationsbeispiel](#), um mehr über dasselbe Szenario zu erfahren, in dem

die PIX/ASA Security Appliance die Softwareversion 8.x ausführt.

Weitere Informationen finden Sie unter [Configuration Professional: Standortübergreifendes IPsec-VPN zwischen ASA/PIX und einem IOS-Router - Konfigurationsbeispiel](#), um mehr über dasselbe Szenario zu erfahren, in dem die ASA-bezogene Konfiguration mithilfe der ASDM-GUI angezeigt wird und die Router-bezogene Konfiguration mithilfe der Cisco CP-GUI angezeigt wird.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- PIX-525 mit PIX Software Version 7.0
- Cisco 2611 Router mit Cisco IOS® Software, Version 12.2(15)T13

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Auf dem PIX arbeiten die Befehle **access-list** und **nat 0** zusammen. Wenn ein Benutzer im 10.1.1.0-Netzwerk zum 10.2.2.0-Netzwerk geht, wird die Zugriffsliste verwendet, um die Verschlüsselung des 10.1.1.0-Netzwerkverkehrs ohne Network Address Translation (NAT) zu ermöglichen. Auf dem Router werden die Befehle **route-map** und **access-list** verwendet, um die Verschlüsselung des 10.2.2.0-Netzwerkverkehrs ohne NAT zu ermöglichen. Wenn jedoch dieselben Benutzer an einen anderen Ort reisen, werden sie mithilfe von Port Address Translation (PAT) in die Adresse 172.17.63.230 übersetzt.

Dies sind die Konfigurationsbefehle, die auf der PIX Security Appliance erforderlich sind, damit Datenverkehr *nicht* über PAT über den Tunnel läuft und Datenverkehr zum Internet über PAT fließt.

```
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
```

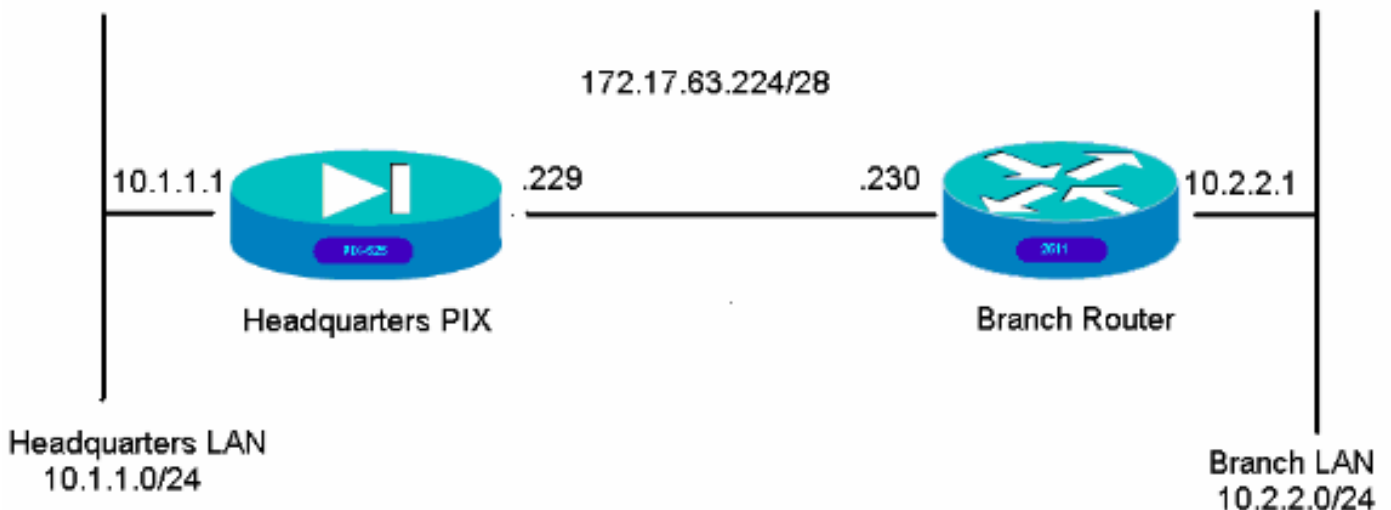
Konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

Diese Konfigurationsbeispiele gelten für die Befehlszeilenschnittstelle. Wenn Sie [ASDM](#) verwenden möchten, lesen Sie den Abschnitt "[Konfiguration mithilfe](#) des [Adaptive Security Device Manager \(ASDM\)](#) dieses Dokuments.

- [Hauptsitz PIX](#)
- [Zweigstellen-Router](#)

Hauptsitz 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
SV-2-8#
```

Zweigstellen-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
```

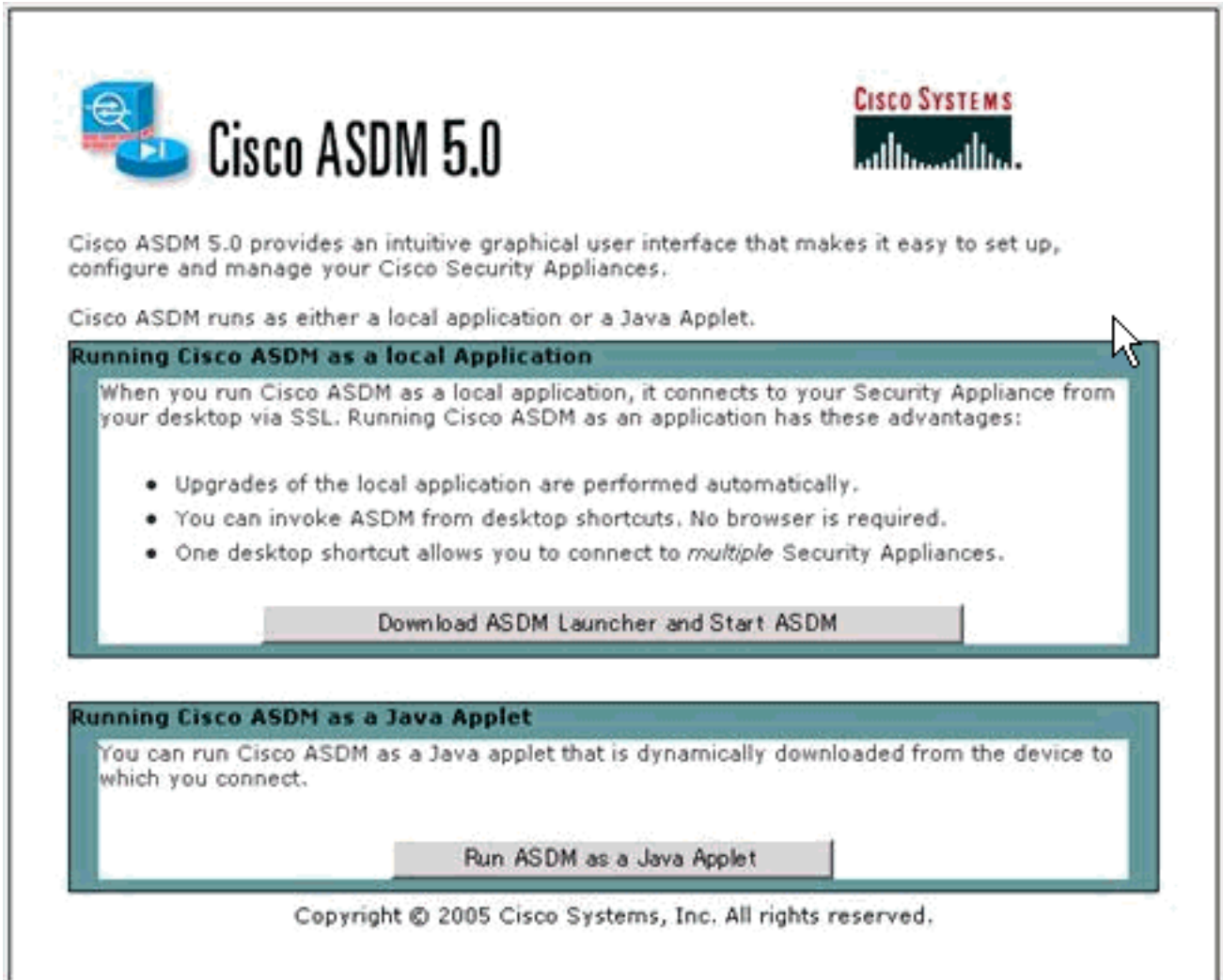
```
no voice hpi capture destination
!
!
mta receive maximum-recipients 0
!
!
!
!
interface Ethernet0/0
ip address 172.17.63.230 255.255.255.240
ip nat outside
no ip route-cache
no ip mroute-cache
half-duplex
crypto map nolan
!
interface Ethernet0/1
ip address 10.2.2.1 255.255.255.0
ip nat inside
half-duplex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

[Konfiguration mit ASDM](#)

In diesem Beispiel wird die Konfiguration des PIX mithilfe der ASDM-GUI veranschaulicht. Ein PC mit Browser und IP-Adresse 10.1.1.2 ist mit der internen Schnittstelle e1 des PIX verbunden. Stellen Sie sicher, dass http auf dem PIX aktiviert ist.

Dieses Verfahren veranschaulicht die ASDM-Konfiguration des PIX-Systems am Hauptsitz.

1. Verbinden Sie den PC mit dem PIX, und wählen Sie eine Download-Methode aus.



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

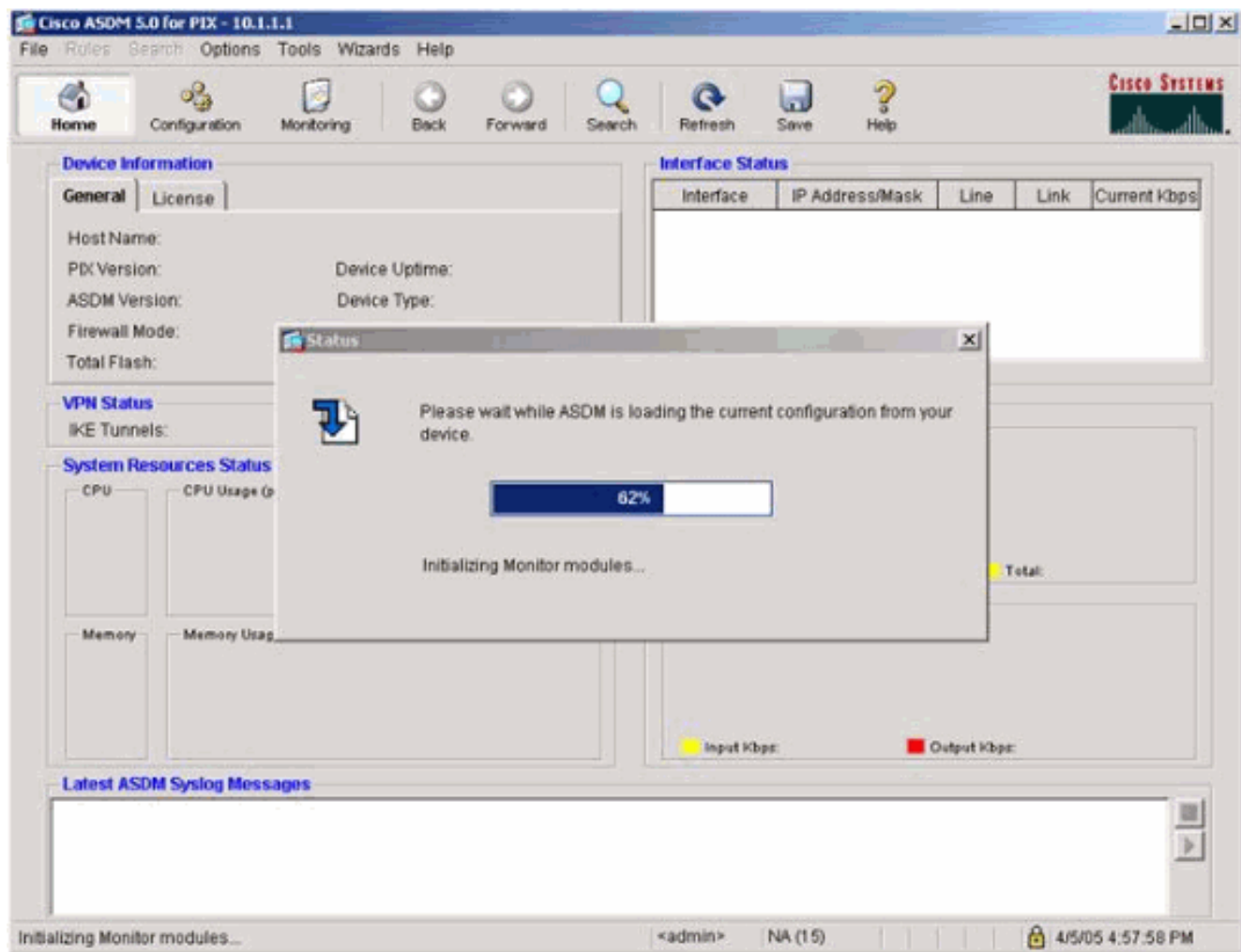
Running Cisco ASDM as a Java Applet

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 lädt die vorhandene Konfiguration aus dem PIX.



Dieses Fenster bietet Überwachungsinstrumente und Menüs.

Cisco ASDM 5.0 for PIX - 10.1.1.1

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Back Forward Search Refresh Save Help

Cisco Systems

Device Information

General License

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

Interface Status

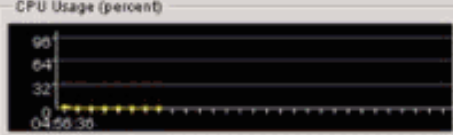
Interface	IP Address/Mask	Line	Link	Current Kbps
inside	10.1.1.1/24	up	up	1


Select an interface to view input and output Kbps

VPN Status

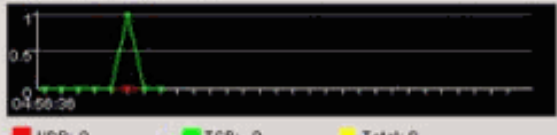
IKE Tunnels: **0** IPsec Tunnels: **0**

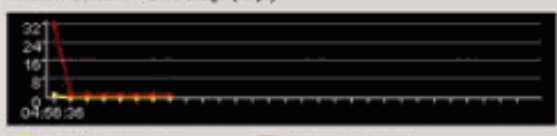
System Resources Status

CPU: **0%** CPU Usage (percent) 

Memory: **67MB** Memory Usage (MB) 

Traffic Status

Connections Per Second Usage 

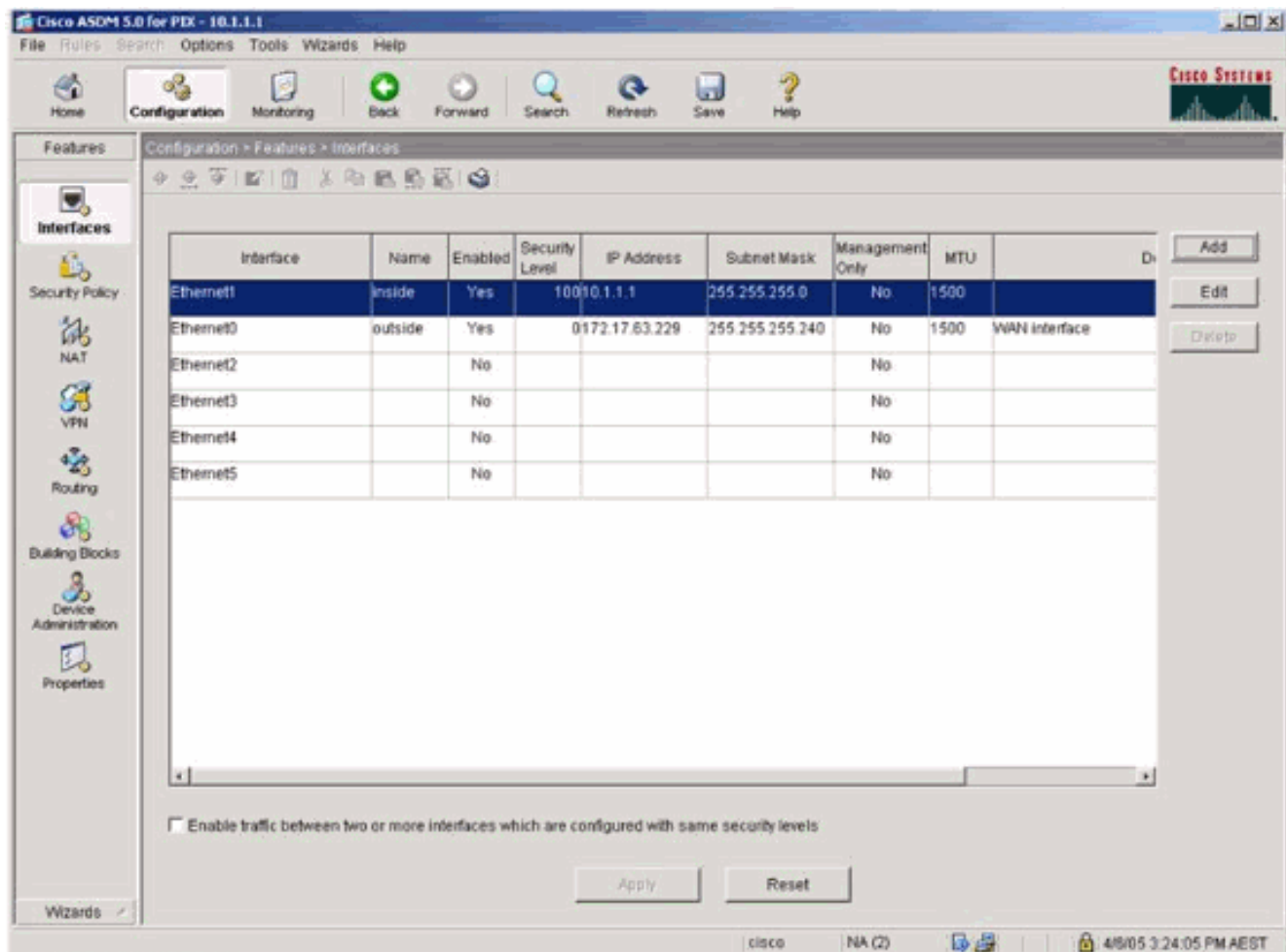
'inside' Interface Traffic Usage (Kbps) 

Latest ASDM Syslog Messages

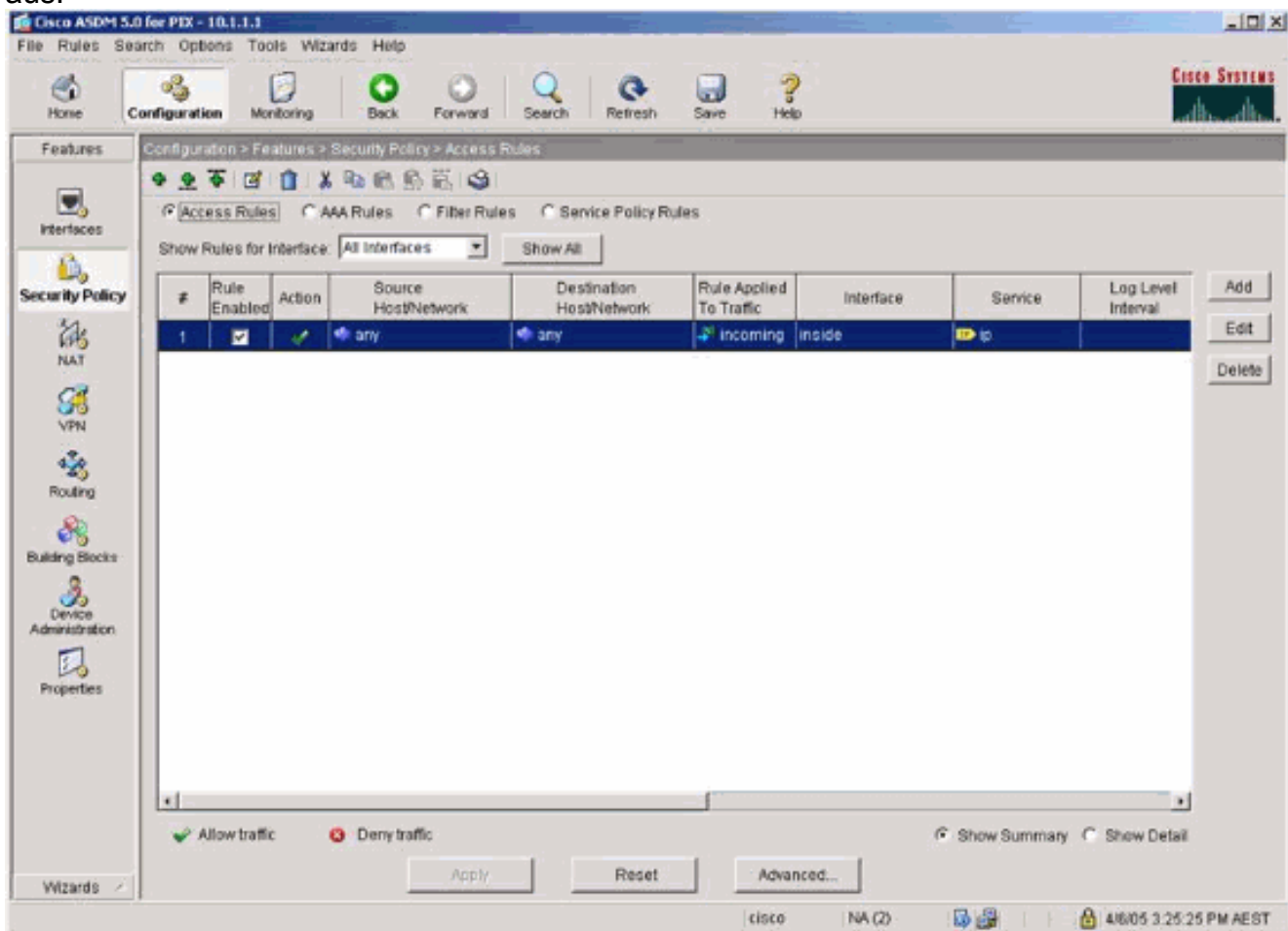
-- Syslog Disabled --

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

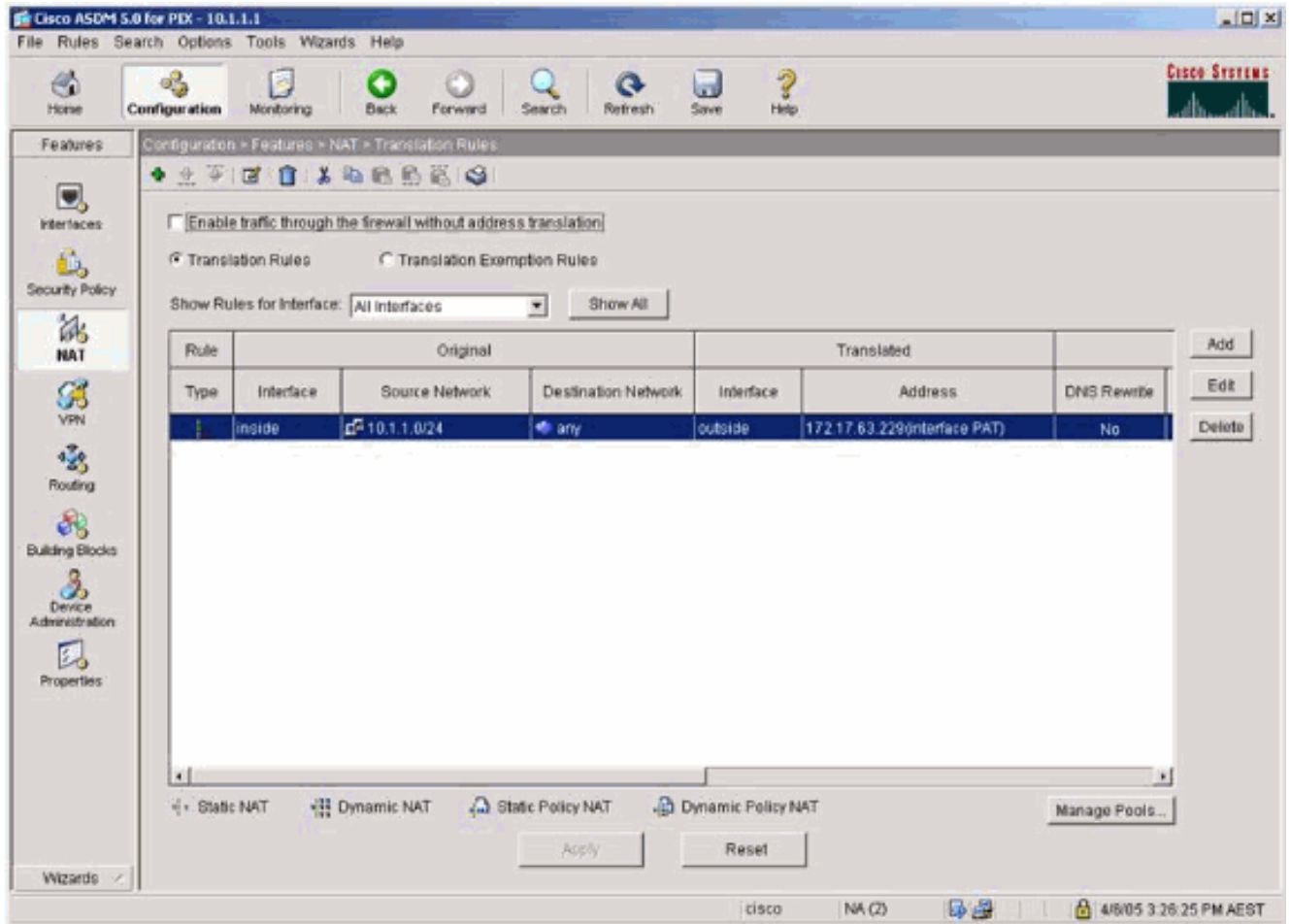
- Wählen Sie **Konfiguration > Funktionen > Schnittstellen** aus, und wählen Sie **Add** für neue Schnittstellen oder **Edit** für eine vorhandene Konfiguration aus.



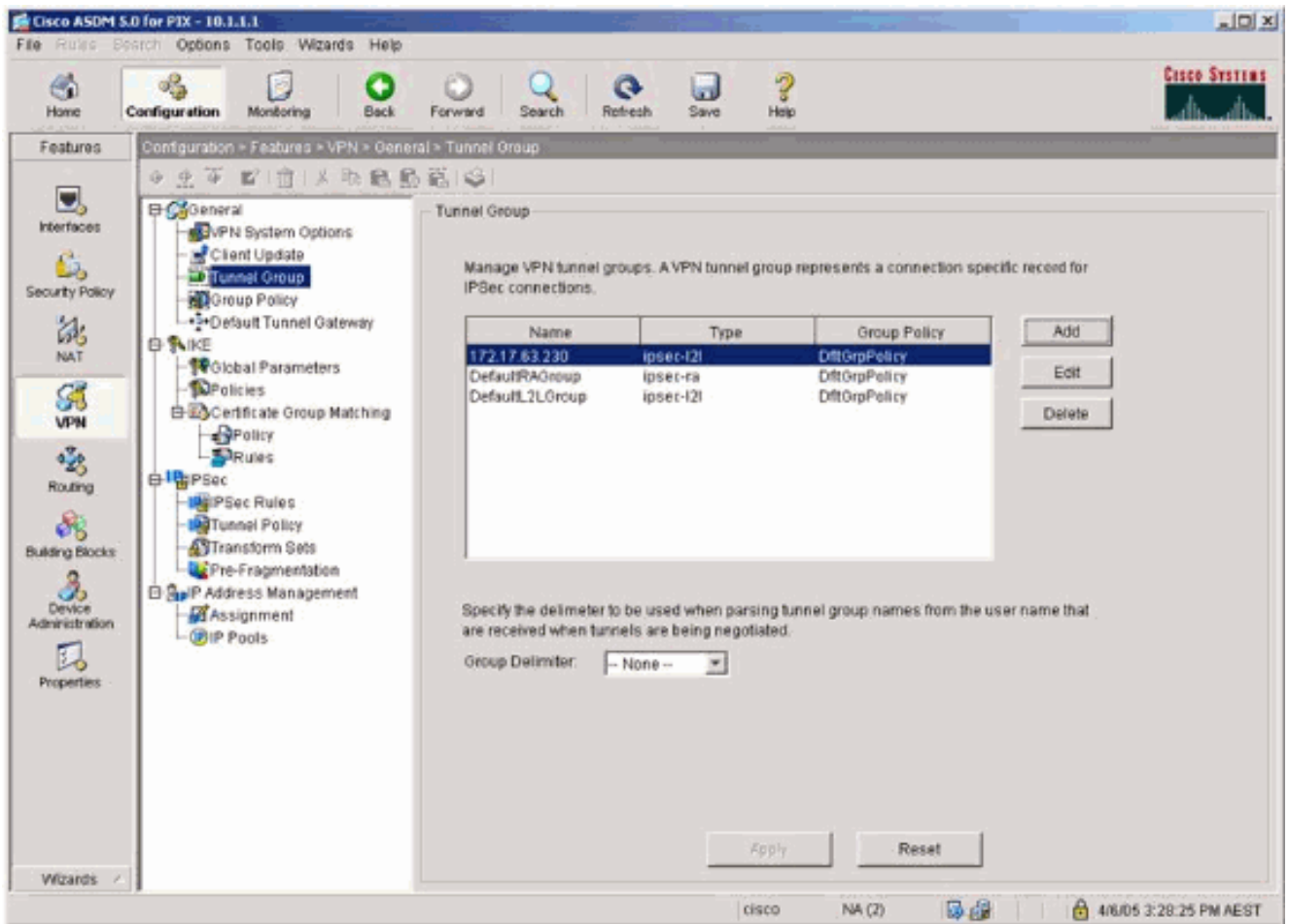
3. Wählen Sie die Sicherheitsoptionen für die interne Schnittstelle aus.



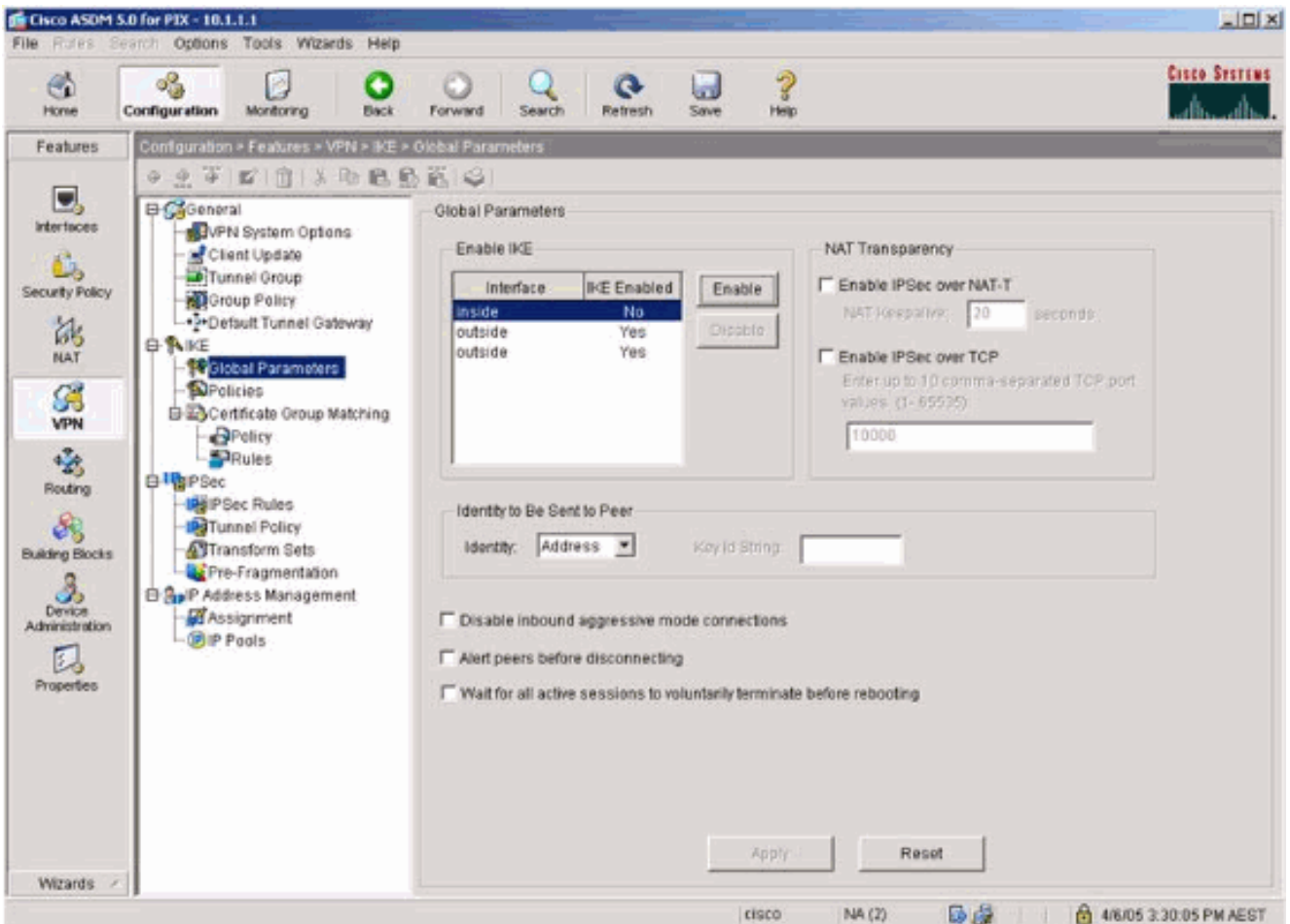
4. In der NAT-Konfiguration ist der verschlüsselte Datenverkehr von der NAT ausgenommen, und der gesamte andere Datenverkehr ist NAT/PAT zur externen Schnittstelle.



5. Wählen Sie VPN >Allgemein > Tunnelgruppe aus, und aktivieren Sie eine Tunnelgruppe.

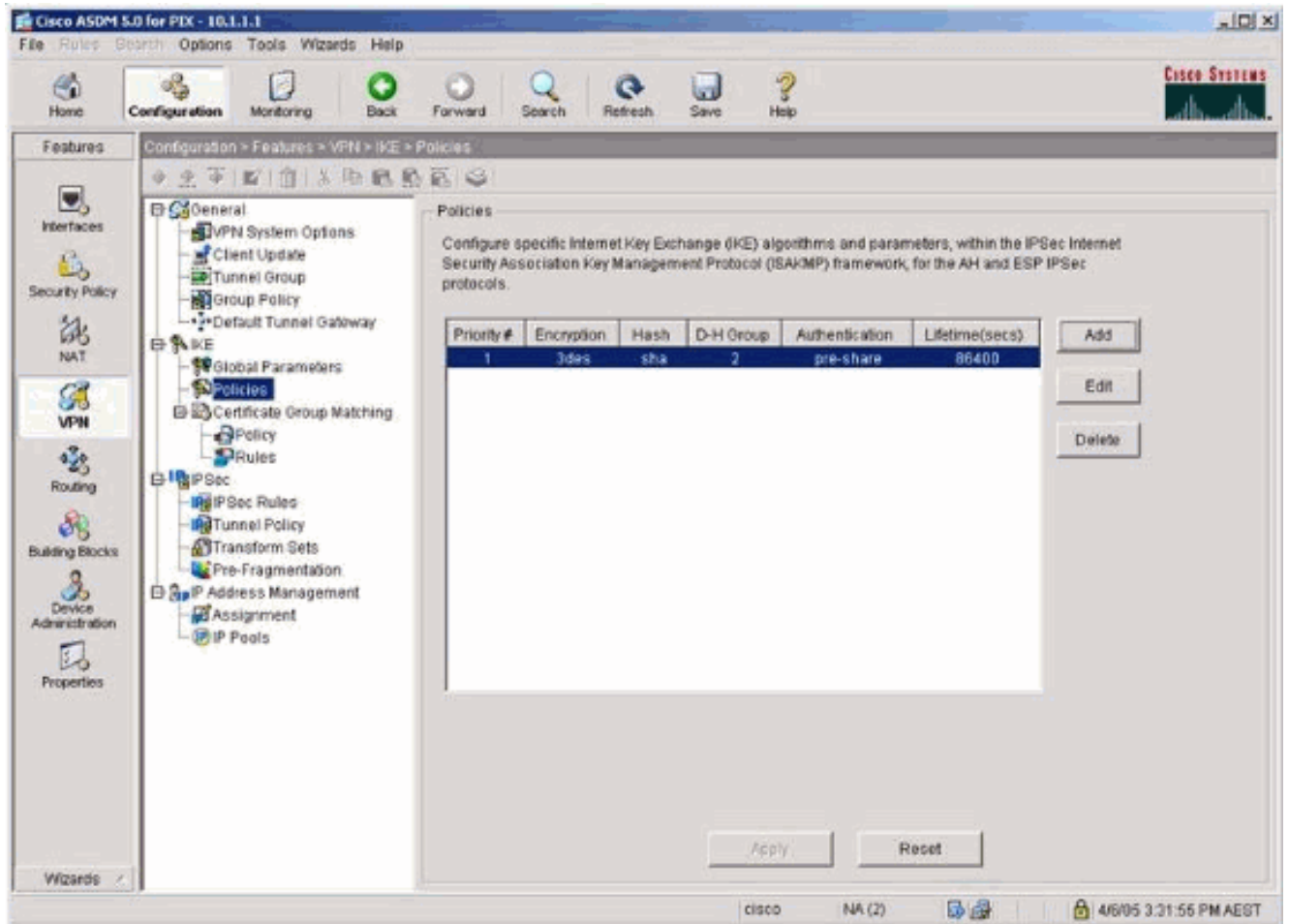


6. Wählen Sie VPN > IKE > Globale Parameter aus, und aktivieren Sie IKE auf der externen Schnittstelle.

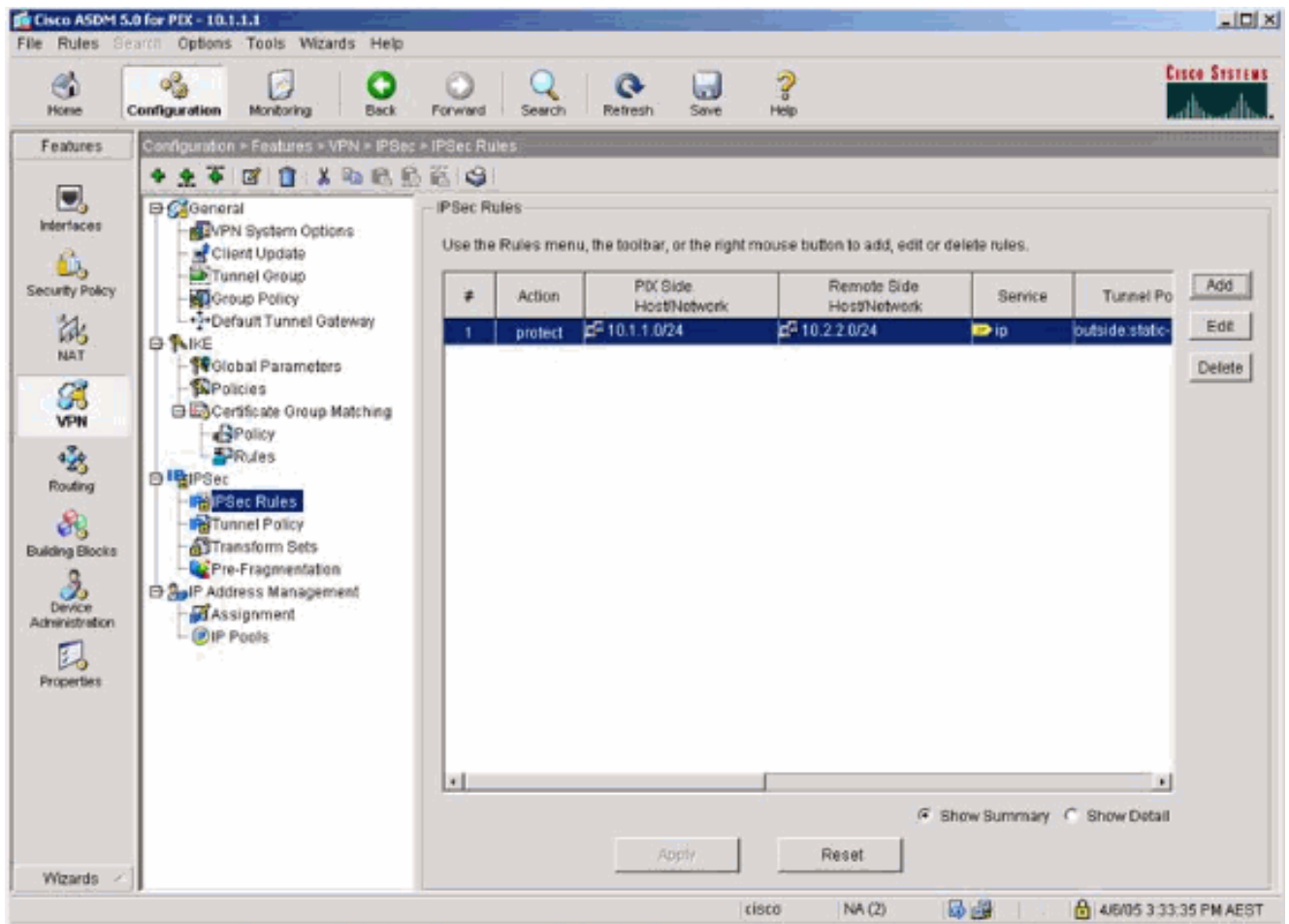


7. Wählen Sie VPN > IKE > Policies (VPN > IKE > Richtlinien) und wählen Sie die IKE-

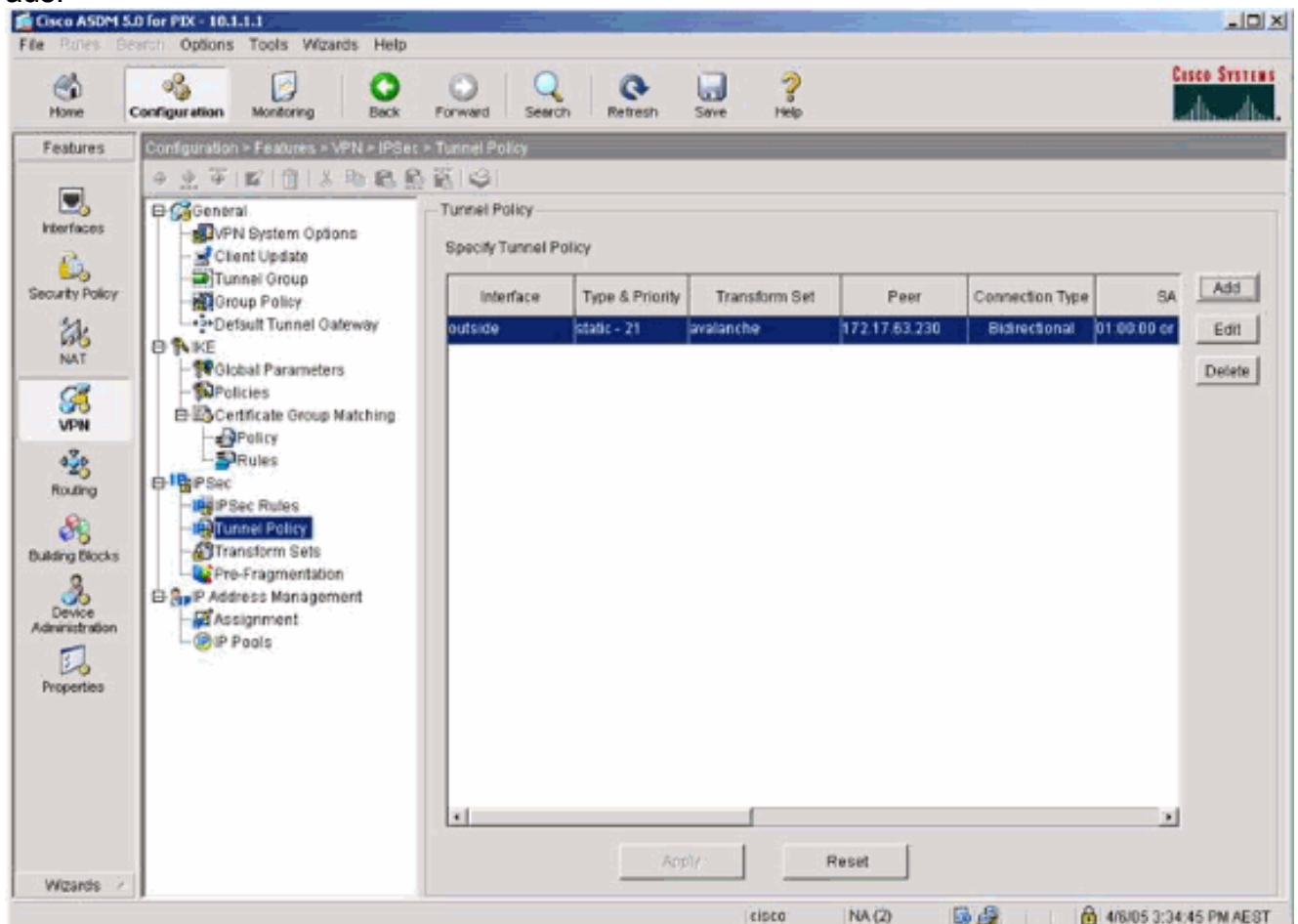
Richtlinien
aus.



8. Wählen Sie VPN > IPsec > IPsec > IPsec Rules und wählen Sie IPsec für die lokale Tunnel- und Remote-Adressierung aus.

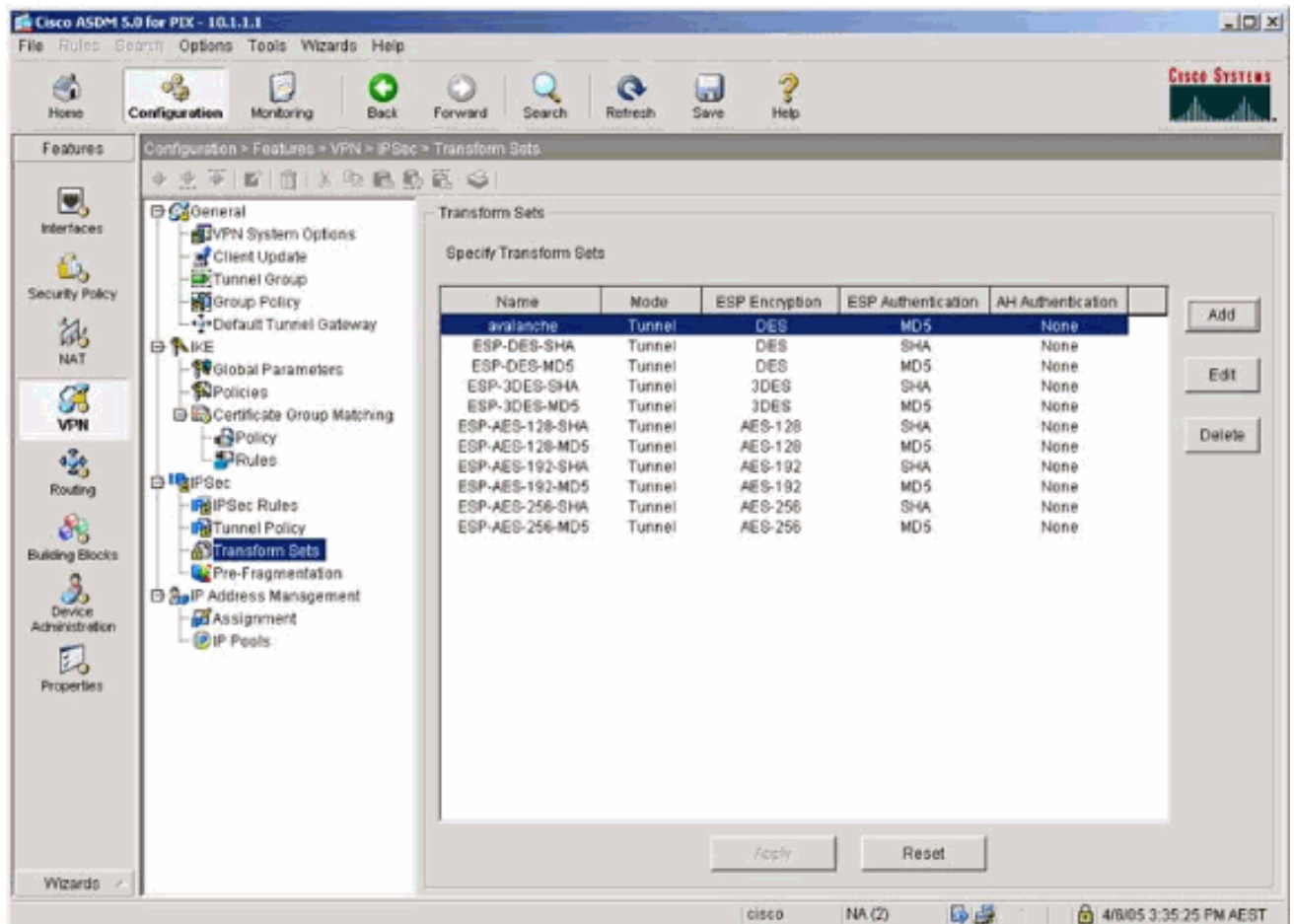


9. Wählen Sie VPN > IPsec > Tunnel Policy aus, und wählen Sie die Tunnelrichtlinie aus.

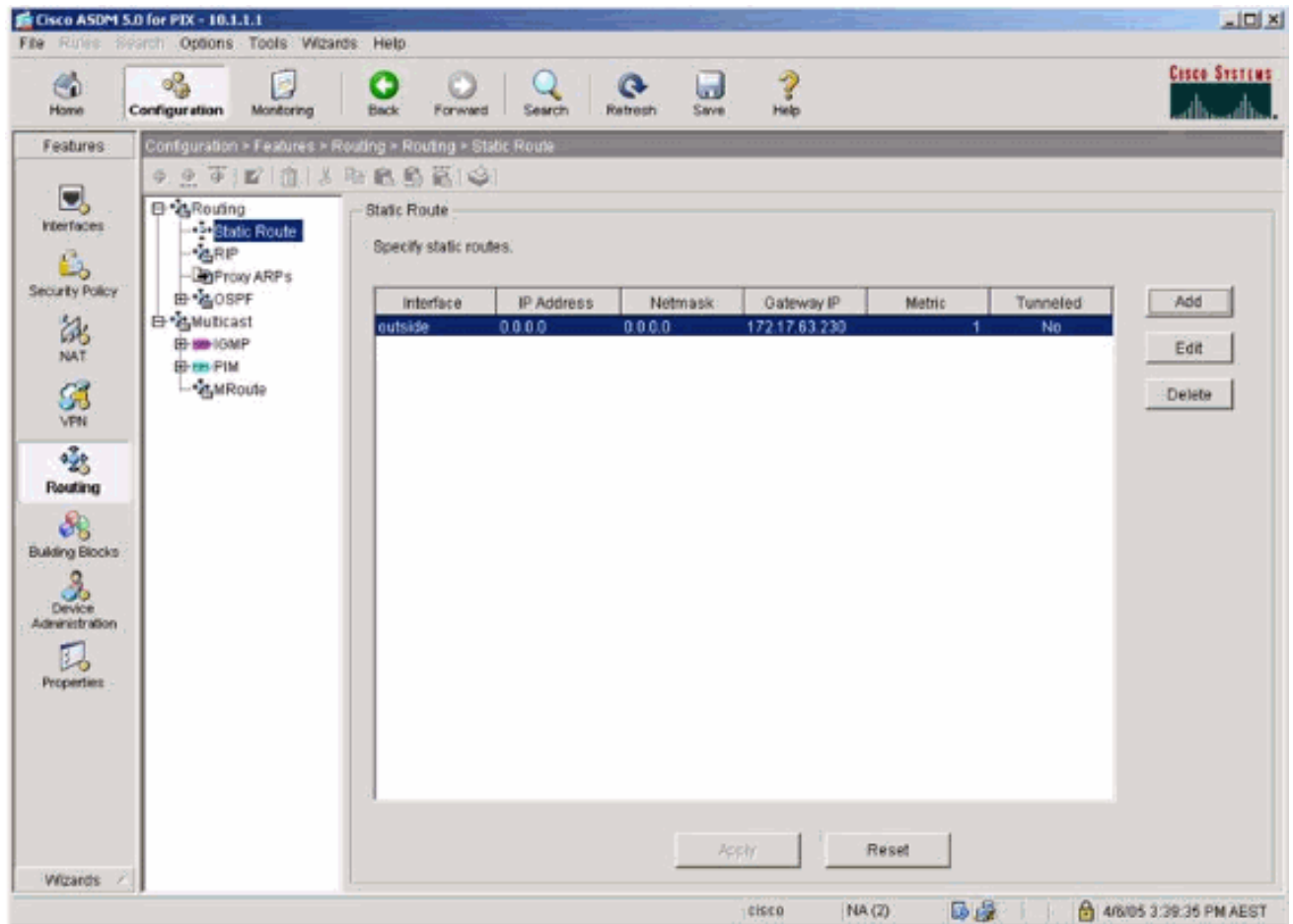


10. Wählen Sie VPN > IPsec > Transform Sets und wählen Sie einen Transform Set

aus.



11. Wählen Sie **Routing > Routing > Statische Route aus**, und wählen Sie eine statische Route zum Gateway-Router aus. In diesem Beispiel verweist die statische Route aus Gründen der Einfachheit auf den Remote-VPN-Peer.



Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des Befehls show** anzuzeigen.

- **show crypto ipsec sa** - Zeigt die Sicherheitszuordnungen für Phase 2 an.
- **show crypto isakmp sa** - Zeigt die Sicherheitszuordnungen für Phase 1 an.

Fehlerbehebung

Sie können ASDM verwenden, um die Protokollierung zu aktivieren und die Protokolle anzuzeigen.

- Wählen Sie **Konfiguration > Eigenschaften > Protokollierung > Protokollierung Setup**, wählen Sie **Protokollierung aktivieren aus**, und klicken Sie auf **Übernehmen**, um die Protokollierung zu aktivieren.
- Wählen Sie **Monitoring > Logging > Log Buffer > On Logging Level aus**, wählen Sie **Logging Buffer aus**, und klicken Sie auf **View**, um die Protokolle anzuzeigen.

Befehle zur Fehlerbehebung

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle.

Verwenden Sie das OIT, um eine Analyse der **Ausgabe des Befehls show** anzuzeigen.

Hinweis: Beachten Sie [vor der](#) Verwendung von **Debug**-Befehlen die [Informationen](#) zu [Debug-Befehlen](#).

- **debug crypto ipsec** - Zeigt die IPsec-Aushandlungen für Phase 2.
- **debug crypto isakmp** - Zeigt die ISAKMP-Verhandlungen für Phase 1.
- **debug crypto engine** - Zeigt den verschlüsselten Datenverkehr an.
- **clear crypto isakmp**: Löscht die Sicherheitszuordnungen für Phase 1.
- **clear crypto sa**: Löscht die Sicherheitszuordnungen für Phase 2.
- **debug icmp trace** - Zeigt, ob ICMP-Anfragen von den Hosts den PIX erreichen. Sie müssen den Befehl **access-list** hinzufügen, um ICMP in der Konfiguration zuzulassen, damit dieses Debuggen ausgeführt werden kann.
- **logging buffer debugging** - Zeigt Verbindungen an, die hergestellt und Hosts verweigert werden, die den PIX durchlaufen. Die Informationen werden im PIX-Protokollpuffer gespeichert, und die Ausgabe wird mit dem Befehl **show log** angezeigt.

Zugehörige Informationen

- [Häufigste L2L- und Remote Access IPSec VPN-Lösungen zur Fehlerbehebung](#)
- [Cisco PIX Firewall-Software](#)
- [Cisco Secure PIX Firewall - Befehlsreferenzen](#)
- [Problemhinweise zu Sicherheitsprodukten \(einschließlich PIX\)](#)
- [Anforderungen für Kommentare \(RFCs\)](#)