

ASA/PIX : Exemple de configuration d'un dispositif de sécurité sur un tunnel IPsec LAN à LAN avec routeur IOS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration utilisant l'ASDM](#)

[Vérifier](#)

[Dépanner](#)

[Dépannage des commandes](#)

[Informations connexes](#)

[Introduction](#)

Ce document explique comment configurer un tunnel IPsec des dispositifs de sécurité PIX 7.x et plus ou du dispositif de sécurité adaptatif (ASA) avec un réseau interne vers un routeur 2611 qui exécute une image chiffrée. Des routes statiques sont utilisées à des fins de simplicité.

Référez-vous à la [configuration d'IPSec - Routeur à PIX](#) pour plus d'informations sur une configuration de tunnel entre réseaux locaux entre un routeur et le PIX.

Référez-vous au [tunnel d'IPSec d'entre réseaux locaux entre l'exemple de configuration de concentrateur de Cisco VPN 3000 et de Pare-feu PIX](#) pour plus d'informations sur une configuration de tunnel entre réseaux locaux entre le Pare-feu PIX et le concentrateur de Cisco VPN 3000.

Référez-vous au [tunnel d'IPsec entre PIX 7.x et exemple de configuration de concentrateur VPN 3000](#) afin de se renseigner plus sur le scénario où le tunnel entre réseaux locaux est entre le concentrateur PIX et VPN.

Référez-vous au [Rai-à-client amélioré par 7.x VPN PIX/ASA avec l'exemple de configuration d'authentification TACACS+](#) afin de se renseigner plus sur le scénario où le tunnel entre réseaux locaux entre le PIXes tient compte également pour qu'un client vpn accède au rai PIX par le concentrateur PIX.

Référez-vous à [SDM : Site à site IPsec VPN entre ASA/PIX et un exemple de configuration de routeur IOS](#) afin d'apprendre un scénario plus à peu près identique où l'apppliance de Sécurité PIX/ASA exécute la version de logiciel 8.x.

Référez-vous à la [Configuration Professionnel : Le site à site IPsec VPN entre ASA/PIX et un exemple de configuration de routeur IOS](#) afin d'apprendre un scénario plus à peu près identique où la configuration liée à l'ASA est affichée utilisant le GUI ASDM et la configuration liée au routeur est affichée utilisant le GUI de Cisco CP.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- PIX-525 avec la version du logiciel PIX 7.0
- Routeur de Cisco 2611 avec la version de logiciel 12.2(15)T13 de Cisco IOS®

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Informations générales

Sur le PIX, la **liste d'accès** et les commandes **0 nat** fonctionnent ensemble. Quand un utilisateur sur le réseau de 10.1.1.0 va à 10.2.2.0 le réseau, la liste d'accès est utilisée pour permettre le trafic réseau de 10.1.1.0 à chiffrer sans Traduction d'adresses de réseau (NAT). Sur le routeur, le **route-map** et les **commandes access-list** sont utilisés de permettre le trafic réseau de 10.2.2.0 à chiffrer sans NAT. Cependant, quand ces mêmes utilisateurs vont n'importe où ailleurs, ils sont traduits à l'adresse de 172.17.63.230 par la translation d'adresses d'adresse du port (PAT).

Ce sont les commandes de configuration exigées sur les dispositifs de sécurité PIX afin du trafic pour ne pas s'exécuter par PAT au-dessus du tunnel, et trafiquent à l'Internet pour s'exécuter par 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
```

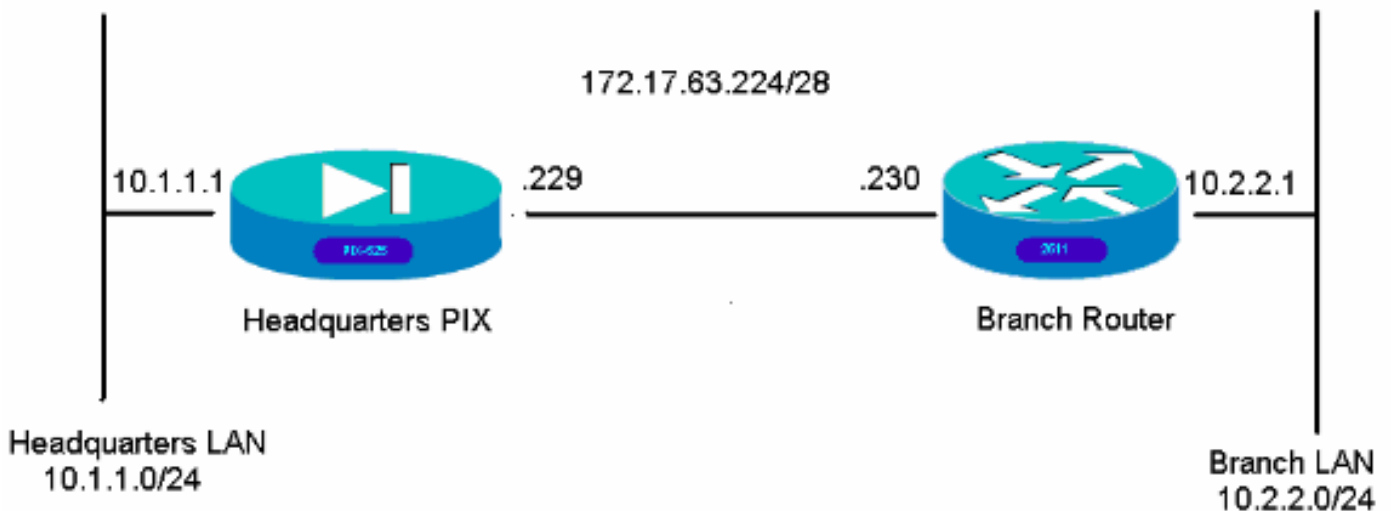
Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil [Command Lookup Tool](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ces exemples de configuration sont pour l'interface de ligne de commande. Voyez la [configuration utilisant la section d'Adaptive Security Device Manager \(ASDM\) de](#) ce document si vous préférez configurer utilisant l'ASDM.

- [Sièges sociaux PIX](#)
- [Routeur secondaire](#)

Sièges sociaux 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 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#
```

Routeur secondaire

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

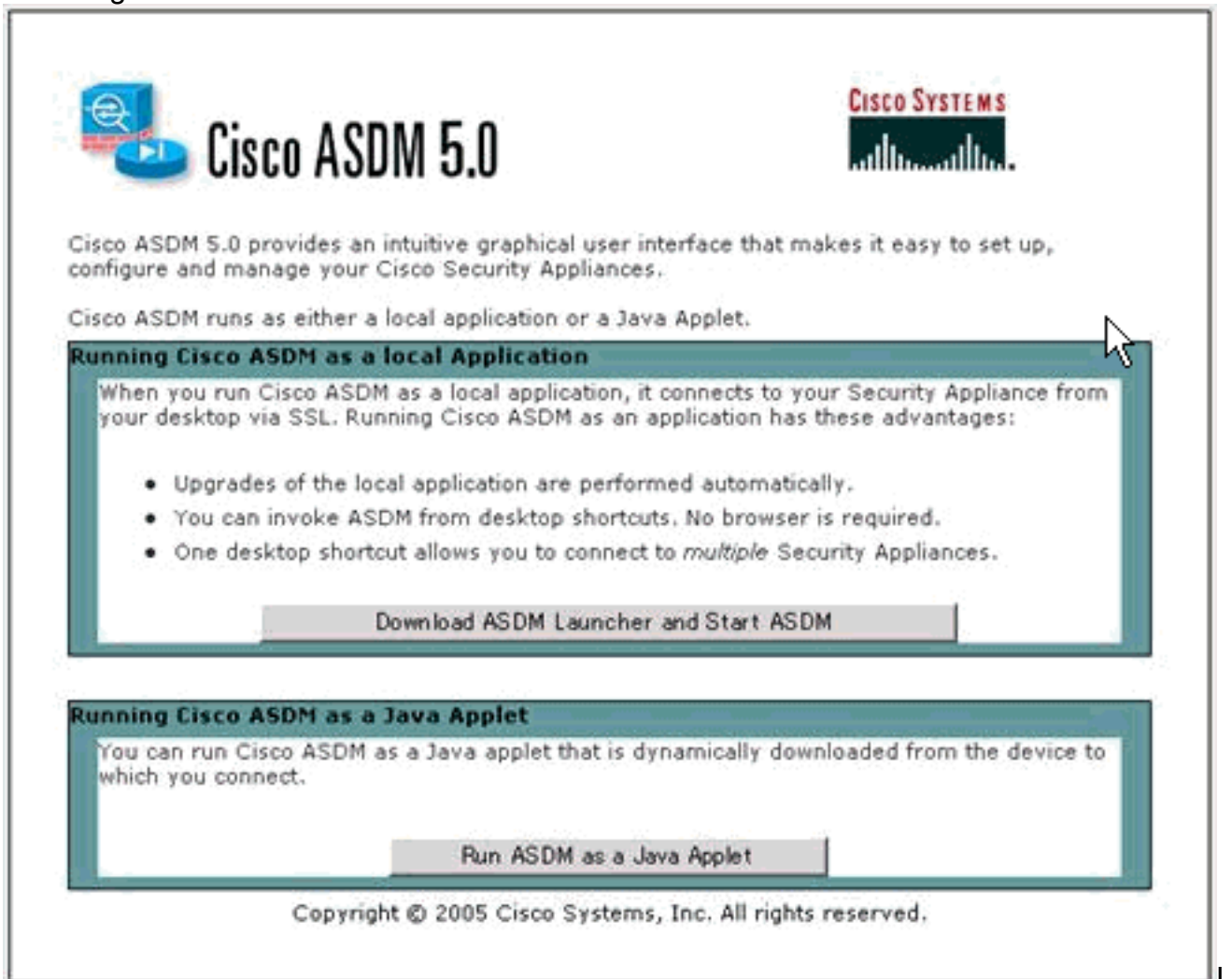
```
!  
no voice hpi capture buffer  
no voice hpi capture destination  
!  
!  
mta receive maximum-recipients 0  
!  
!  
!  
!  
interface Ethernet0/0  
ip address 172.17.63.230 255.255.255.240  
ip nat outside  
no ip route-cache  
no ip mroute-cache  
half-duplex  
crypto map nolan  
!  
interface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

Configuration utilisant l'ASDM

Cet exemple explique comment configurer le PIX utilisant le GUI ASDM. Un PC avec un navigateur et une adresse IP 10.1.1.2 est connecté à l'E1 d'interface interne du PIX. Assurez que le HTTP est activé sur le PIX.

Cette procédure montre la configuration ASDM des sièges sociaux PIX.

1. Connectez le PC au PIX et choisissez une méthode de téléchargement.



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

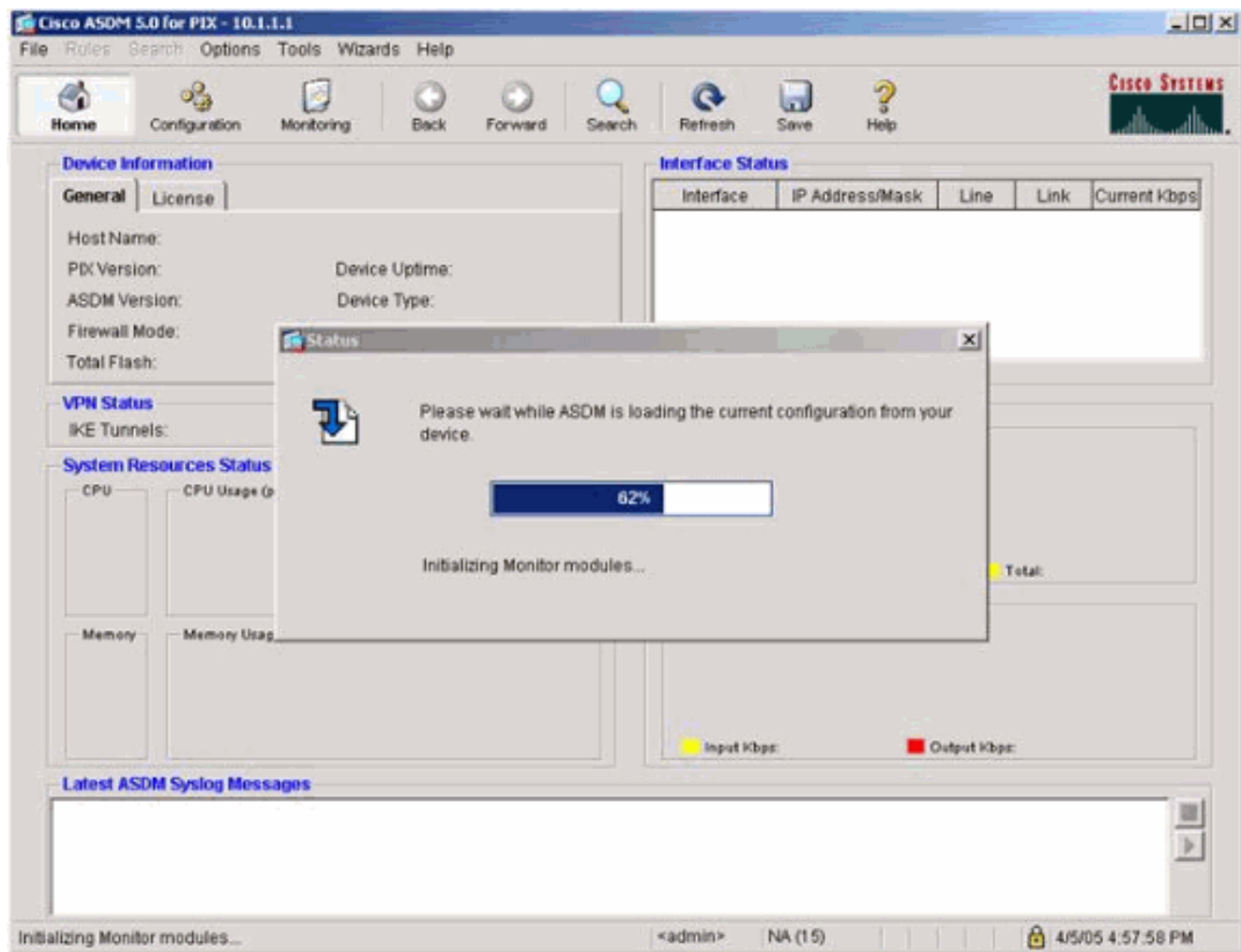
Running Cisco ASDM as a Java Applet

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 charge la configuration existante du PIX.



Cette fenêtre fournit des instruments et des menus de surveillance.

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

CPU Usage (percent)

0%
04:57:46

Memory

Memory Usage (MB)

67MB
04:57:46

Traffic Status

Connections Per Second Usage

UDP: 0 TCP: 0 Total: 0

'inside' Interface Traffic Usage (Kbps)

Input Kbps: 0 Output Kbps: 1

Latest ASDM Syslog Messages

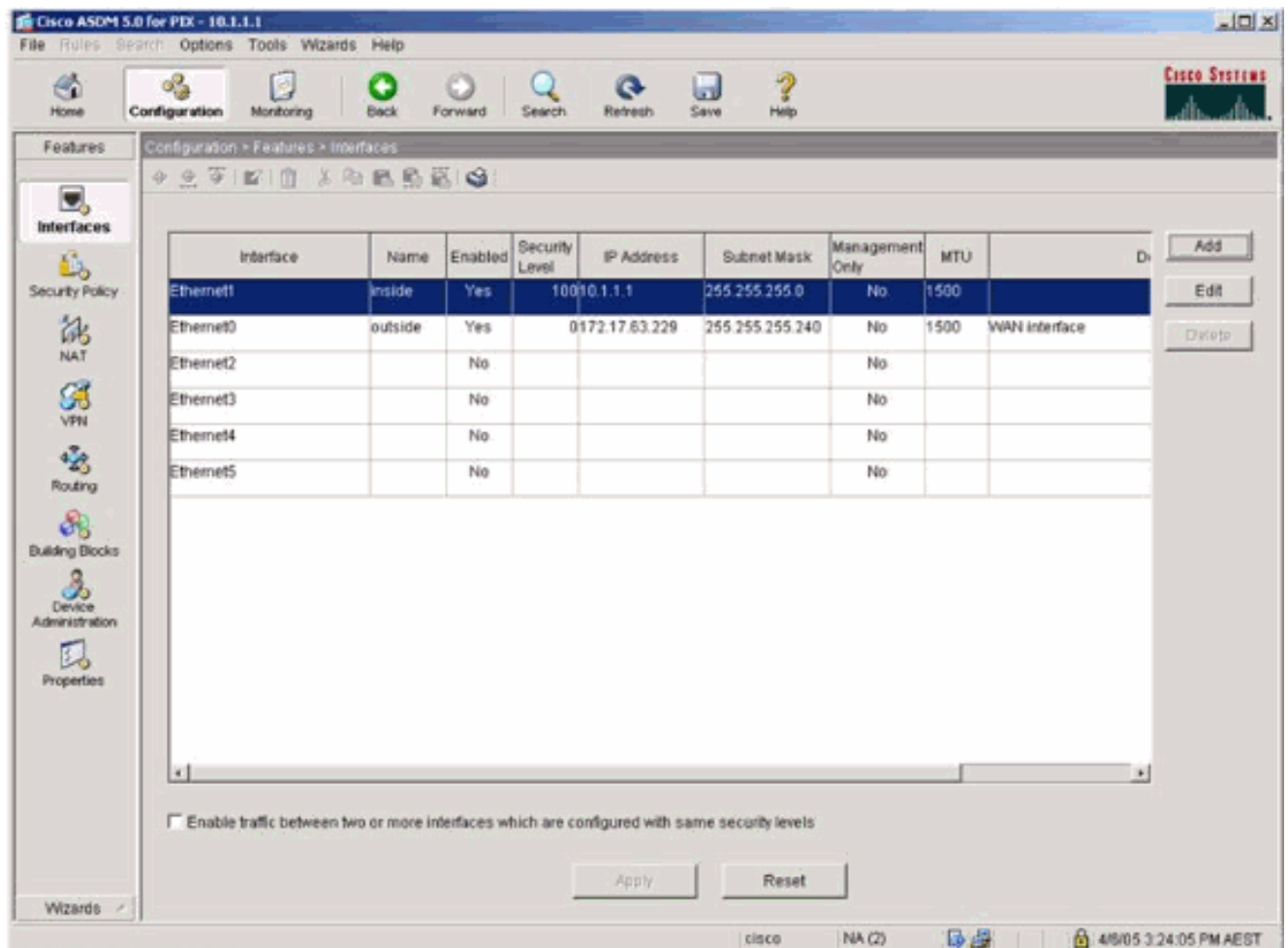
-- Syslog Disabled --

Configure ASDM Syslog Filters

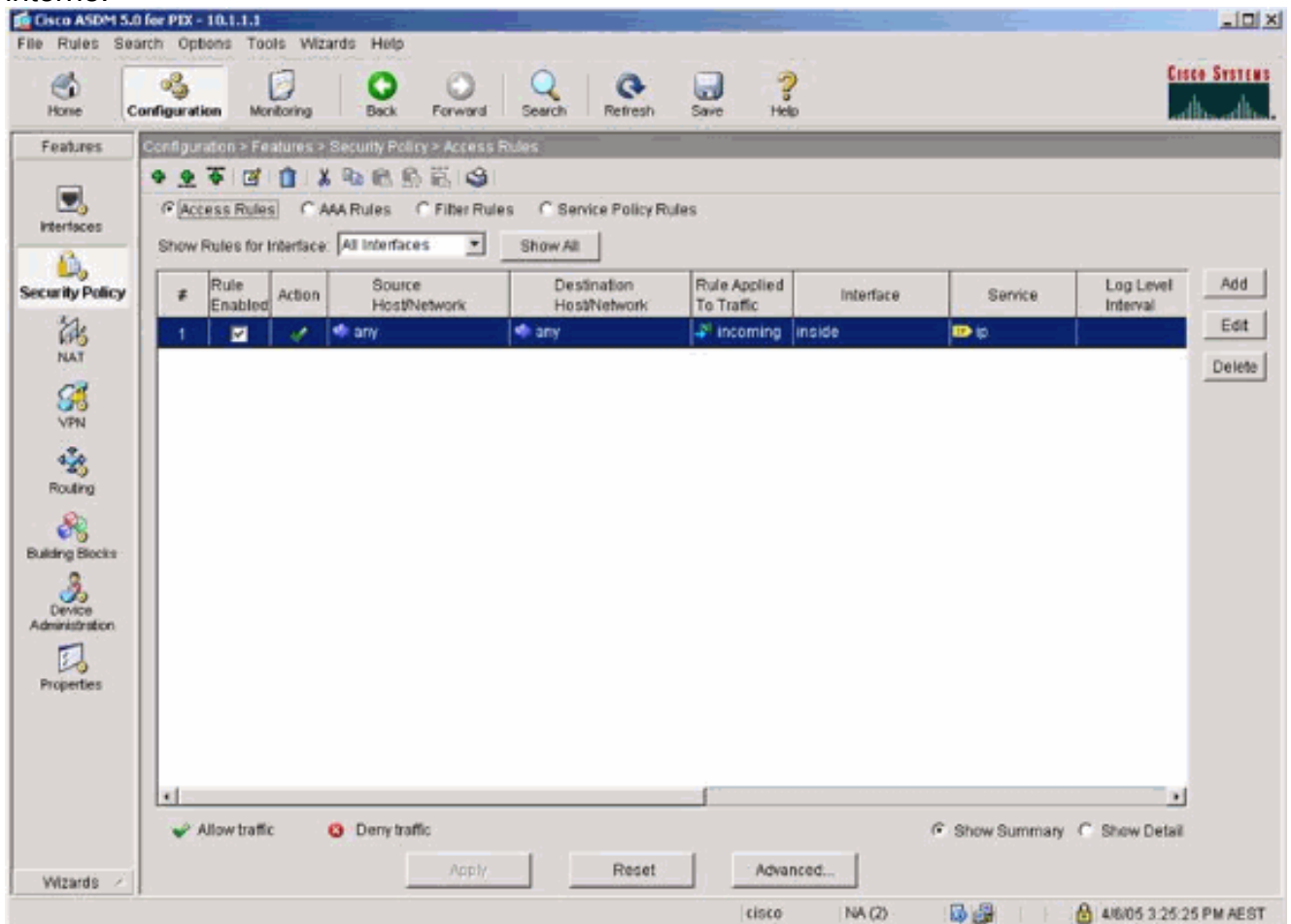
Device configuration loaded successfully.

<admin> NA (15) 4/5/05 4:57:46 AM UTC

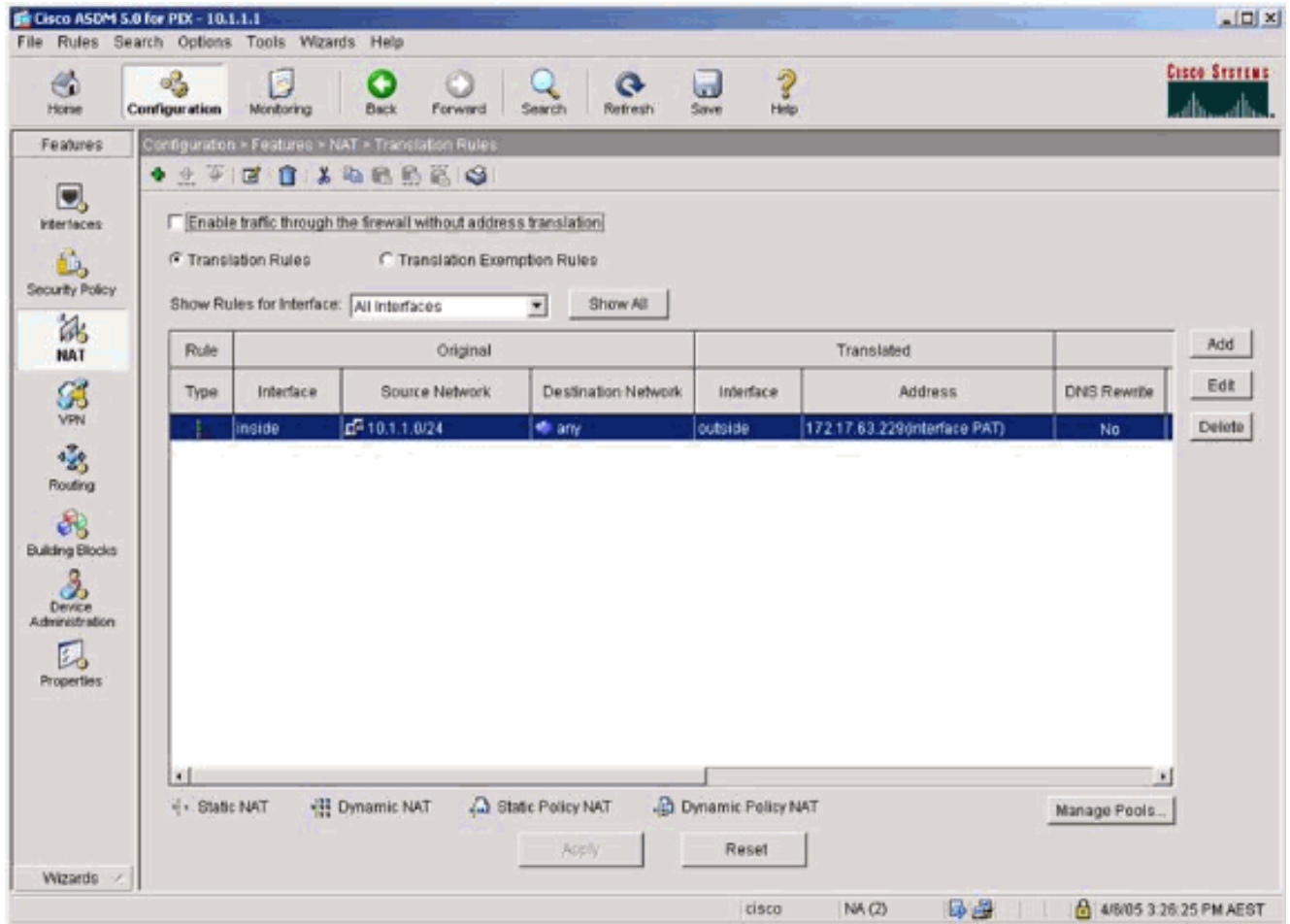
2. La configuration choisie > comporte > des interfaces et choisi ajoutez pour de nouvelles interfaces ou éditez pour une configuration existante.



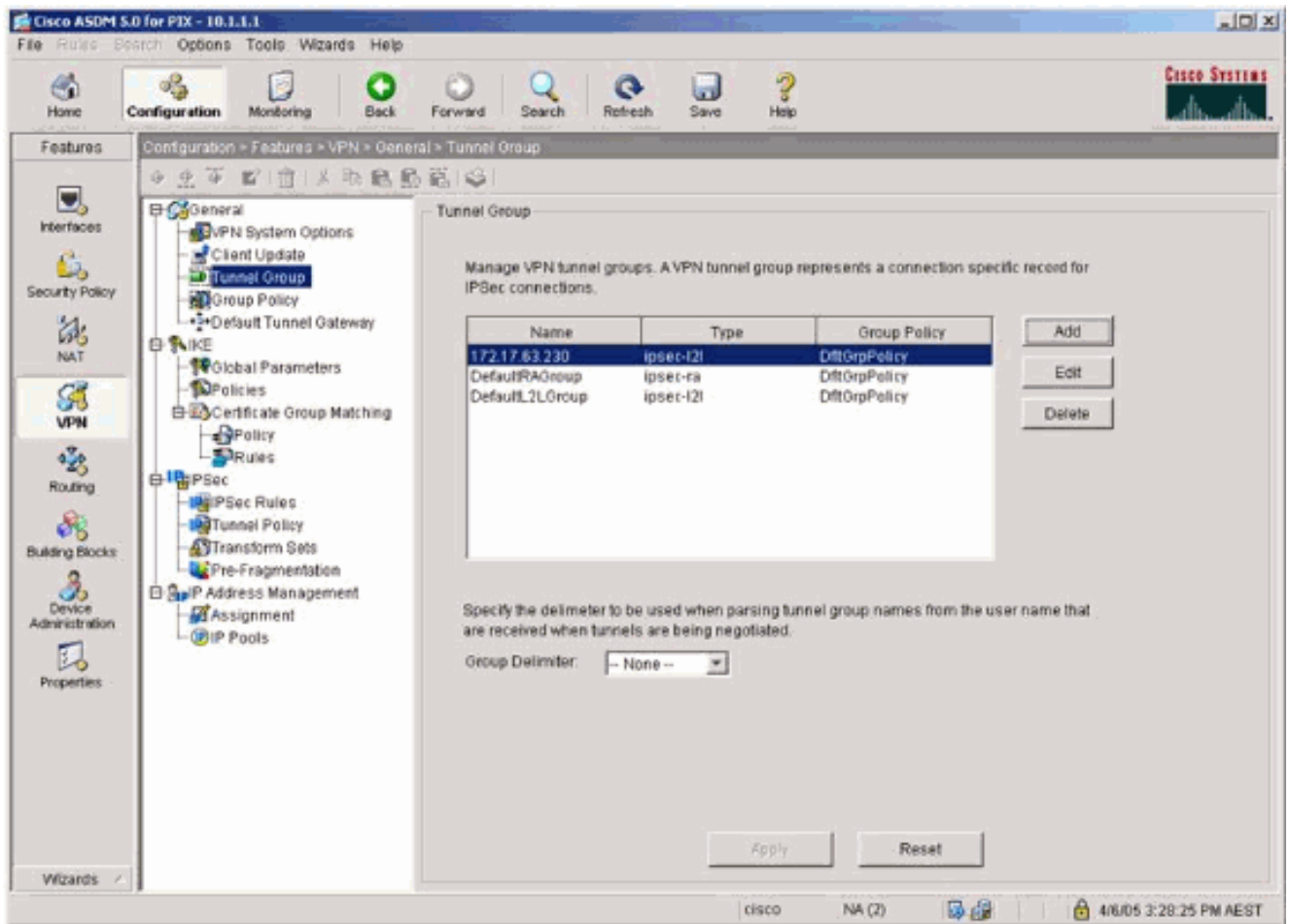
3. Sélectionnez les options de Sécurité pour l'interface interne.



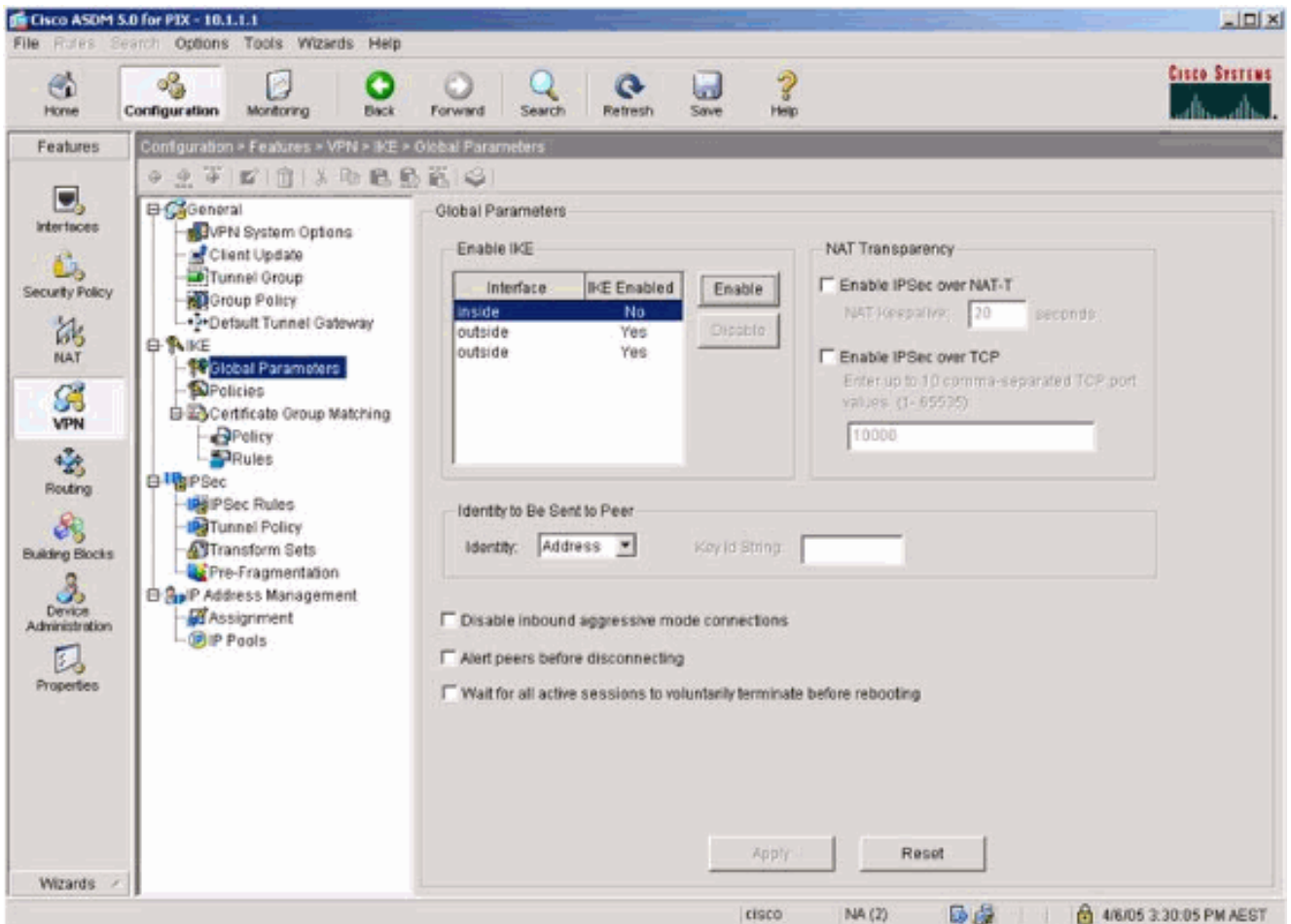
4. Dans la configuration NAT, le trafic chiffré est Nat-exempt et tout autre trafic est NAT/PAT à l'interface extérieure.



5. Le VPN choisi >General > groupe de tunnel et activent un groupe de tunnel

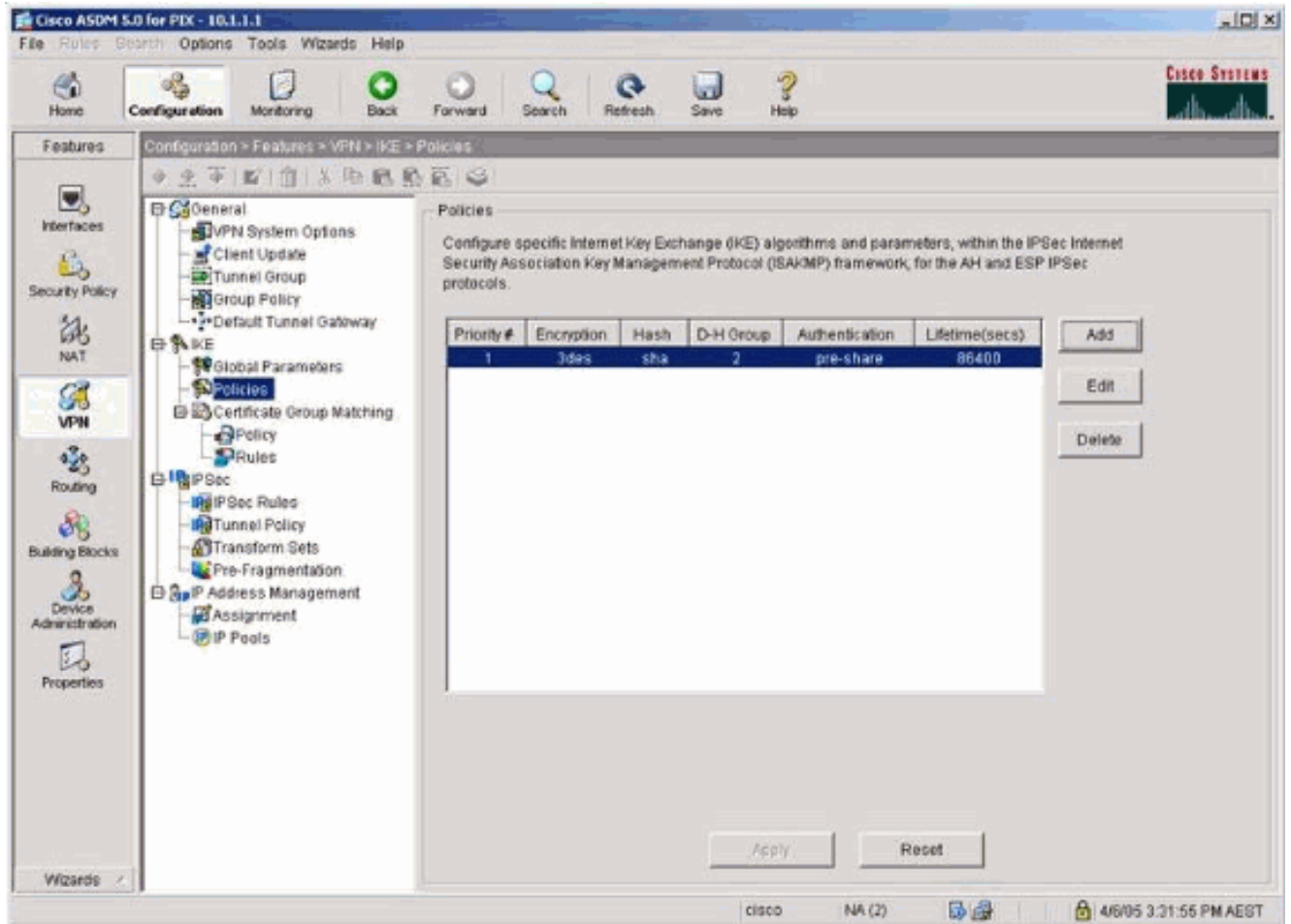


6. Choisi VPN > IKE > paramètres globaux et IKE d'enable sur l'interface extérieure.

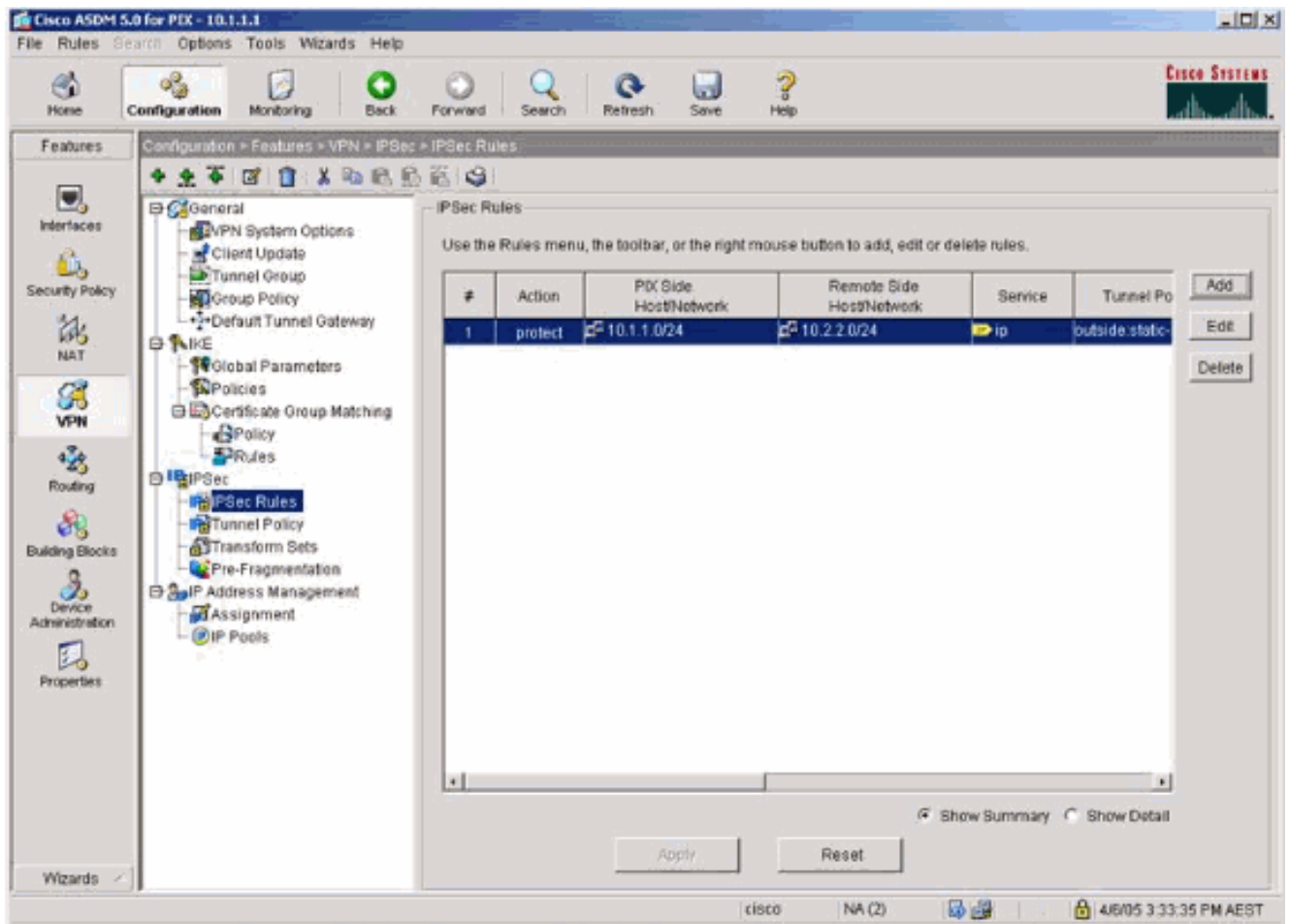


7. Choisi le VPN > l'IKE > les stratégies et choisissent les stratégies

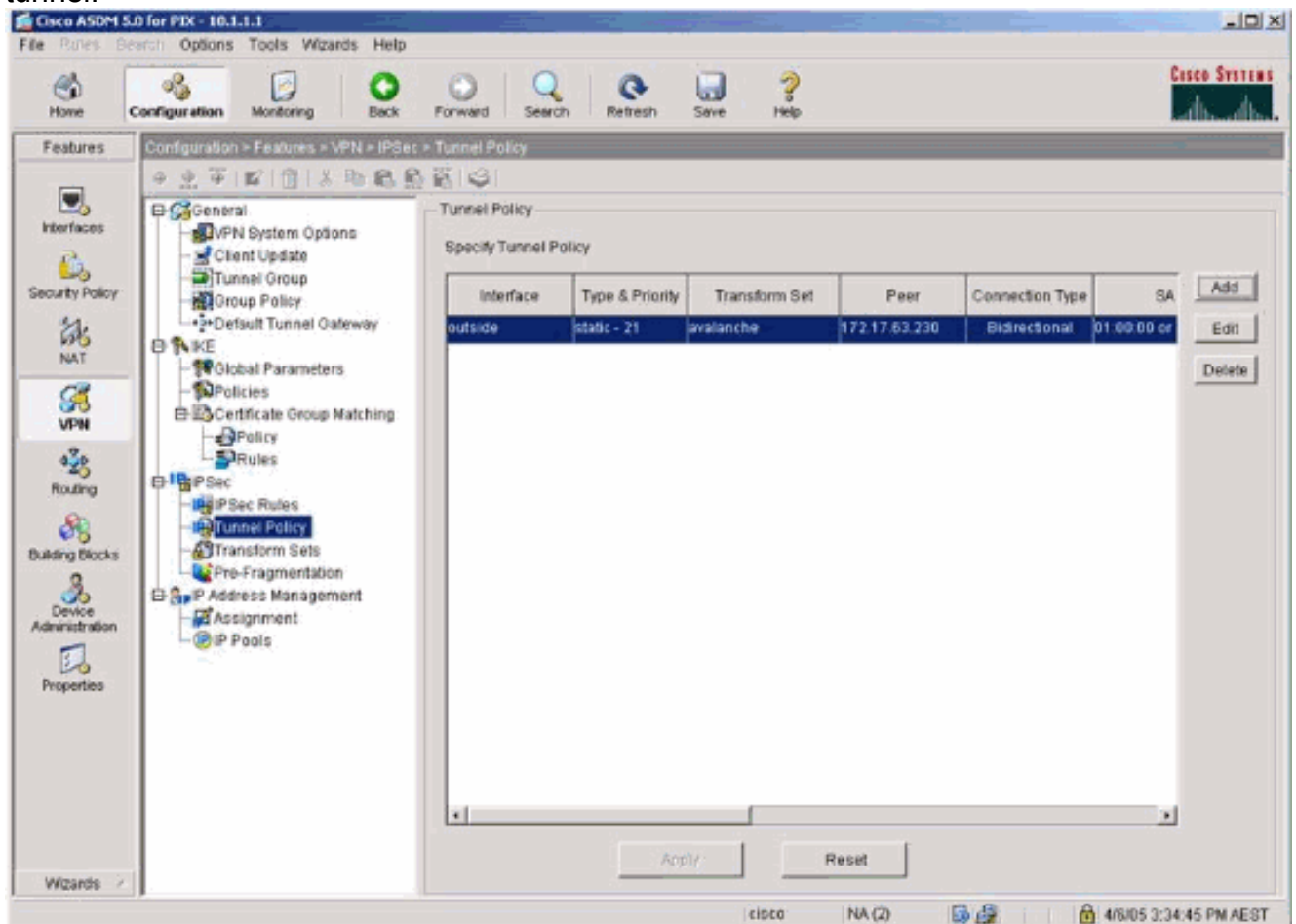
IKE.



8. Choisi le VPN > l'IPsec > les règles d'IPsec et choisissent IPsec pour le tunnel local et l'adressage distant.

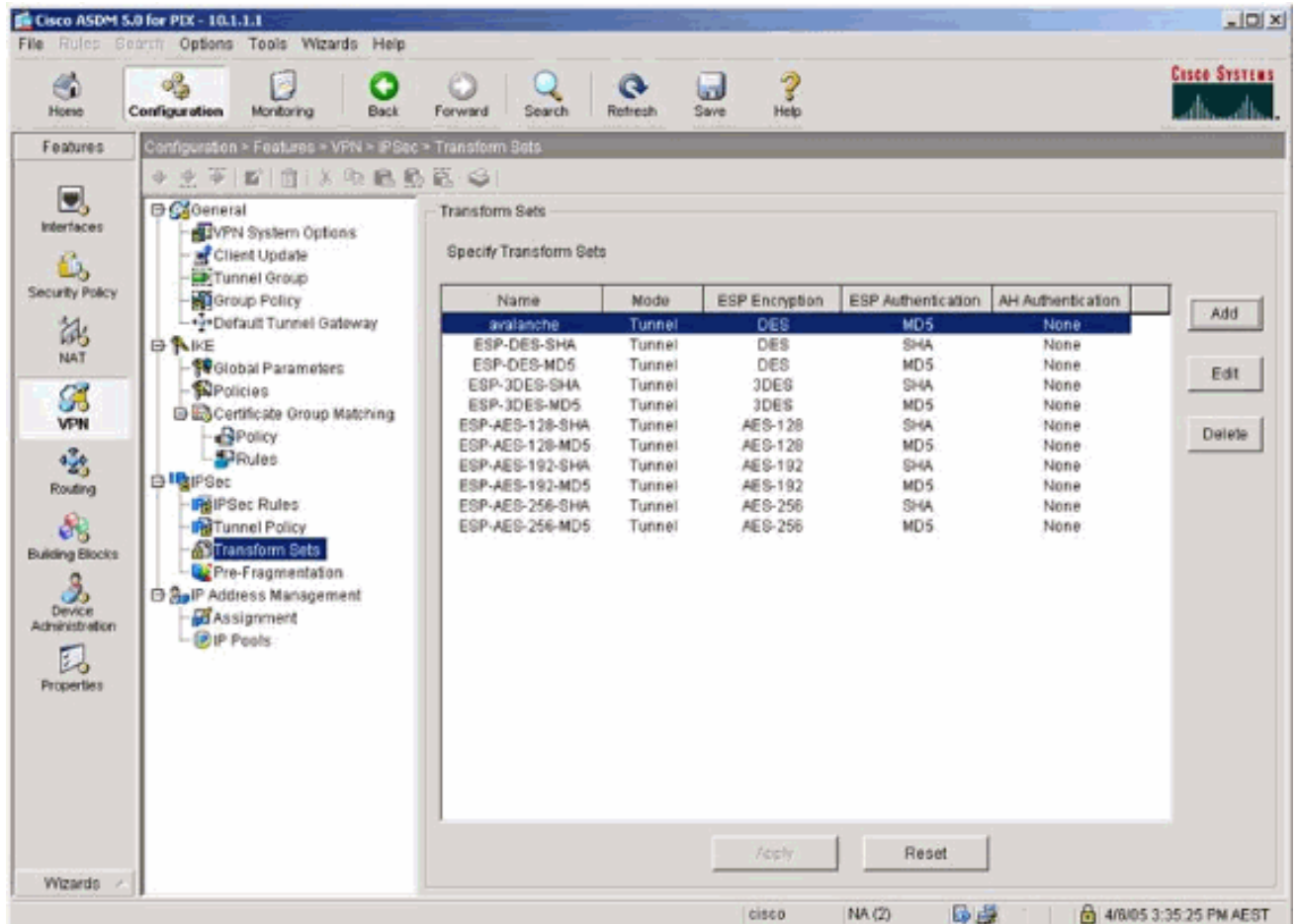


9. Choisi le VPN > l'IPsec > la stratégie de tunnel et choisissent la stratégie de tunnel.

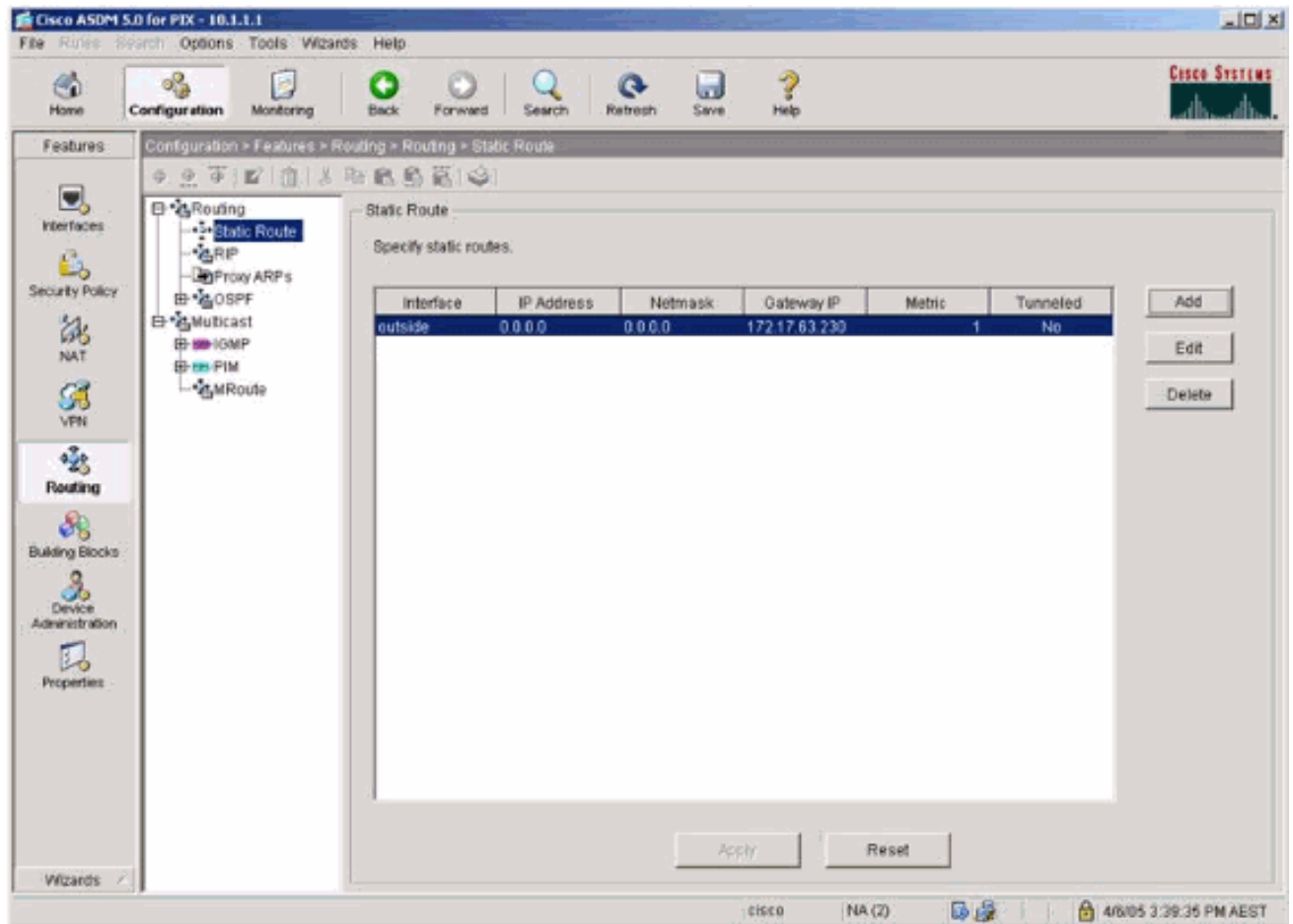


10. Choisi le VPN > l'IPsec > les jeux de transformations et choisissent un jeu de

transformations.



11. **Le routage** choisi > **le routage** > **artère statique** et choisissent une artère statique au routeur de passerelle. Dans cet exemple, les points d'acheminement statiques à l'homologue VPN distant pour la simplicité.



Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'[Outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

- **show crypto ipsec sa** - Montre les associations de sécurisation de phase 2.
- **show crypto isakmp sa** - Montre les associations de sécurisation de phase 1.

Dépanner

Vous pouvez employer l'ASDM pour activer se connecter et pour visualiser les logs.

- Sélectionnez la **configuration > le Propriétés > en se connectant > en se connectant l'installation**, choisissez **Enable se connecter** et cliquez sur **Apply** pour activer se connecter.
- Sélectionnez la **surveillance > en se connectant > mémoire tampon de log > sur se connecter le niveau**, choisissez le **tampon de journalisation**, et cliquez sur la **vue** pour visualiser les logs.

Dépannage des commandes

L'[Outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

Remarque: Référez-vous aux [informations importantes sur les commandes de débogage](#) avant d'utiliser les commandes de **débogage**.

- **debug crypto ipsec** — Affiche les négociations IPSecs de la phase 2.
- **debug crypto isakmp** — Affiche les négociations ISAKMP de la phase 1.
- **debug crypto engine** - Montre le trafic crypté.
- **clear crypto isakmp** — Autorise les associations de sécurité liées à la phase 1.
- **clear crypto sa** — Autorise les associations de sécurité liées à la phase 2.
- **mettez au point le suivi d'ICMP** — Affiche si les demandes d'ICMP des hôtes atteignent le PIX. Vous devez ajouter la **commande access-list** de permettre à l'ICMP dans votre configuration afin d'exécuter ceci mettez au point.
- **élimination des imperfections de tampon de journalisation** — Connexions d'expositions étant établies et refusées aux hôtes qui passent par le PIX. Les informations sont stockées dans la mémoire tampon de log PIX et vous pouvez voir la sortie avec le **show log command**.

[Informations connexes](#)

- [Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance](#)
- [Logiciels pare-feu Cisco PIX](#)
- [Références des commandes du pare-feu Cisco Secure PIX](#)
- [Notices de champs relatives aux produits de sécurité \(y compris PIX\)](#)
- [Demandes de commentaires \(RFC\)](#)