

ASA/PIX - Configurazione di un tunnel IPsec da LAN a LAN per router Cisco IOS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione con ASDM](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene illustrato come configurare un tunnel IPsec da PIX Security Appliance 7.x e versioni successive o da Adaptive Security Appliance (ASA) con una rete interna su un router 2611 con immagine crittografica. Le route statiche vengono utilizzate per maggiore semplicità.

Per ulteriori informazioni sulla configurazione del tunnel tra una rete LAN e una rete LAN, fare riferimento a [Configurazione di IPsec - Da router a PIX](#).

Per ulteriori informazioni sulla configurazione del tunnel IPsec tra Cisco VPN 3000 Concentrator e Cisco VPN 3000 Concentrator, fare riferimento a [Esempio di configurazione del tunnel IPsec LAN-LAN tra PIX Firewall e Cisco VPN 3000 Concentrator](#).

Per ulteriori informazioni sullo scenario in cui il tunnel LAN-LAN è posizionato tra il PIX e il concentratore VPN, fare riferimento all'[esempio di configurazione](#) del [tunnel IPsec tra](#) il PIX e il concentratore VPN.

Per ulteriori informazioni sullo scenario in cui il tunnel LAN-LAN tra i PIX consente anche a un client VPN di accedere al PIX spoke tramite il PIX dell'hub, fare riferimento all'[esempio di configurazione](#) dell'[autenticazione TACACS+ 7.x Enhanced Spoke-to-Client VPN](#) con autenticazione TACACS+.

Per ulteriori informazioni, fare riferimento al documento [SDM: Esempio di VPN IPsec da sito a sito](#)

[tra ASA/PIX e un router IOS](#) per ulteriori informazioni sullo stesso scenario in cui la versione software della appliance di sicurezza PIX/ASA è 8.x.

Per ulteriori informazioni, fare riferimento al documento [Configuration Professional: Esempio di VPN IPsec da sito a sito tra ASA/PIX e un router IOS](#) Per ulteriori informazioni sullo stesso scenario in cui la configurazione relativa all'ASA viene mostrata utilizzando l'interfaccia GUI di ASDM e la configurazione relativa al router viene mostrata utilizzando l'interfaccia GUI del Cisco TCP.

[Prerequisiti](#)

[Requisiti](#)

Nessun requisito specifico previsto per questo documento.

[Componenti usati](#)

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- PIX-525 con software PIX versione 7.0
- Router Cisco 2611 con software Cisco IOS® versione 12.2(15)T13

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

[Convenzioni](#)

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

[Premesse](#)

Sul PIX, i comandi **access-list** e **nat 0** funzionano insieme. Quando un utente della rete 10.1.1.0 passa alla rete 10.2.2.0, l'elenco degli accessi viene utilizzato per consentire la crittografia del traffico di rete 10.1.1.0 senza NAT (Network Address Translation). Sul router, i comandi **route-map** e **access-list** vengono usati per consentire il traffico di rete 10.2.2.0 da crittografare senza NAT. Tuttavia, quando gli stessi utenti si spostano altrove, vengono convertiti nell'indirizzo 172.17.63.230 tramite Port Address Translation (PAT).

Questi sono i comandi di configurazione richiesti sulle appliance di sicurezza PIX per *fare in* modo che il traffico *non* passi attraverso PAT sul tunnel e il traffico verso Internet per passare attraverso 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
```

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Questi esempi di configurazione sono relativi all'interfaccia della riga di comando. Se si preferisce configurare l'uso di ASDM, vedere la sezione [Configurazione con Adaptive Security Device Manager \(ASDM\)](#) di questo documento.

- [PIX sede centrale](#)
- [Router per filiali](#)

PIX sede centrale

```
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 per filiali

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

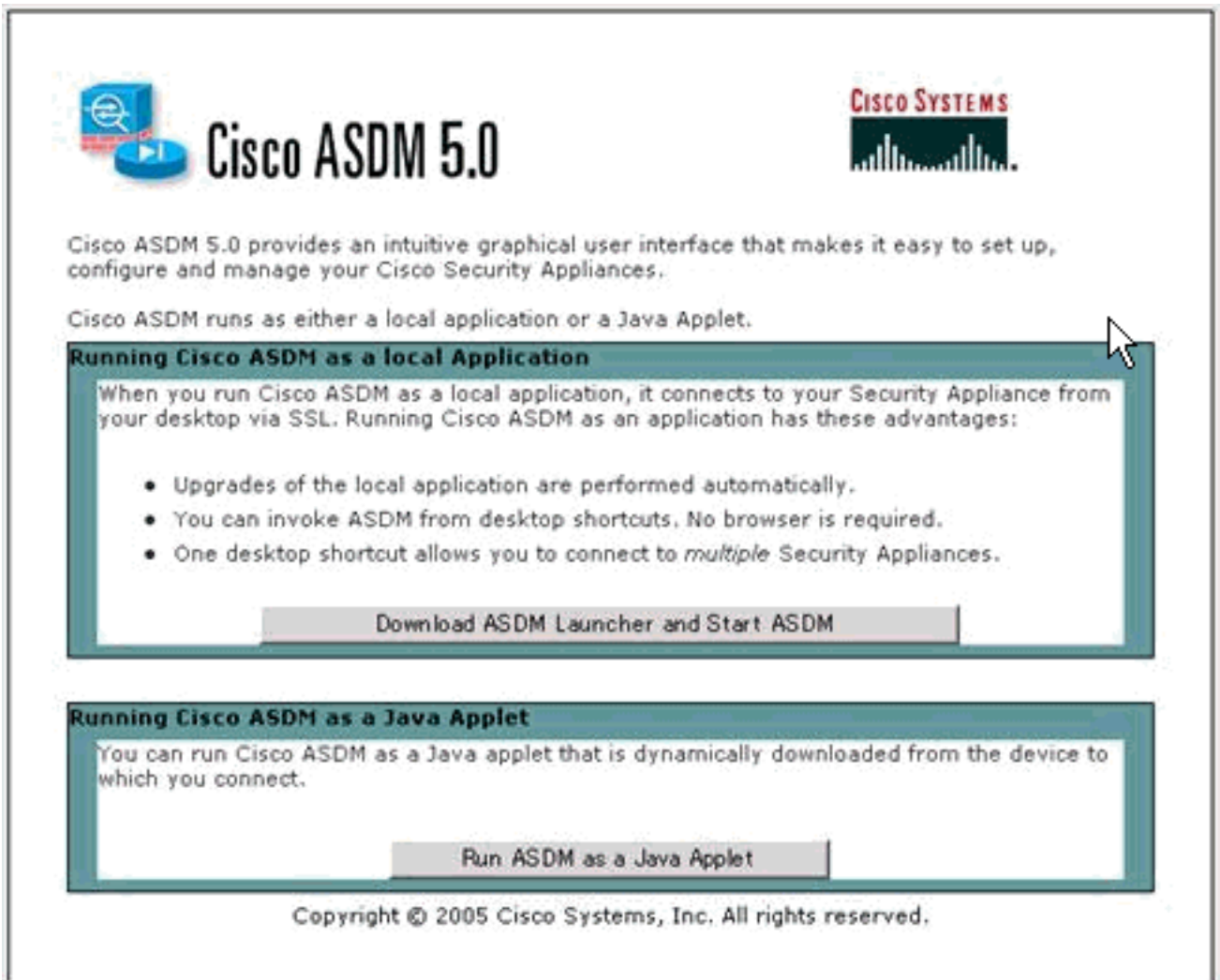
```
!  
no voice hpi capture buffer  
no voice hpi capture destination  
!  
!  
mta receive maximum-recipients 0  
!  
!  
!  
!  
interface Ethernet0/0  
ip address 172.17.63.230 255.255.255.240  
ip nat outside  
no ip route-cache  
no ip mroute-cache  
half-duplex  
crypto map nolan  
!  
interface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

Configurazione con ASDM

Nell'esempio viene mostrato come configurare il PIX con l'interfaccia grafica ASDM. Un PC con browser e indirizzo IP 10.1.1.2 è collegato all'interfaccia interna e1 del PIX. Assicurarsi che sia abilitato http sul PIX.

Questa procedura mostra la configurazione ASDM del PIX della sede centrale.

1. Collegare il PC al PIX e scegliere un metodo di download.



The screenshot shows the Cisco ASDM 5.0 installation wizard. At the top left is the ASDM logo, and at the top right is the Cisco Systems logo. Below the logos, there is a descriptive paragraph about the software. The main content is divided into two sections, each with a title and a button:

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.

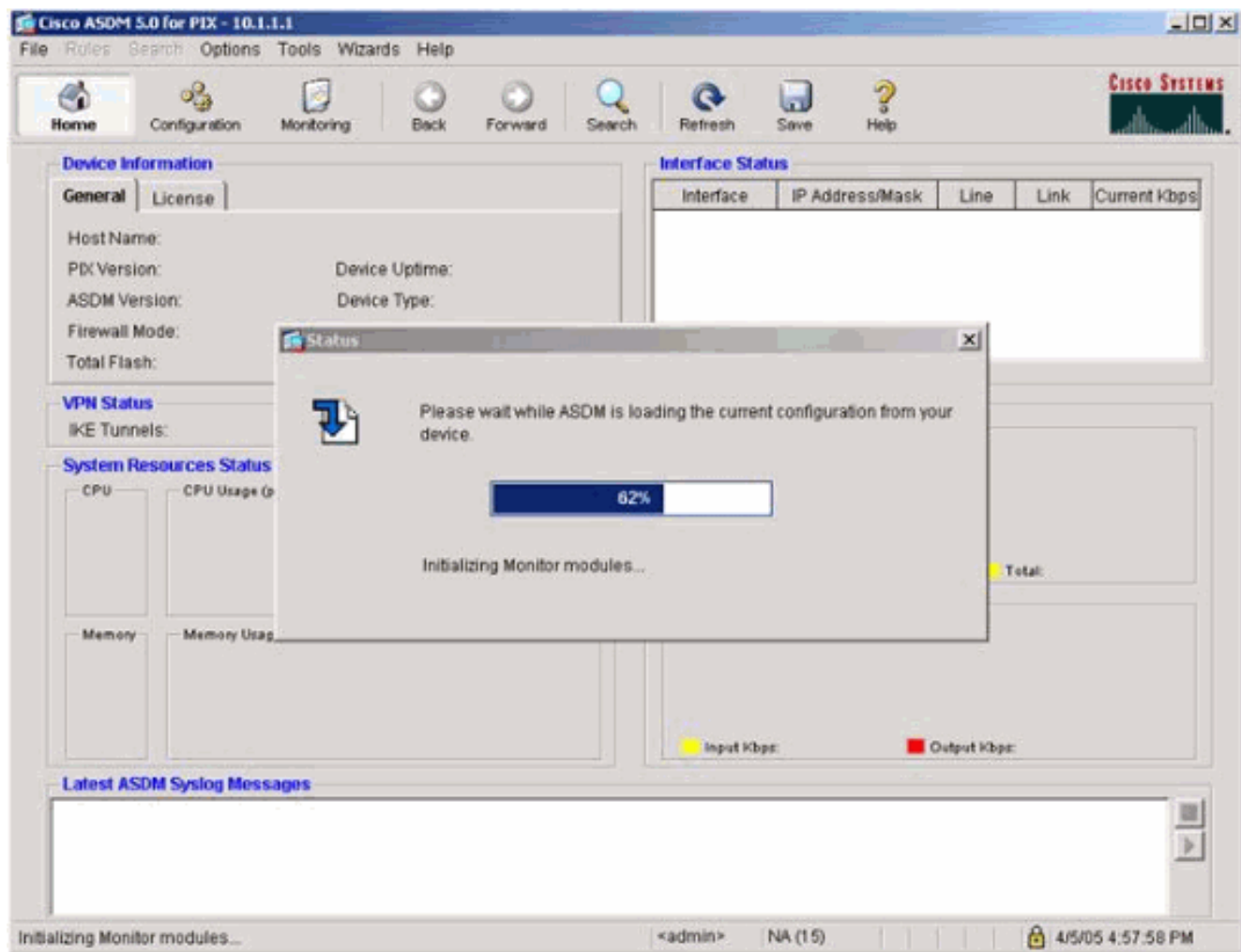
[Download ASDM Launcher and Start ASDM](#)

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 carica la configurazione esistente dal PIX.



Questa finestra fornisce strumenti e menu di controllo.

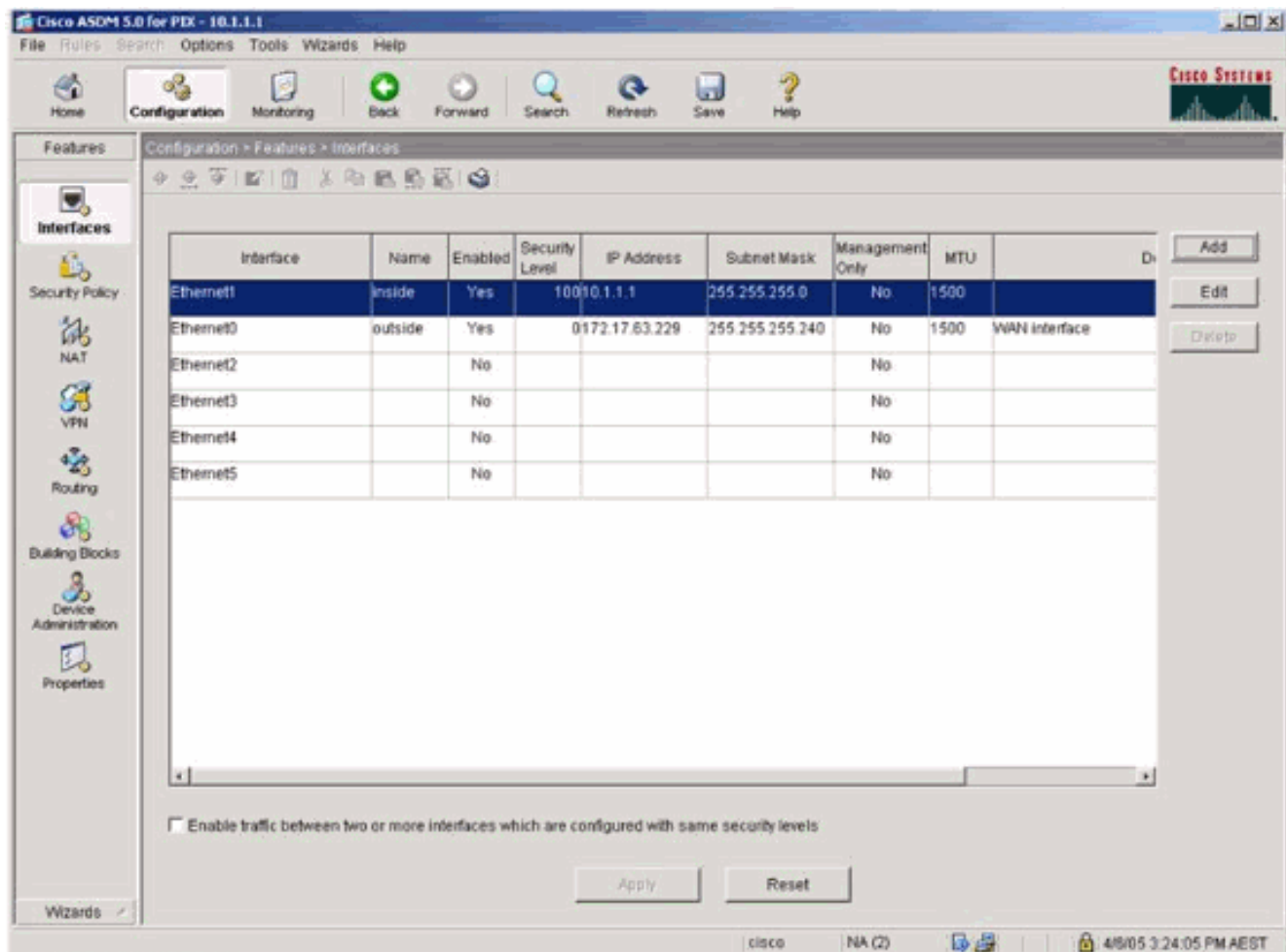
The screenshot displays the Cisco ASDM 5.0 for PIX - 10.1.1.1 interface. The main content is divided into several sections:

- 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:**

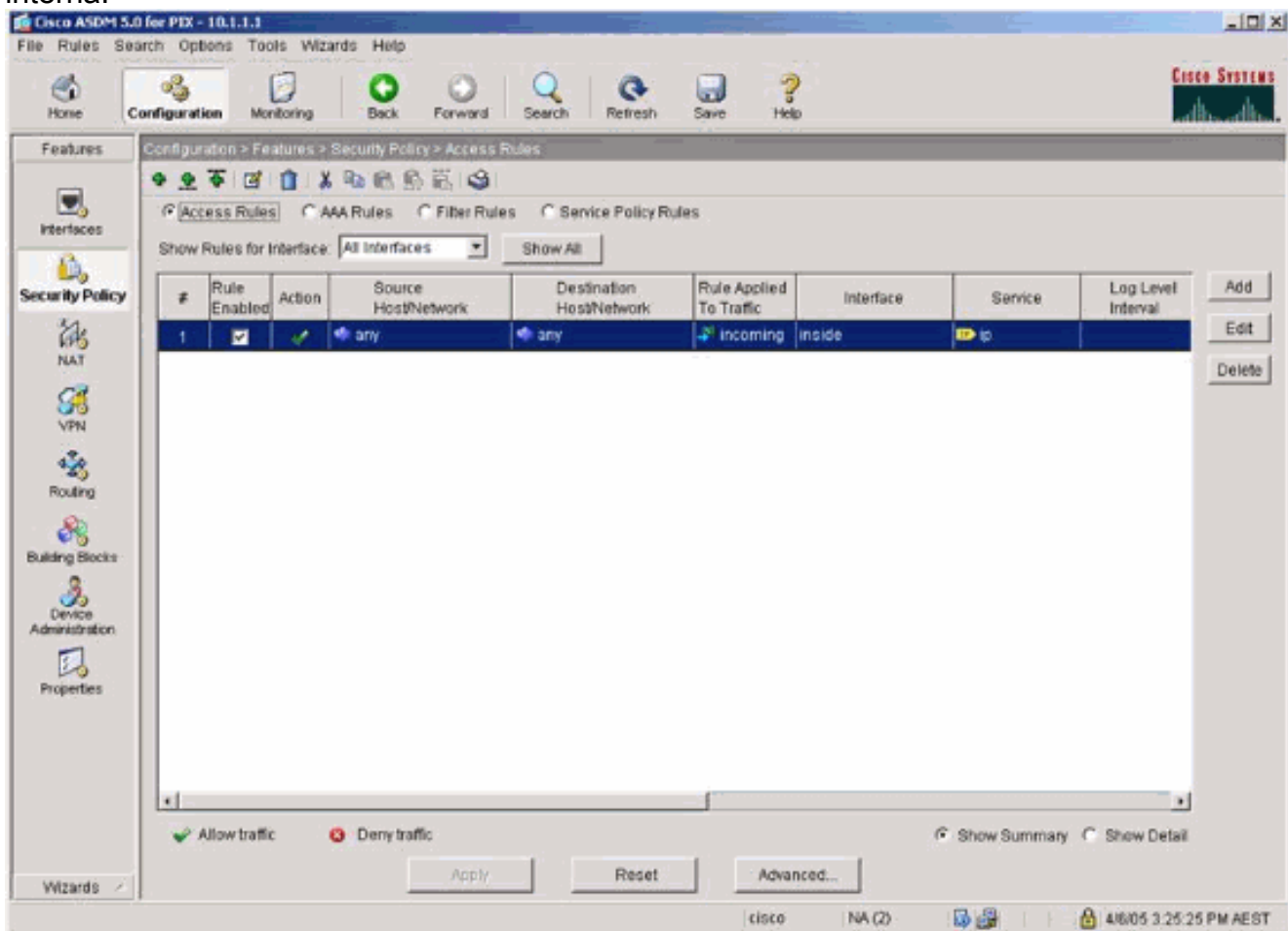
Interface	IP Address/Mask	Line	Link	Current Kbps
inside	10.1.1.1/24	up	up	1
- VPN Status:** IKE Tunnels: 0, IPsec Tunnels: 0.
- System Resources Status:**
 - CPU: 0% (04:57:46), CPU Usage (percent) graph showing 0% usage.
 - Memory: 67MB (04:57:46), Memory Usage (MB) graph showing 67MB usage.
- Traffic 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 --

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

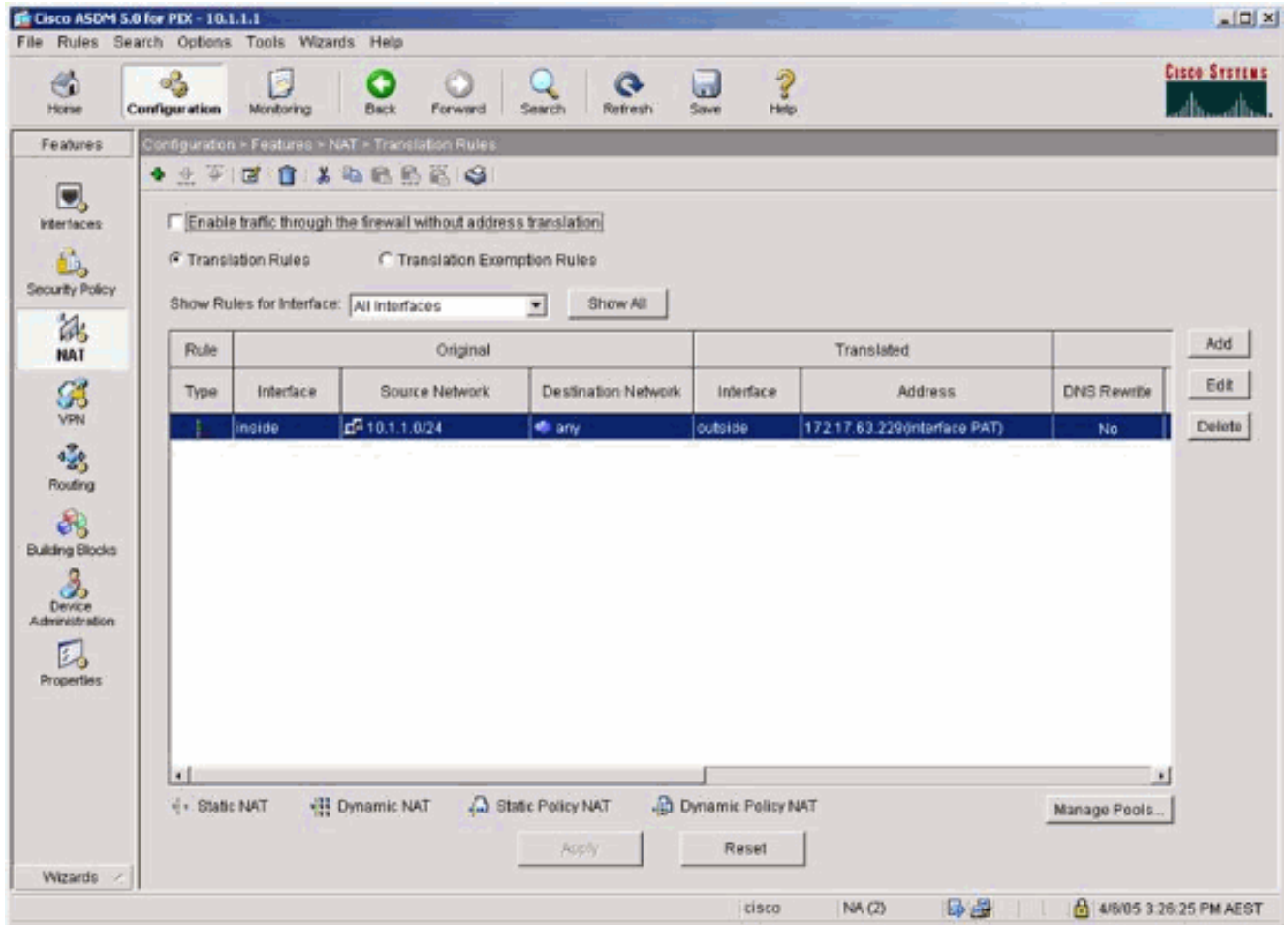
2. Selezionare **Configurazione > Funzionalità > Interfacce** e selezionare **Aggiungi** per le nuove interfacce o **Modifica** per una configurazione esistente.



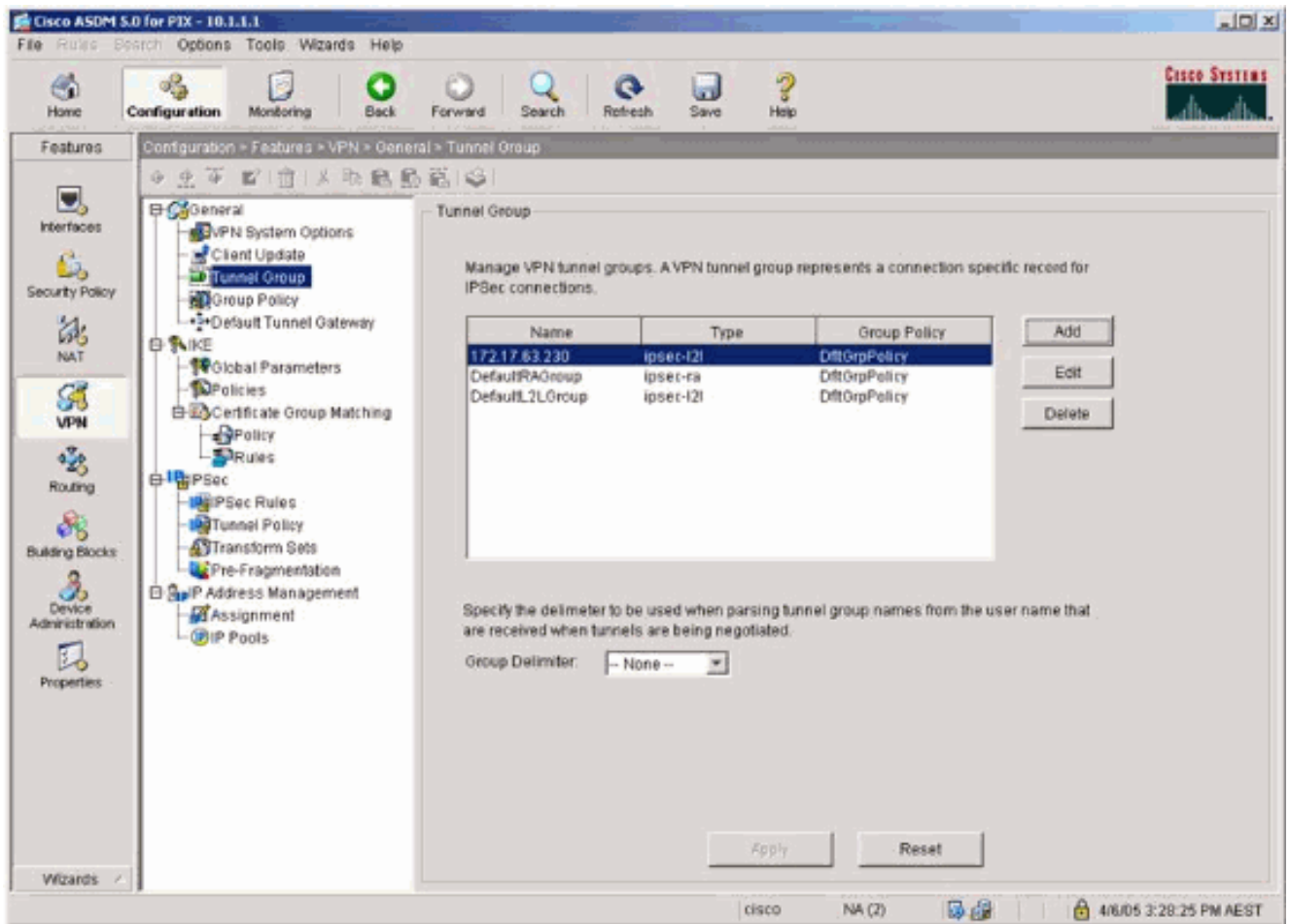
3. Selezionare le opzioni di protezione per l'interfaccia interna.



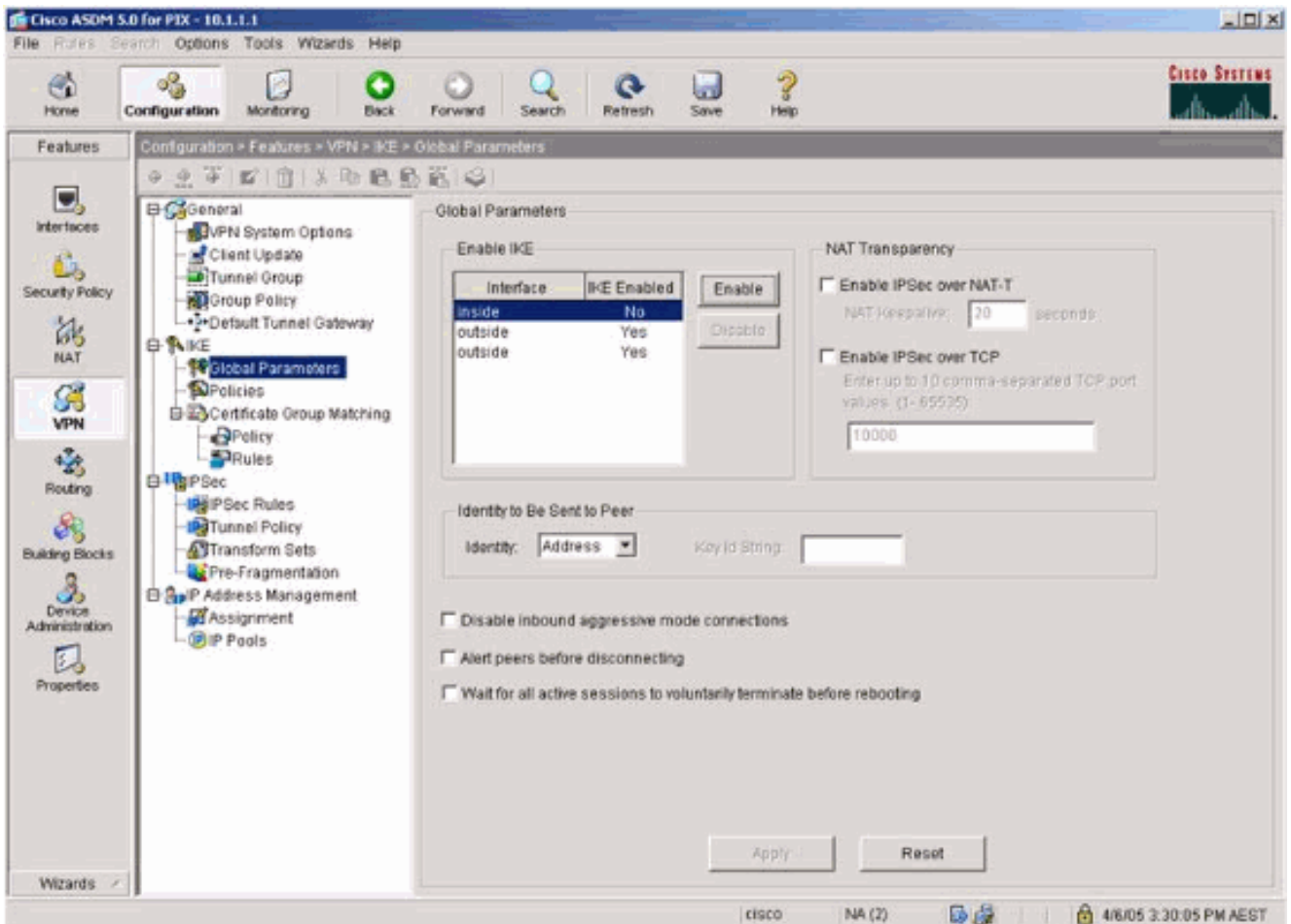
4. Nella configurazione NAT, il traffico crittografato è esente da NAT e tutto il resto del traffico è NAT/PAT verso l'interfaccia esterna.



5. Selezionare VPN > Generale > Gruppo di tunnel e abilitare un gruppo di tunnel



6. Selezionare VPN > IKE > Global Parameters e abilitare IKE sull'interfaccia esterna.



7. Selezionare VPN > IKE > Policy e scegliere le policy

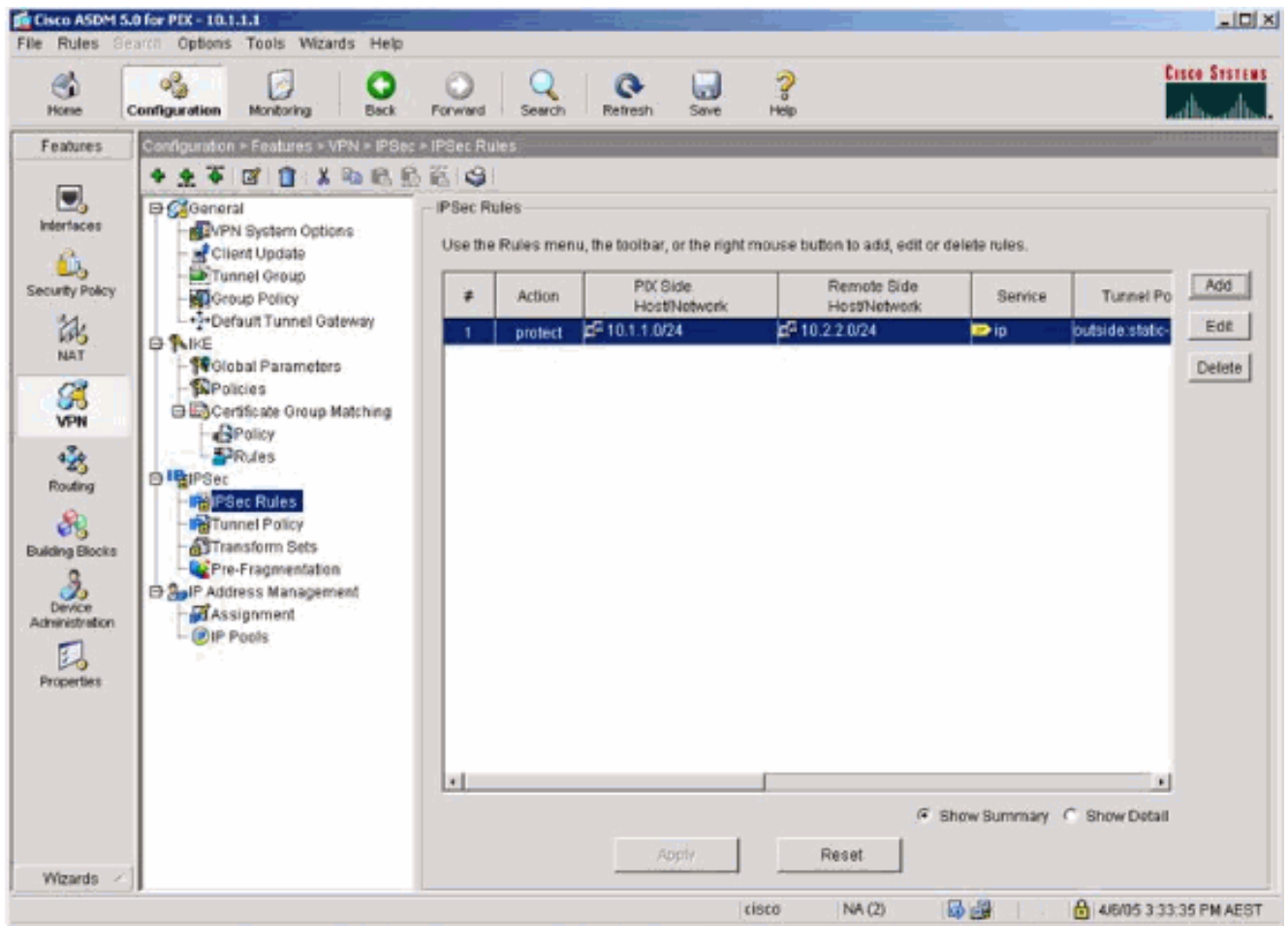
IKE.

The screenshot shows the Cisco ASDM 5.0 for PDK - 10.1.1.1 interface. The left sidebar contains a tree view of configuration categories, with 'VPN' expanded to show 'IKE' and 'IPSec'. The main pane displays the 'Policies' configuration page for IKE. The page title is 'Policies' and the description reads: 'Configure specific Internet Key Exchange (IKE) algorithms and parameters, within the IPSec Internet Security Association Key Management Protocol (ISAKMP) framework, for the AH and ESP IPSec protocols.'

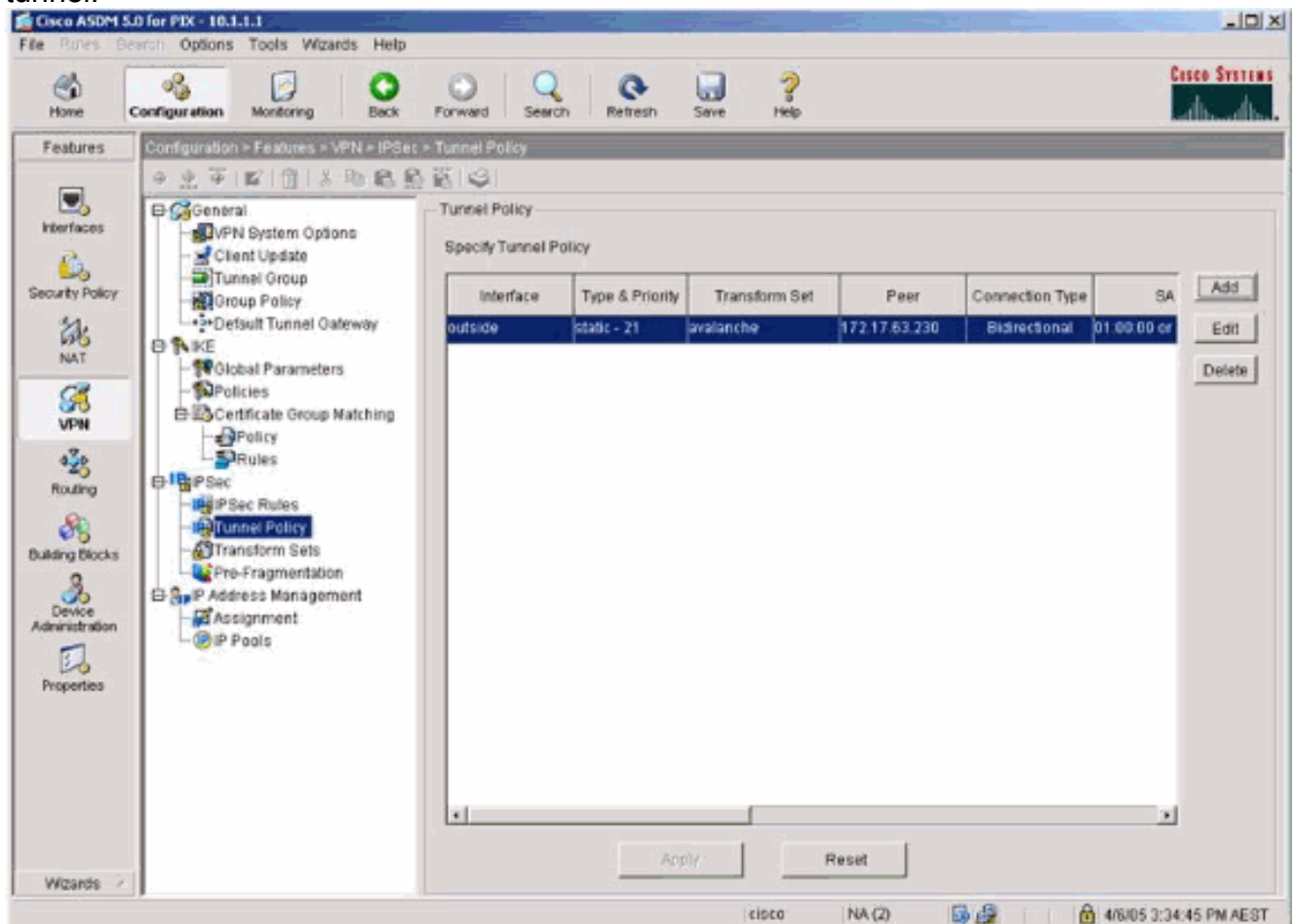
Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime(secs)	
1	3des	sha	2	pre-share	86400	<input type="button" value="Add"/>

Below the table are buttons for 'Edit' and 'Delete'. At the bottom of the main pane are 'Apply' and 'Reset' buttons. The status bar at the bottom shows 'cisco NA (2)' and the time '4/6/05 3:21:55 PM AEST'.

8. Selezionare **VPN > IPsec > Regole IPsec** e scegliere **IPsec** per il tunnel locale e l'indirizzamento remoto.

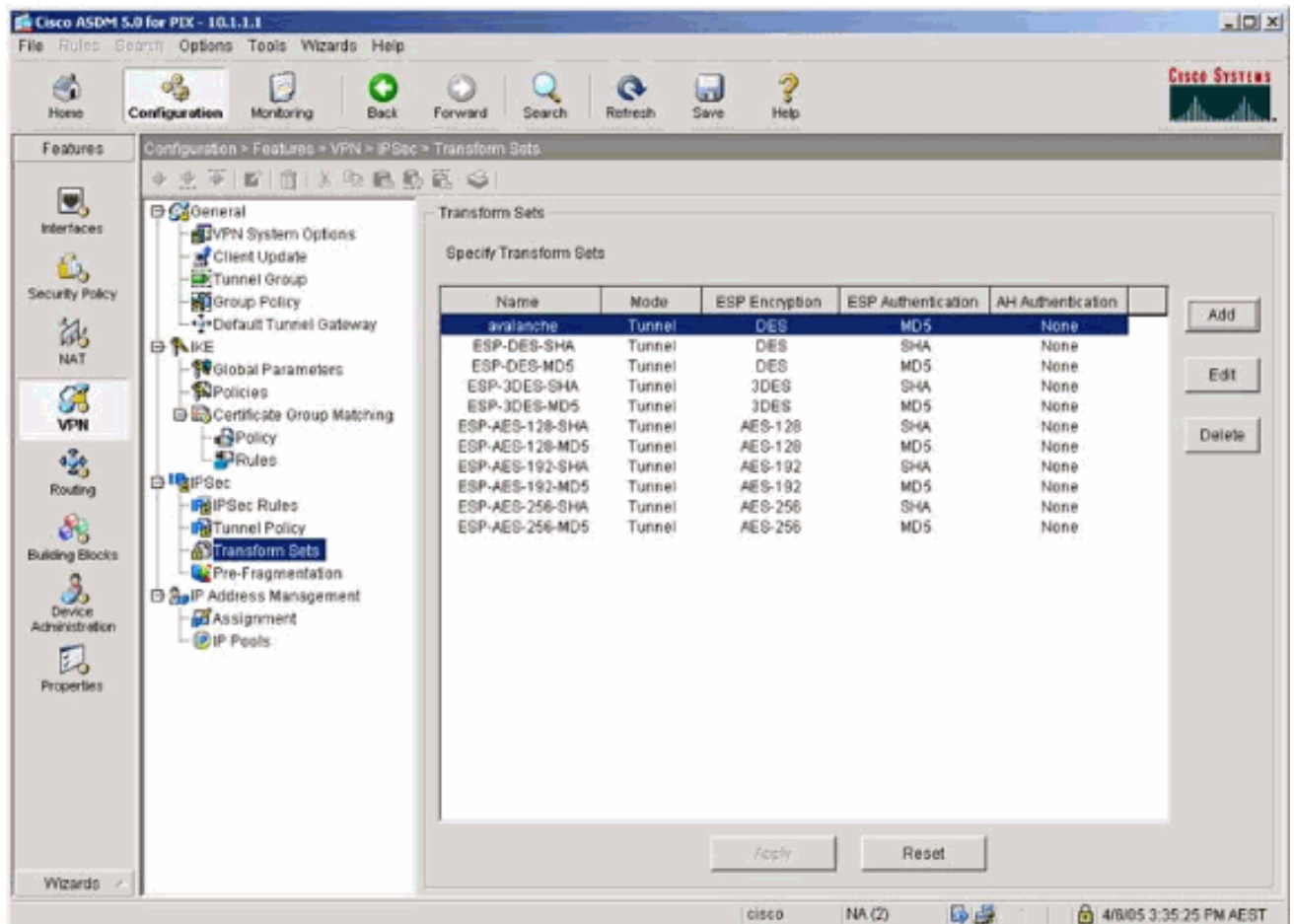


9. Selezionare VPN > IPsec > Criteri tunnel e scegliere il criterio tunnel.

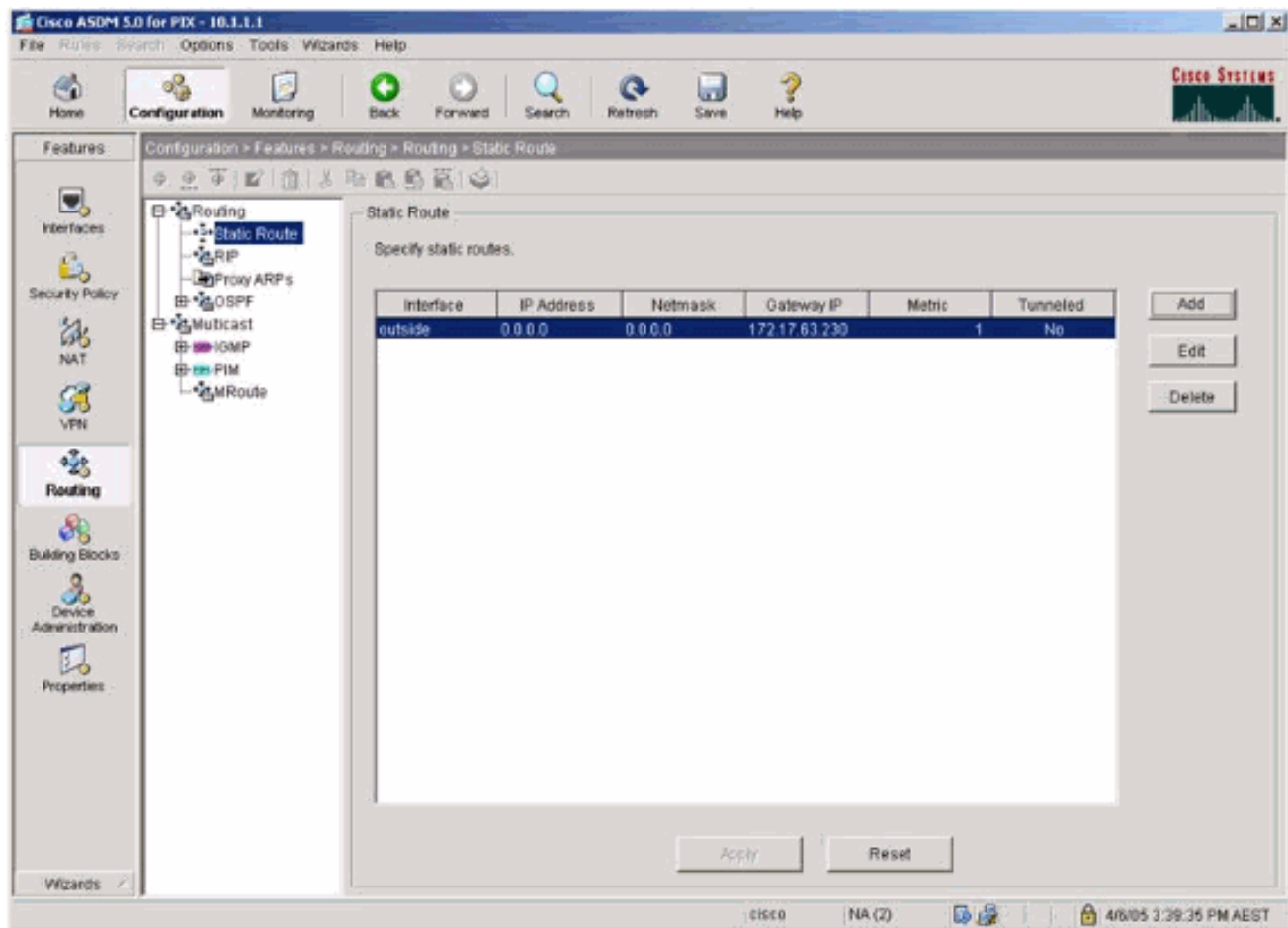


10. Selezionate VPN > IPsec > Set di trasformazioni e scegliete un set di

trasformazioni.



11. Selezionare **Routing > Routing > Static Route** e scegliere una route statica al router gateway. Nell'esempio, il percorso statico punta al peer VPN remoto per semplicità.



Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show crypto ipsec sa**: visualizza le associazioni di sicurezza della fase 2.
- **show crypto isakmp sa**: visualizza le associazioni di sicurezza della fase 1.

Risoluzione dei problemi

È possibile utilizzare ASDM per abilitare il log e visualizzarne i log.

- Selezionare **Configurazione > Proprietà > Registrazione > Impostazione registrazione**, scegliere **Abilita registrazione** e fare clic su **Applica** per abilitare la registrazione.
- Selezionare **Monitoraggio > Log > Buffer di log > Al livello di log**, scegliere **Buffer di log** e fare clic su **Visualizza** per visualizzare i log.

Comandi per la risoluzione dei problemi

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di debug.

- **debug crypto ipsec:** visualizza le negoziazioni IPsec della fase 2.
- **debug crypto isakmp:** visualizza le negoziazioni ISAKMP della fase 1.
- **debug crypto engine:** visualizza il traffico crittografato.
- **clear crypto isakmp:** cancella le associazioni di sicurezza correlate alla fase 1.
- **clear crypto sa:** cancella le associazioni di sicurezza correlate alla fase 2.
- **debug icmp trace:** visualizza se le richieste ICMP dagli host raggiungono il PIX. Per eseguire il debug, è necessario aggiungere il comando **access-list** per autorizzare l'ICMP nella configurazione.
- **logging buffer debugging:** visualizza le connessioni stabilite e negate agli host che passano attraverso il PIX. Le informazioni vengono memorizzate nel buffer di registro PIX e l'output può essere visualizzato con il comando **show log**.

[Informazioni correlate](#)

- [Soluzioni per la risoluzione dei problemi più comuni di VPN IPsec di L2L e ad accesso remoto](#)
- [Software Cisco PIX Firewall](#)
- [Riferimenti per i comandi di Cisco Secure PIX Firewall](#)
- [Avvisi sui prodotti per la sicurezza \(inclusi PIX\)](#)
- [RFC \(Requests for Comments\)](#)