ASA/PIX : configuration d'un tunnel IPsec LAN à LAN d'un routeur Cisco IOS

Contenu

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 Configuration d'IPSec - Router to PIX pour plus d'informations sur une configuration de tunnel LAN à LAN entre un routeur et le PIX.

Référez-vous à Exemple de configuration de tunnel IPSec LAN à LAN entre le concentrateur Cisco VPN 3000 et le pare-feu PIX pour plus d'informations sur une configuration de tunnel LAN à LAN entre le pare-feu PIX et le concentrateur Cisco VPN 3000.

Référez-vous à Exemple de configuration du tunnel IPsec entre PIX 7.x et VPN 3000 afin d'en savoir plus sur le scénario où le tunnel LAN à LAN se trouve entre le concentrateur PIX et VPN.

Référez-vous à Exemple de configuration de VPN satellite à client amélioré avec authentification TACACS+ PIX/ASA 7.x afin d'en savoir plus sur le scénario où le tunnel LAN à LAN entre les PIX permet également à un client VPN d'accéder au PIX satellite via le PIX concentrateur.

Reportez-vous à SDM : Exemple de configuration d'un VPN IPsec site à site entre ASA/PIX et un routeur IOS afin d'en savoir plus sur le même scénario où l'appliance de sécurité PIX/ASA exécute le logiciel version 8.x.

Reportez-vous à Configuration Professional : Exemple de configuration d'un VPN IPsec site à site entre ASA/PIX et un routeur IOS afin d'en savoir plus sur le même scénario où la configuration liée à ASA est affichée à l'aide de l'interface utilisateur graphique ASDM et la configuration liée au routeur est affichée à l'aide de l'interface utilisateur graphique Cisco CP.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- PIX-525 avec logiciel PIX version 7.0
- Routeur Cisco 2611 avec logiciel Cisco IOS® Version 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

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

Informations générales

Sur PIX, les commandes **access-list** et **nat 0** fonctionnent ensemble. Lorsqu'un utilisateur du réseau 10.1.1.0 se rend sur le réseau 10.2.2.0, la liste d'accès est utilisée pour permettre au trafic réseau 10.1.1.0 d'être chiffré sans traduction d'adresses de réseau (NAT). Sur le routeur, les commandes **route-map** et **access-list** permettent de chiffrer le trafic réseau 10.2.2.0 sans NAT. Cependant, lorsque ces mêmes utilisateurs se rendent ailleurs, ils sont traduits vers l'adresse 172.17.63.230 via la traduction d'adresses de port (PAT).

Voici les commandes de configuration requises sur le dispositif de sécurité PIX afin que le trafic *ne* passe *pas* par PAT sur le tunnel, et le trafic vers Internet pour passer 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
```

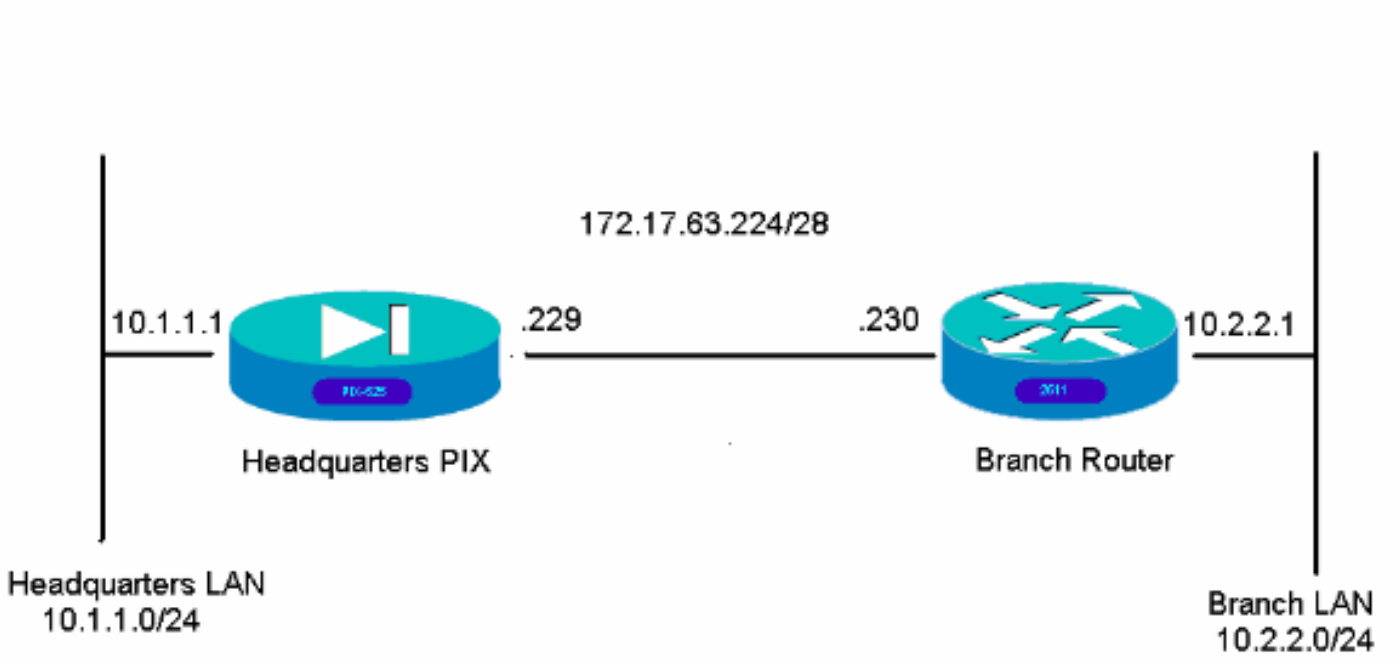
Configuration

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

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) 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 concernent l'interface de ligne de commande. Reportez-vous à la section Configuration using Adaptive Security Device Manager (ASDM) de ce document si vous préférez configurer à l'aide d'ASDM.

- PIX du siège
- Routeur de filiale

PIX du siège

```
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 de filiale

```
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
!
!
```

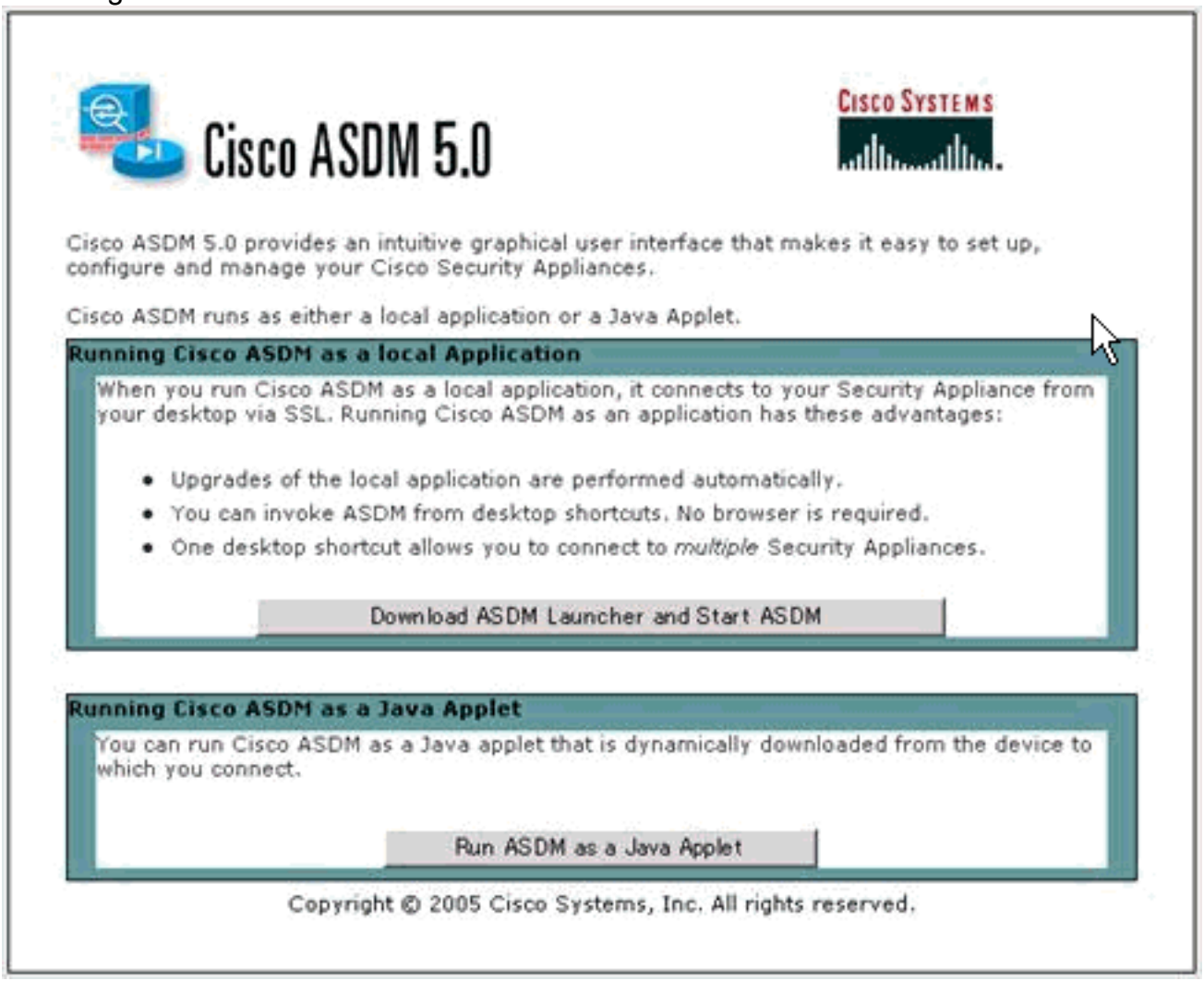
```
!
!
interface Ethernet0/0
ip address 172.17.63.230 255.255.255.240
ip nat outside
no ip route-cache
no ip mroute-cache
half-duplex
crypto map nolan
!
interface Ethernet0/1
ip address 10.2.2.1 255.255.255.0
ip nat inside
half-duplex
!
ip nat pool branch 172.17.63.230 172.17.63.230 netmask
255.255.255.0
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 à l'aide d'ASDM

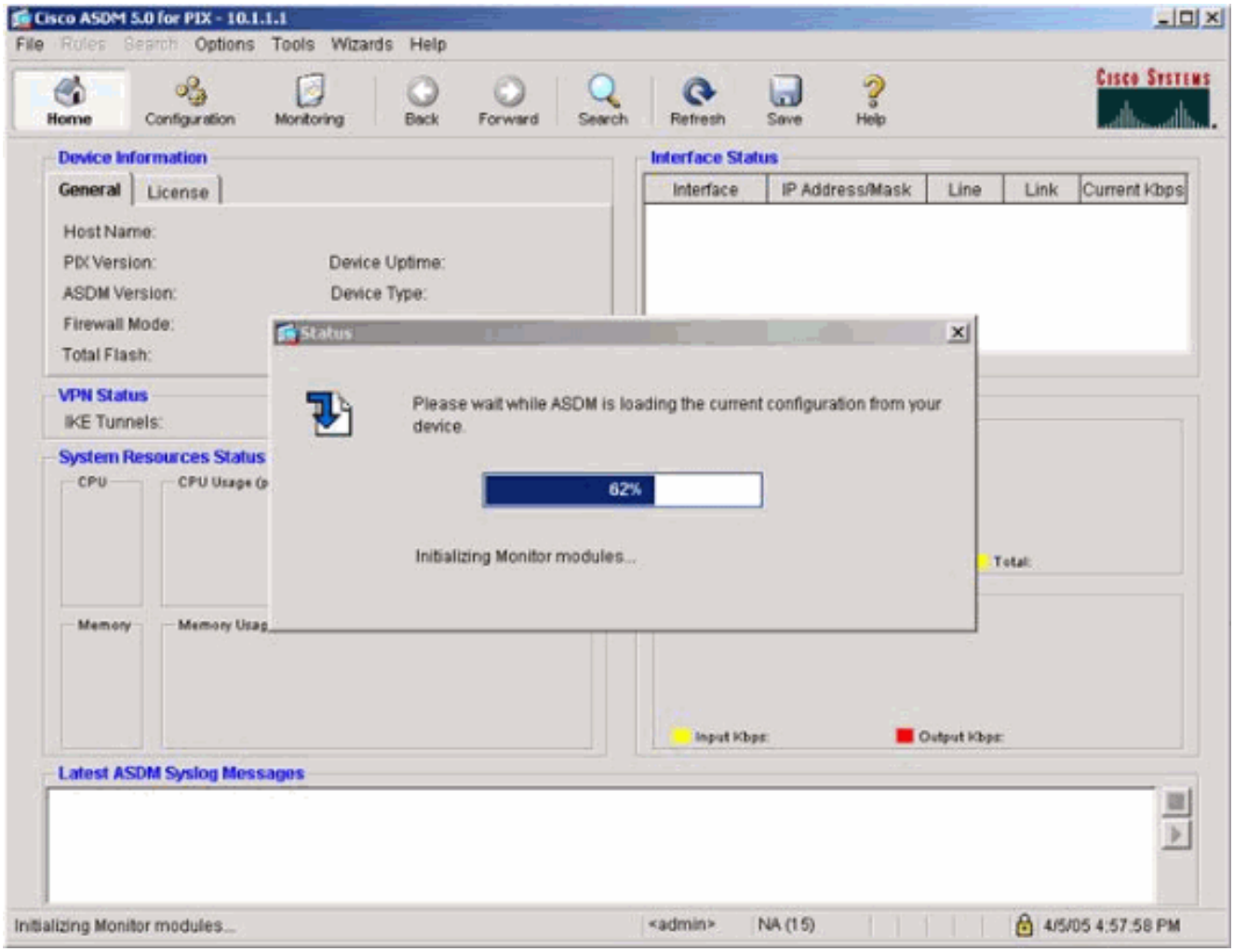
Cet exemple montre comment configurer le PIX à l'aide de l'interface utilisateur graphique ASDM. Un PC avec un navigateur et l'adresse IP 10.1.1.2 est connecté à l'interface interne e1 du PIX. Assurez-vous que http est activé sur le PIX.

Cette procédure illustre la configuration ASDM du PIX du siège.

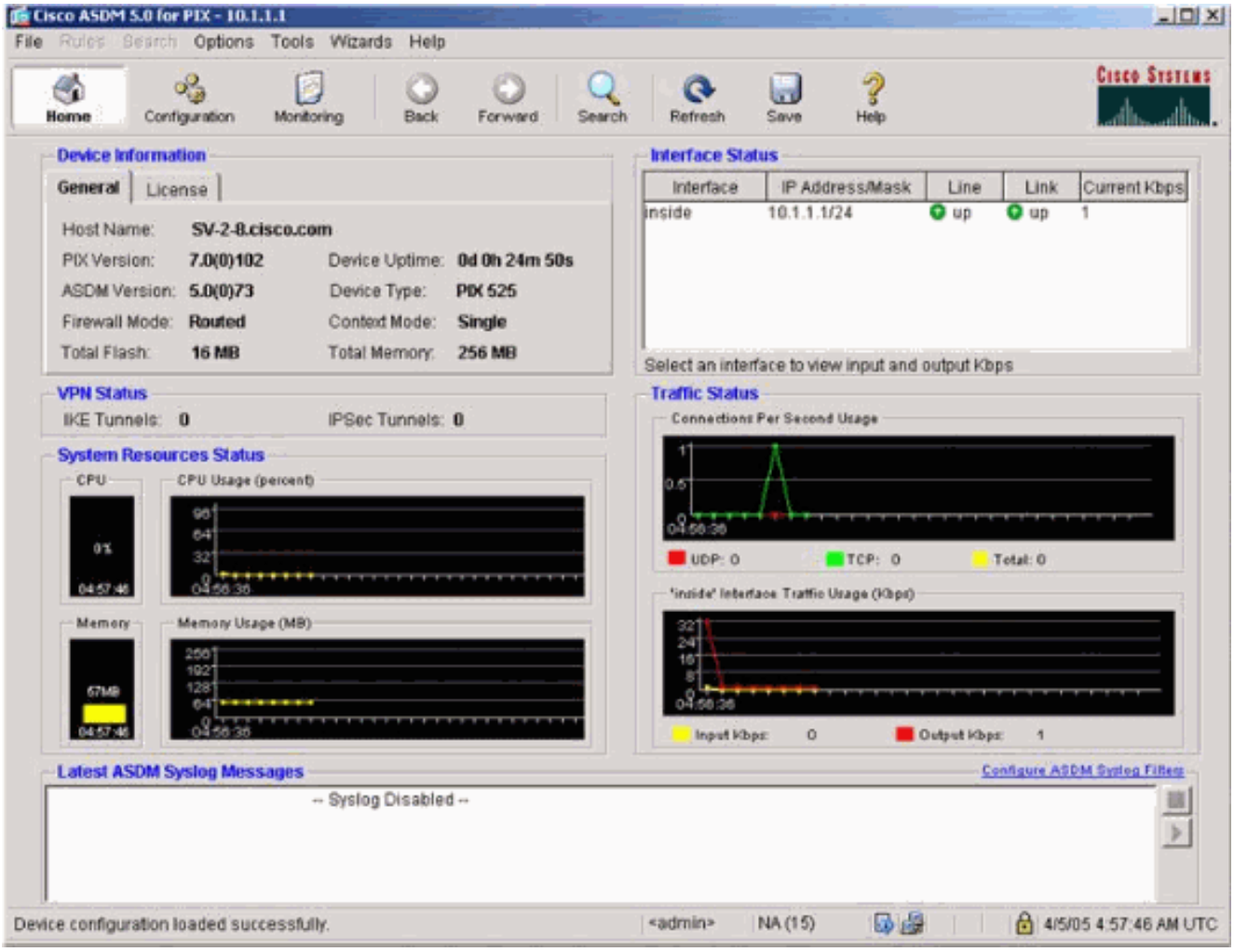
1. Connectez le PC au PIX et choisissez une méthode de téléchargement.



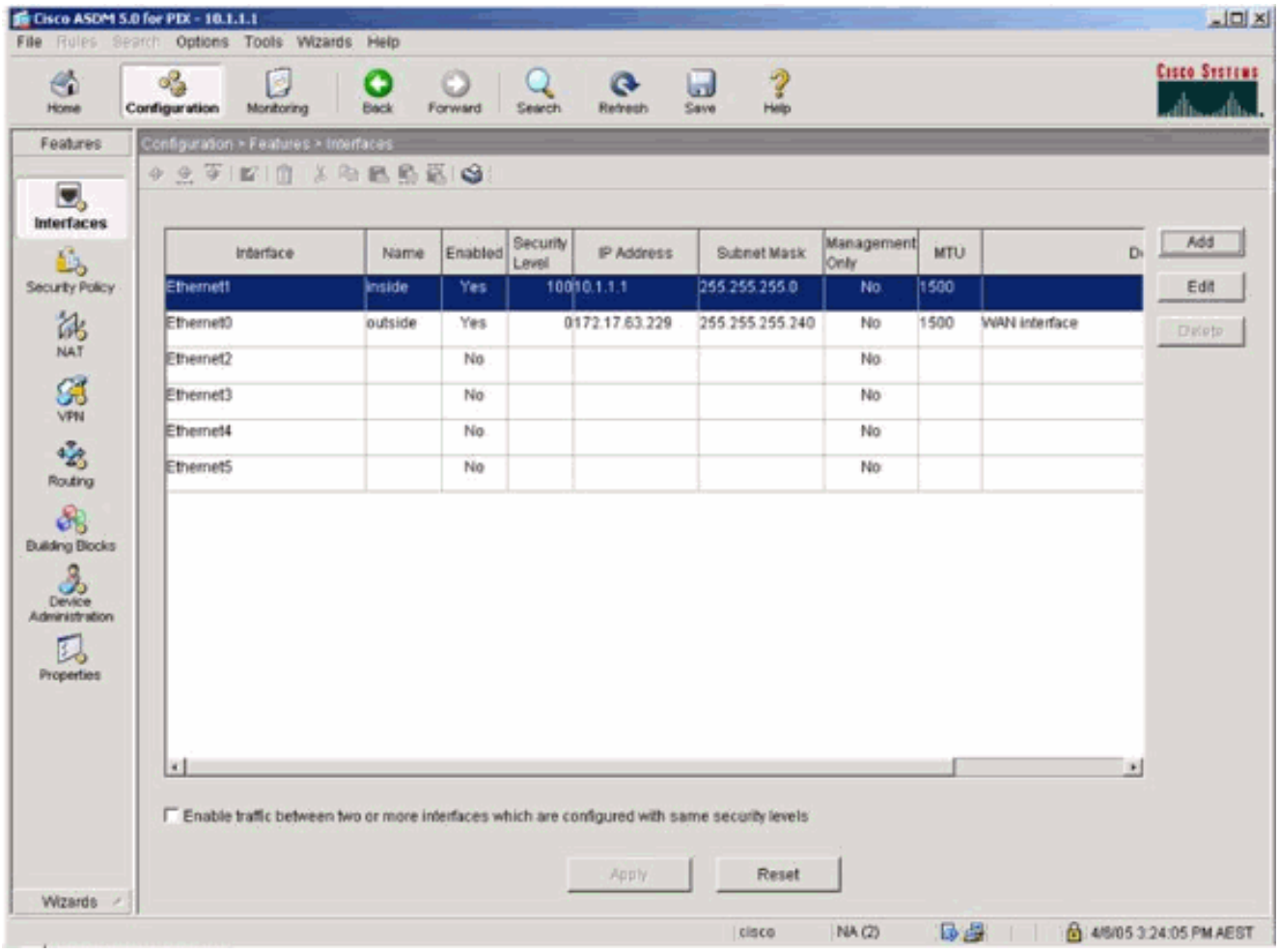
ASDM charge la configuration existante à partir du PIX.



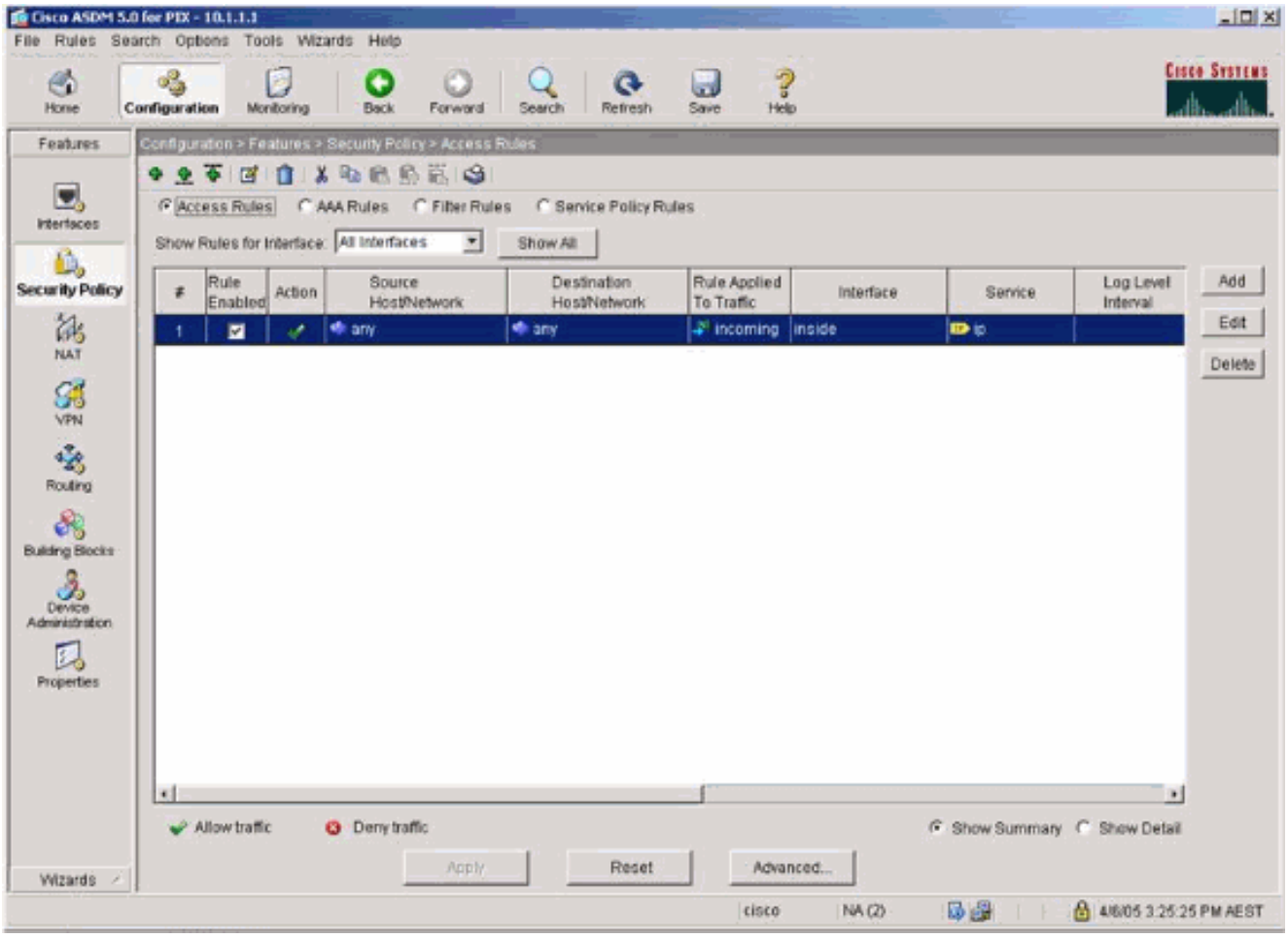
Cette fenêtre fournit des outils de surveillance et des menus.



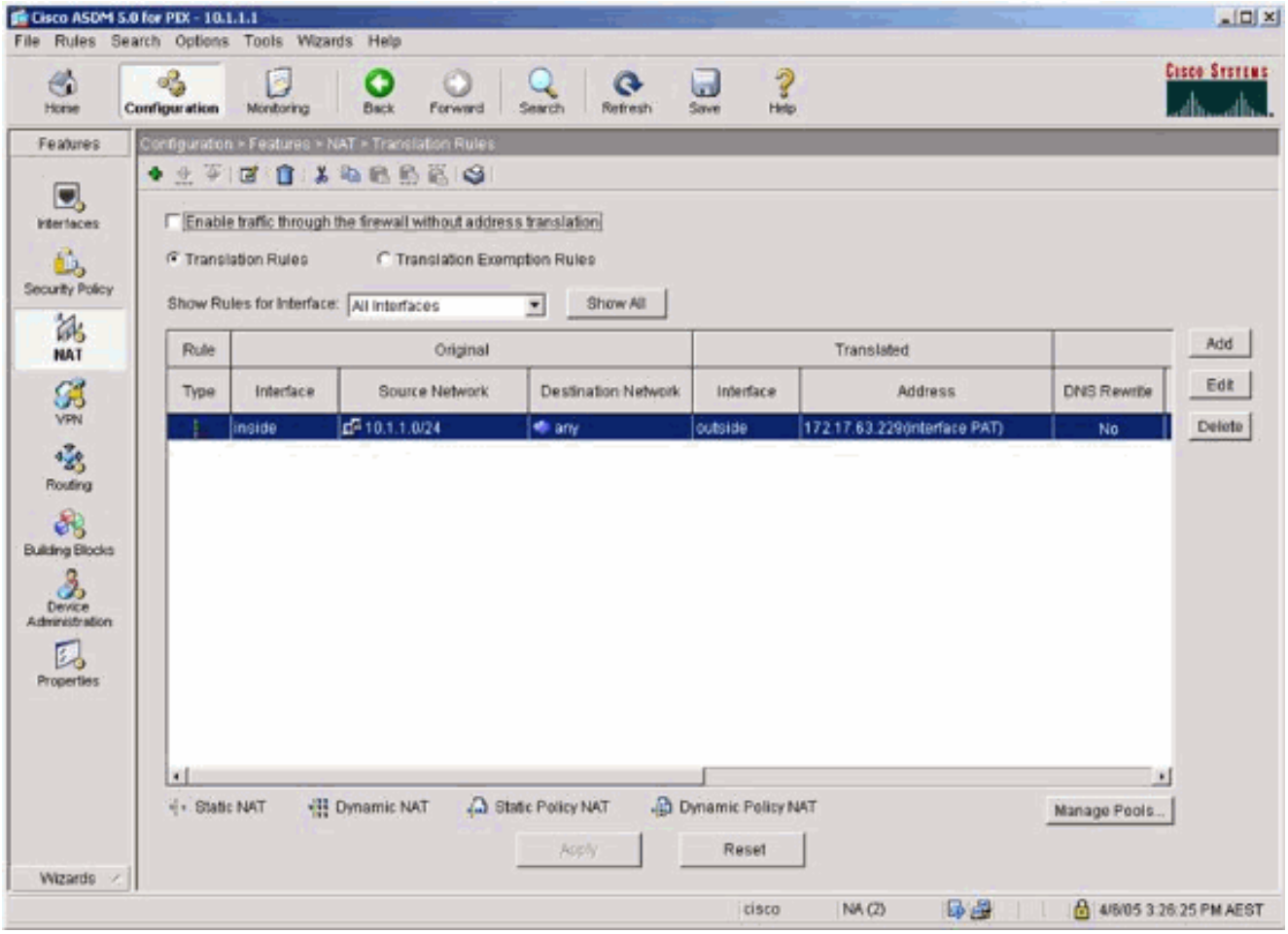
2. Sélectionnez **Configuration > Features > Interfaces** et sélectionnez **Add** pour les nouvelles interfaces ou **Edit** pour une configuration existante.



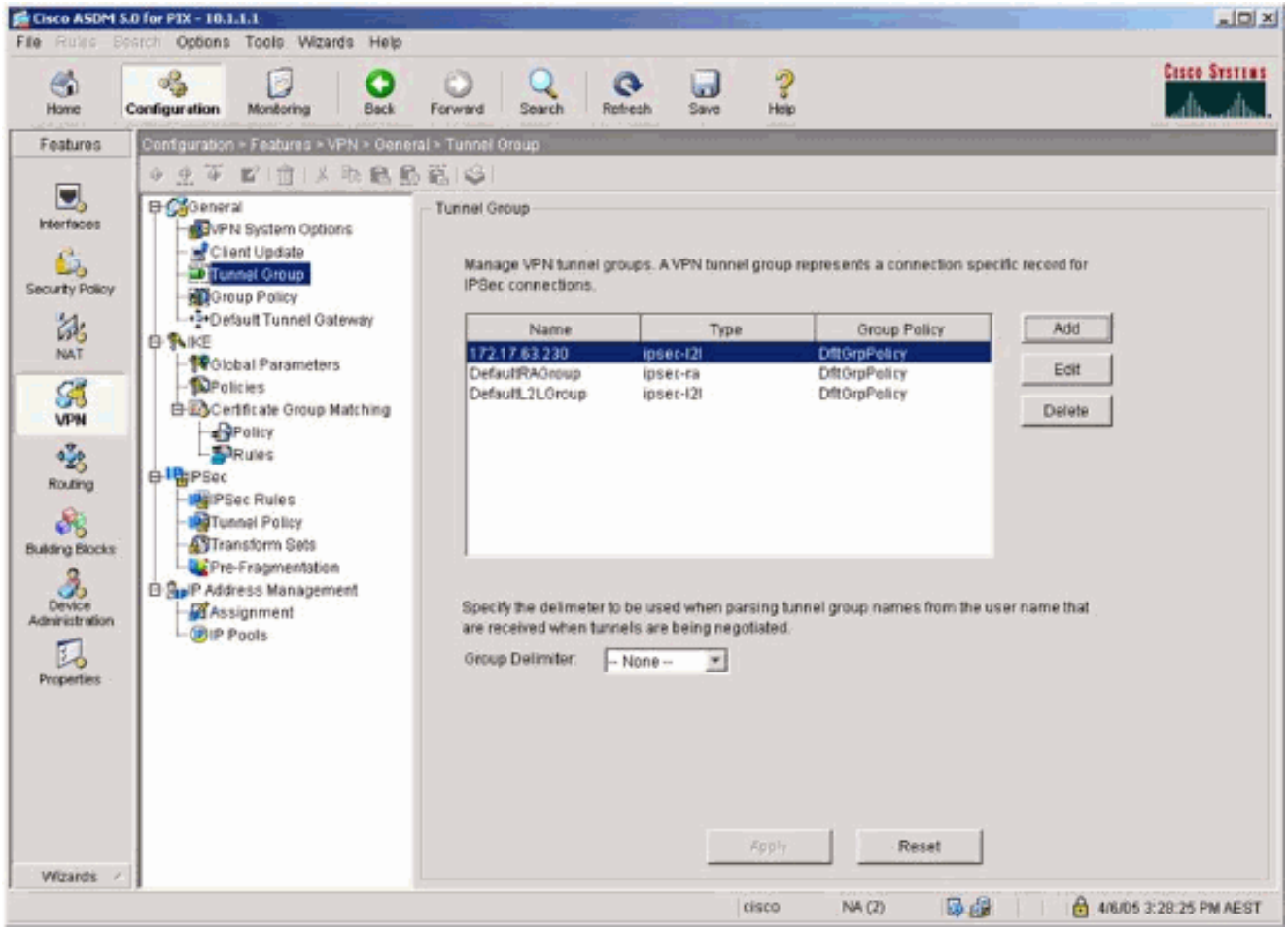
3. Sélectionnez les options de sécurité pour l'interface interne.



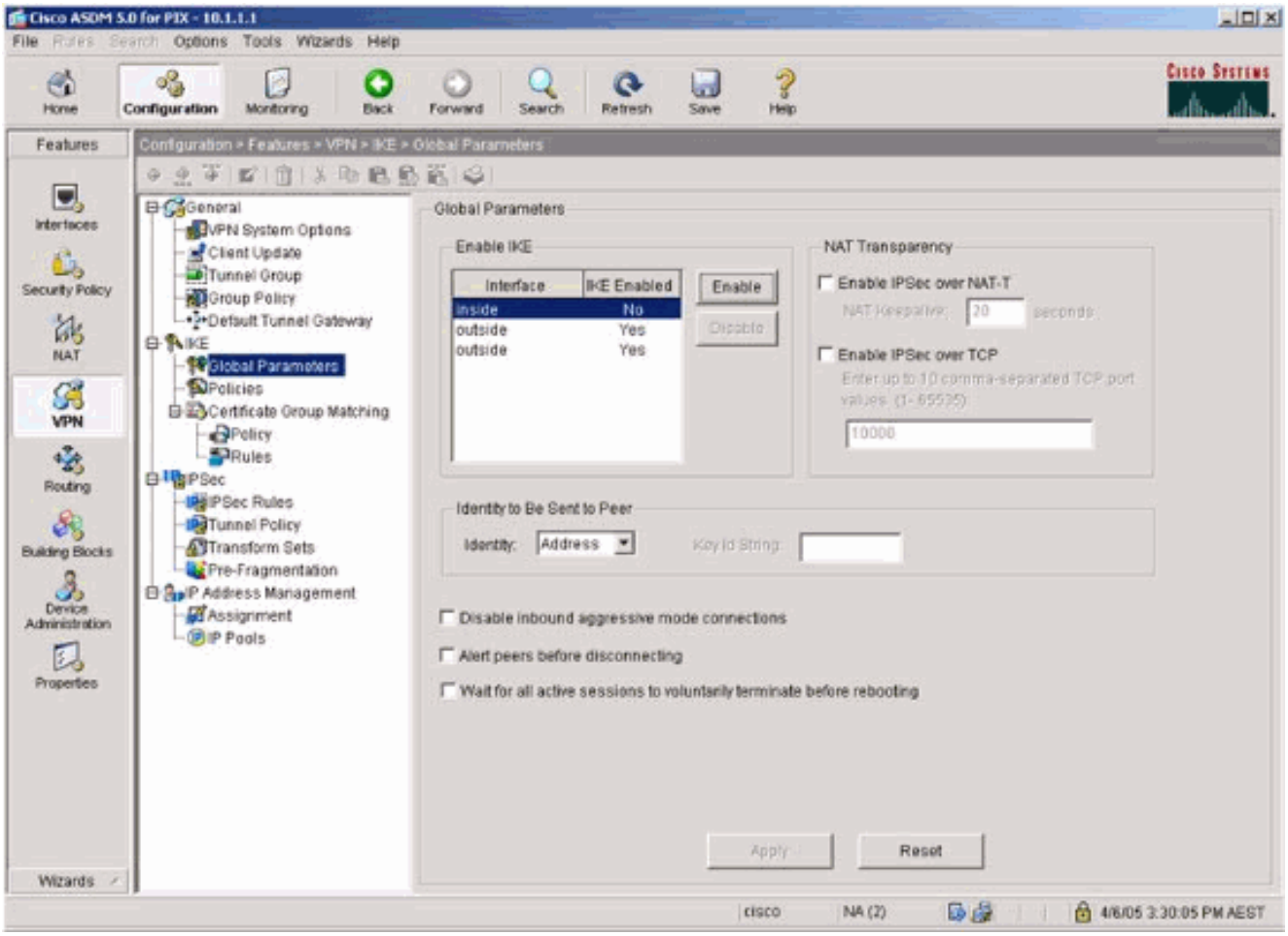
4. Dans la configuration NAT, le trafic chiffré est exempt de NAT et tout autre trafic est NAT/PAT vers l'interface
externe.



5. Sélectionnez **VPN >General > Tunnel Group** et activez un groupe de
tunnels

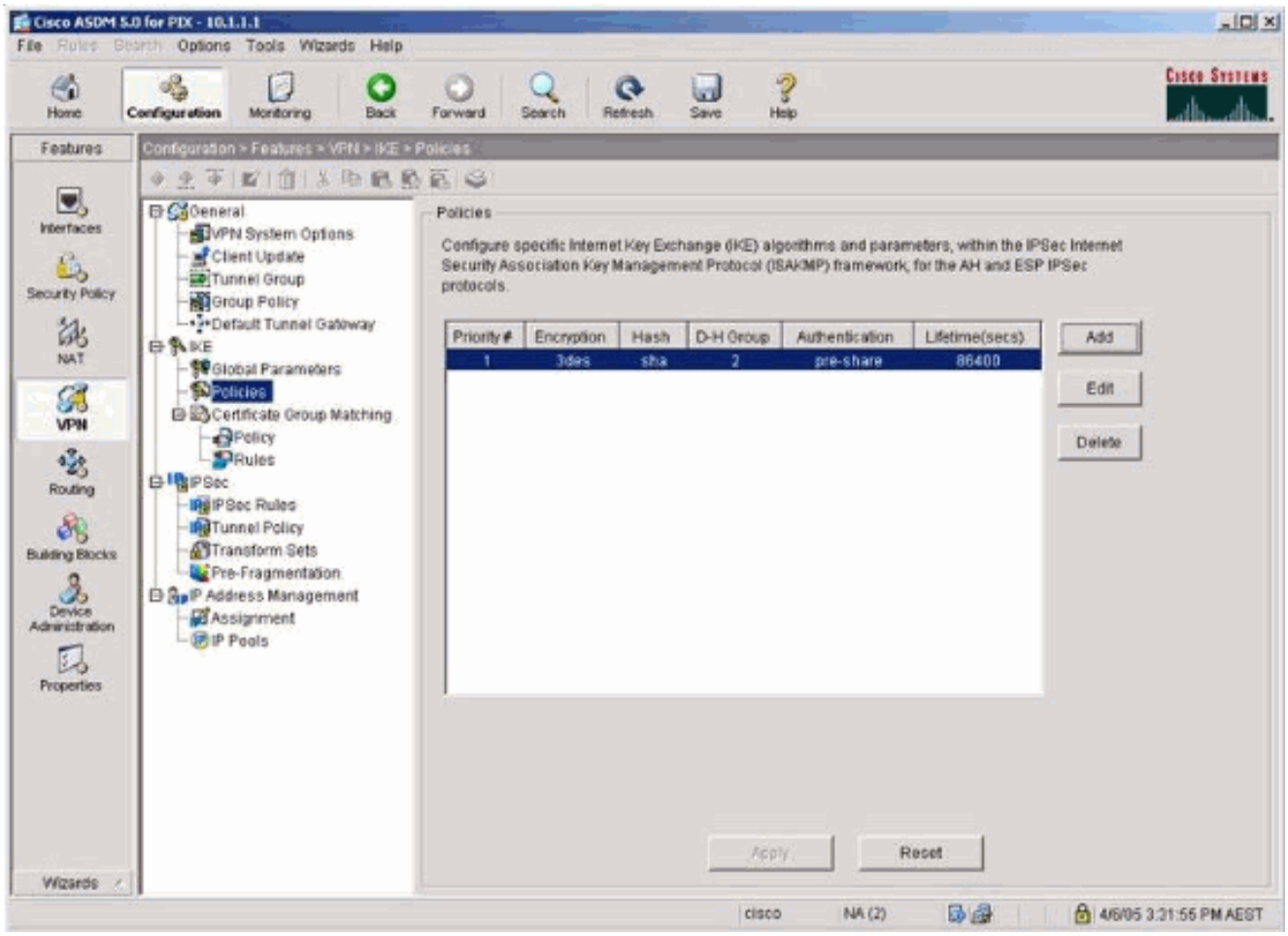


6. Sélectionnez **VPN > IKE > Global Parameters** et activez IKE sur l'interface externe.

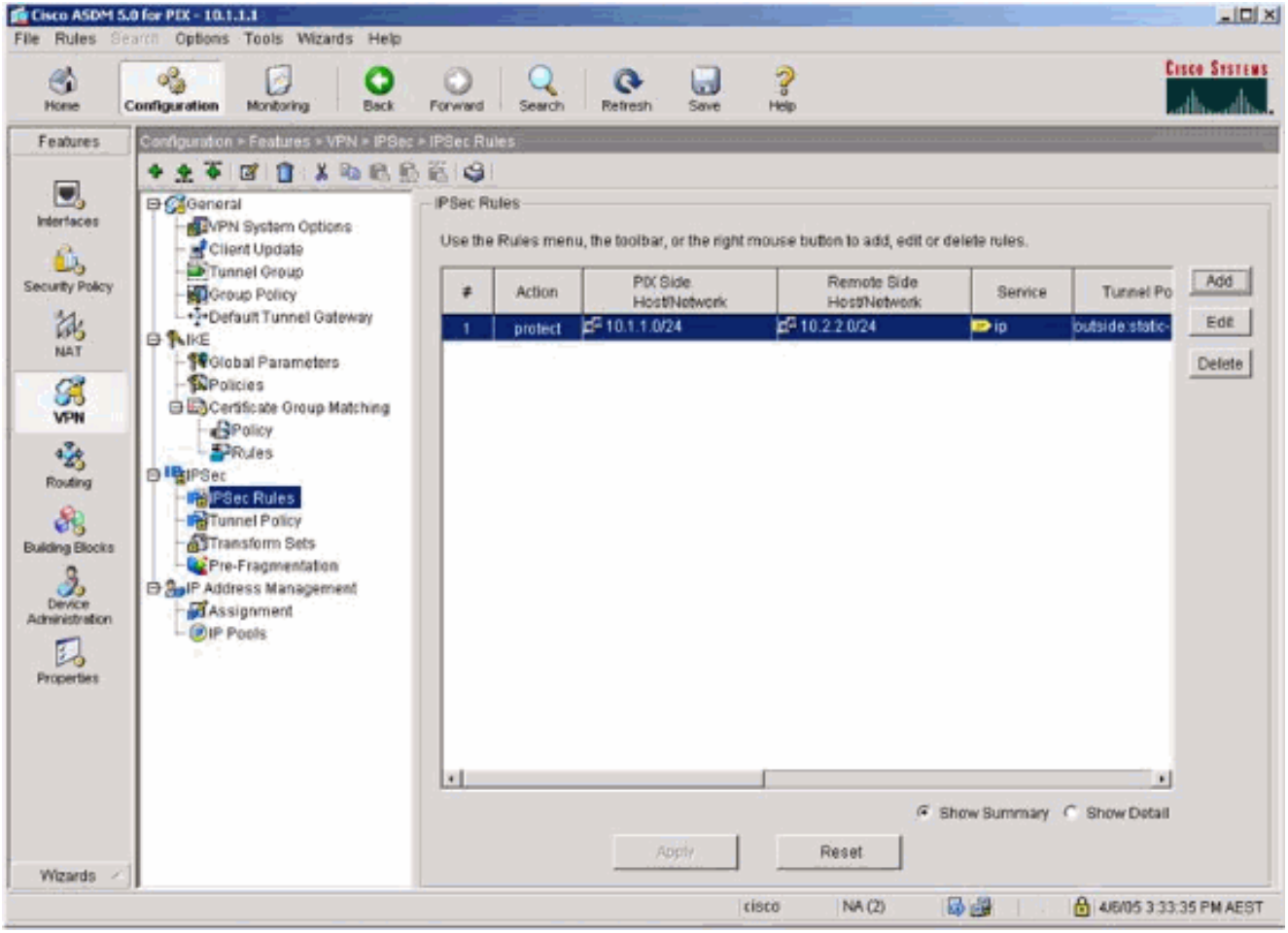


7. Sélectionnez **VPN > IKE > Policies** et choisissez les stratégies

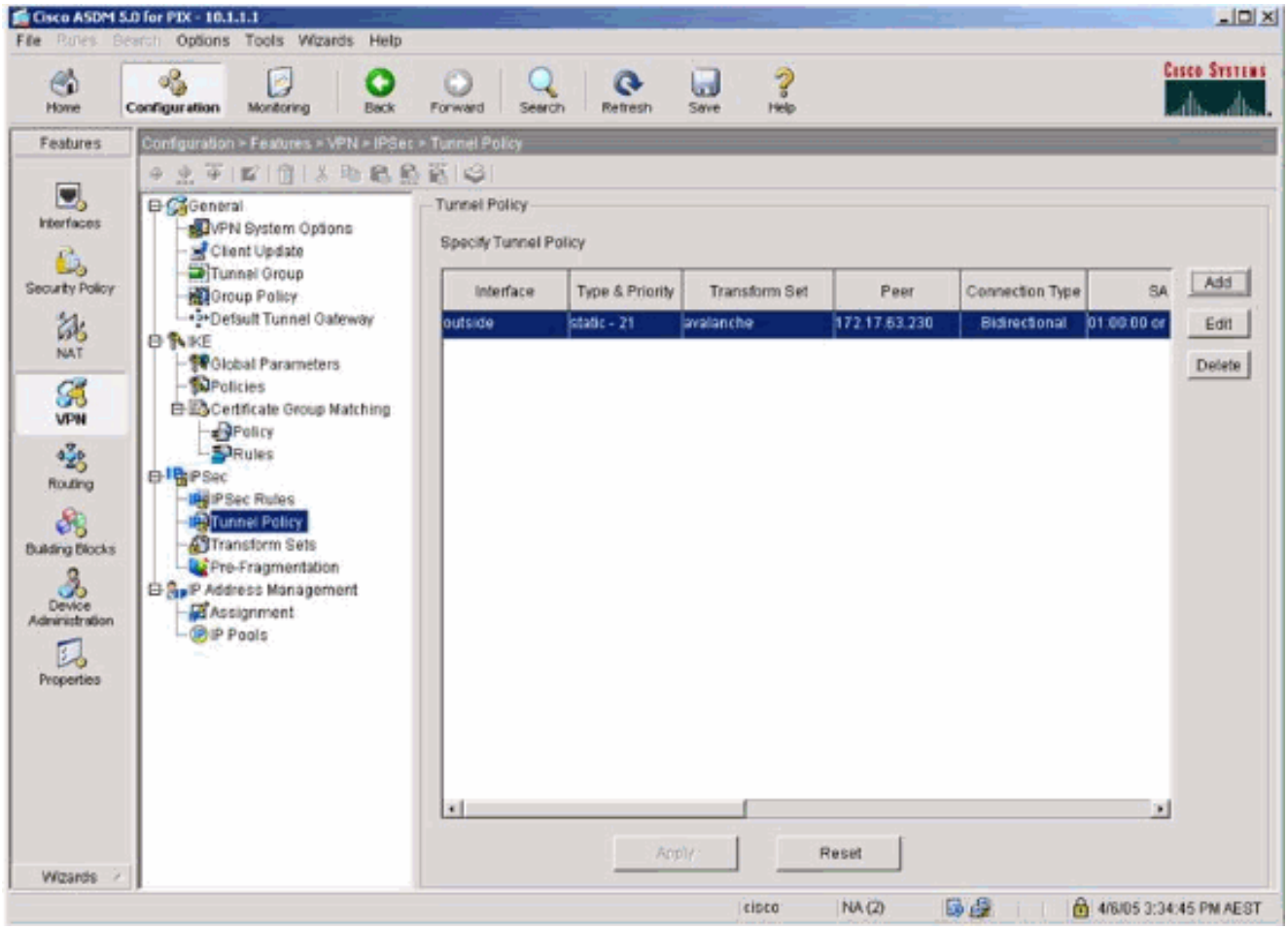
IKE.



8. Sélectionnez **VPN > IPsec > IPsec Rules** et choisissez **IPsec** pour le tunnel local et l'adressage
distant.

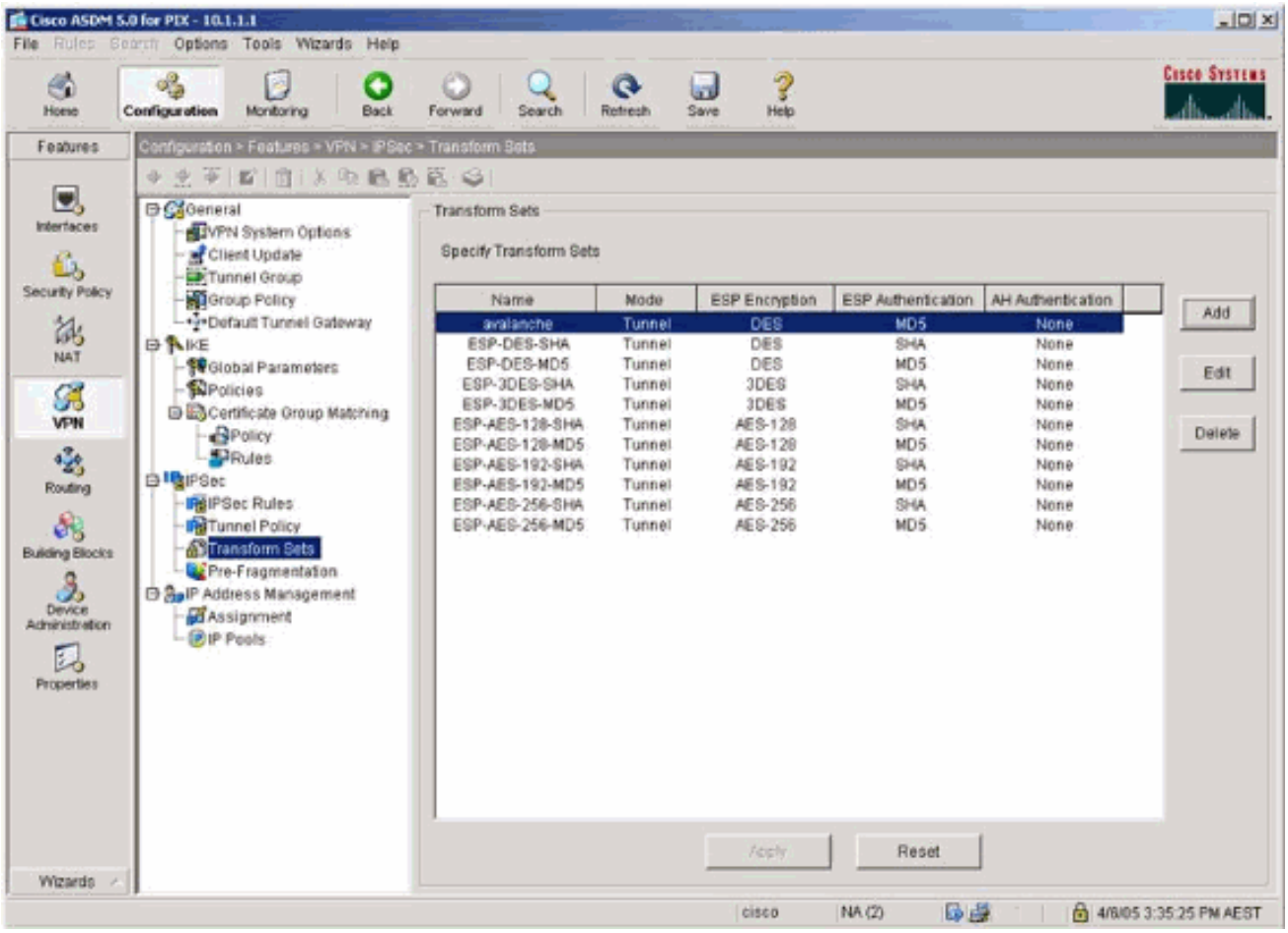


9. Sélectionnez **VPN > IPsec > Tunnel Policy** et choisissez la stratégie de tunnel.

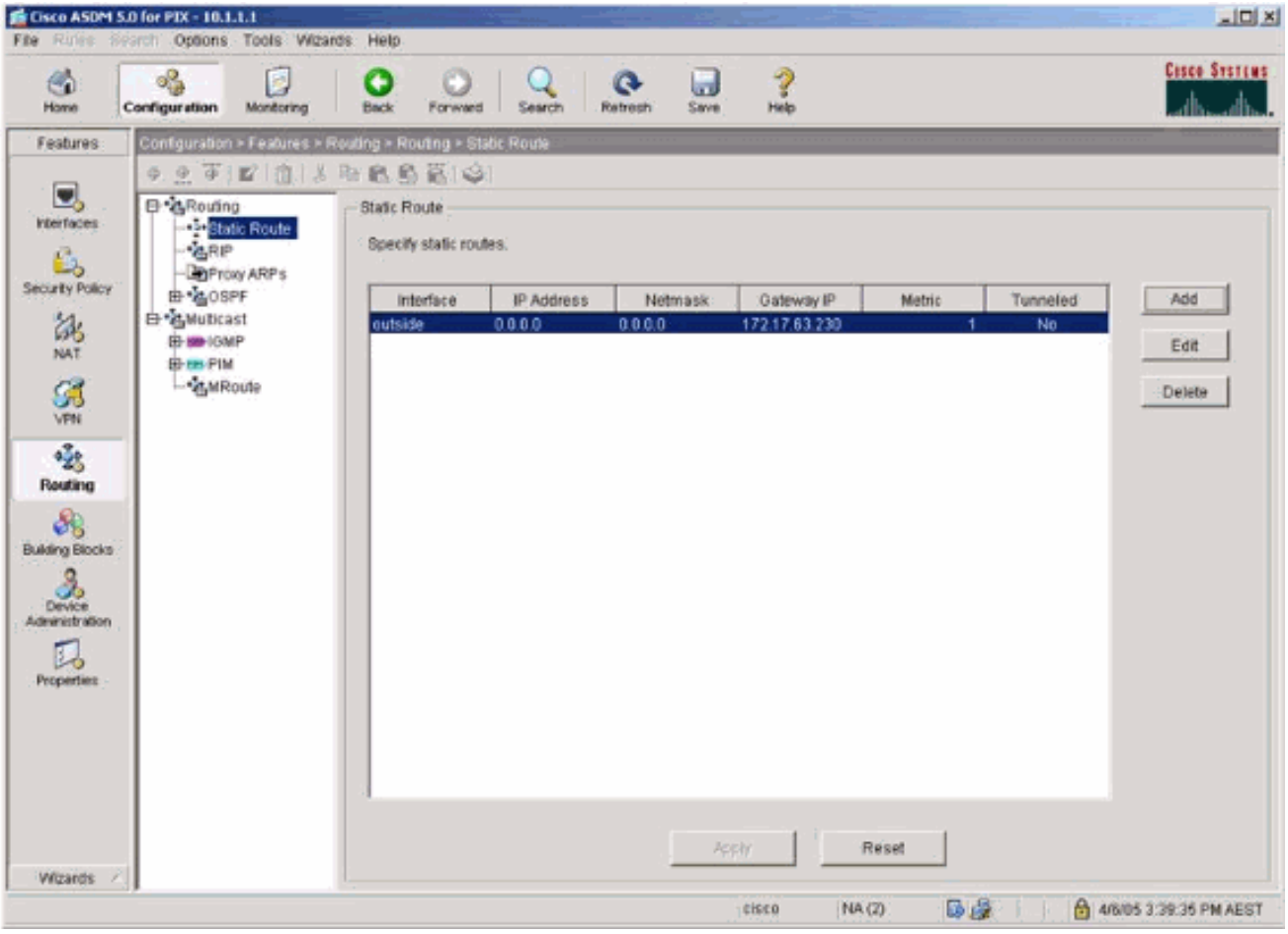


10. Sélectionnez **VPN > IPsec > Transform Sets** et choisissez un jeu

Transform.



11. Sélectionnez **Routing > Routing > Static Route** et choisissez une route statique vers le routeur de passerelle. Dans cet exemple, la route statique pointe vers l'homologue VPN distant pour plus de
simplicité.



Vérification

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.**

Dépannage

Vous pouvez utiliser ASDM pour activer la journalisation et pour afficher les journaux.

- Sélectionnez **Configuration > Properties > Logging > Logging Setup**, choisissez **Enable Logging** et cliquez sur **Apply** pour activer la journalisation.
- Sélectionnez **Monitoring > Logging > Log Buffer > On Logging Level**, choisissez **Logging Buffer**, puis cliquez sur **View** pour afficher les journaux.

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 : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug crypto ipsec : Cette commande affiche les négociations IPSec 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** : efface les associations de sécurité liées à la phase 1.
- **clear crypto sa** : efface les associations de sécurité liées à la phase 2.
- **debug icmp trace** - Indique si les requêtes ICMP des hôtes atteignent le PIX. Vous devez ajouter la commande **access-list** pour autoriser ICMP dans votre configuration afin d'exécuter ce débogage.
- **logging buffer debugging** - Affiche les connexions en cours d'établissement et refusées aux hôtes qui passent par PIX. Les informations sont stockées dans la mémoire tampon du journal PIX et vous pouvez voir la sortie avec la commande **show log**.

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)