

# Exemple de configuration d'un tunnel VPN IPsec PIX/ASA (version 7.x et ultérieure) avec traduction d'adresses réseau

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Produits connexes](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Dispositifs de sécurité et configuration de liste d'accès PIX](#)

[Dispositifs de sécurité PIX et configuration MPF \(cadre de stratégie modulaire\)](#)

[Vérifiez](#)

[Dépannez](#)

[Commandes de dépannage pour le routeur IPsec](#)

[Effacer les associations de sécurité.](#)

[Commandes de dépannage pour PIX](#)

[Informations connexes](#)

## [Introduction](#)

Cet exemple de configuration montre un tunnel VPN IPsec passant à travers un pare-feu qui exécute la traduction d'adresses de réseau (NAT). **Cette configuration ne fonctionne pas avec la translation d'adresses d'adresse du port (PAT) si vous utilisez des versions logicielles de Cisco IOS® plus tôt qu'et pas comprenant 12.2(13)T.** Ce type de configuration peut être utilisé pour percer un tunnel le trafic IP. Cette configuration ne peut pas être utilisée pour chiffrer le trafic qui ne passe pas par un Pare-feu, tel que l'IPX ou les mises à jour de routage. Le perçage d'un tunnel d'Encapsulation de routage générique (GRE) est un choix plus approprié. Dans cet exemple, les Routeurs de Cisco 2621 et 3660 il y a les périphériques du tunnel d'IPsec qui joignent deux réseaux privés, avec des conduits ou le Listes de contrôle d'accès (ACL) sur le PIX dans l'intervalle afin de permettre le trafic d'IPsec.

**Note:** NAT est une traduction d'adresses linéaire, à pas confondre avec PAT, une traduction de beaucoup (à l'intérieur du pare-feu) -à-un. Pour plus d'informations sur l'exécution NAT et la configuration, référez-vous à [vérifier l'exécution NAT et le dépannage NAT de base](#) ou [comment les travaux NAT](#).

**Note:** IPsec avec PAT ne pourrait pas fonctionner correctement parce que le périphérique extérieur de périphérique du tunnel ne peut pas manipuler de plusieurs tunnels d'une adresse IP. Contactez votre constructeur afin de déterminer si les périphériques de périphérique du tunnel fonctionnent avec PAT. Supplémentaire, dans le Logiciel Cisco IOS version 12.2(13)T et plus tard, la caractéristique NAT de transparence peut être utilisée pour le brevet. Pour plus de détails, référez-vous à la [transparence NAT d'IPSec](#). Référez-vous au [soutien de l'ESP d'IPSec par NAT](#) afin de se renseigner plus sur ces caractéristiques dans le Logiciel Cisco IOS version 12.2(13)T et plus tard.

**Note:** Avant que vous ouvriez une valise avec le support technique de Cisco, référez-vous aux [forums aux questions NAT](#), qui a beaucoup de réponses aux questions communes.

Référez-vous à [configurer un tunnel d'IPSec par un Pare-feu avec NAT](#) pour plus d'informations sur la façon configurer le tunnel d'IPsec par le Pare-feu avec NAT sur la version de PIX 6.x et plus tôt.

## [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 :

- Version du logiciel Cisco IOS 12.0.7.T (jusqu'à la limite du Logiciel Cisco IOS version 12.2(13)T) Pour des versions plus récentes, référez-vous à la [transparence NAT d'IPSec](#).
- Routeur de Cisco 2621
- Routeur de Cisco 3660
- Cisco PIX 500 Series Security Appliance qui exécute 7.x et en haut.

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](#).

### [Produits connexes](#)

Ce document peut également être utilisé avec l'appliance de sécurité adaptable de gamme Cisco 5500 (ASA) avec la version de logiciel 7.x et plus tard.

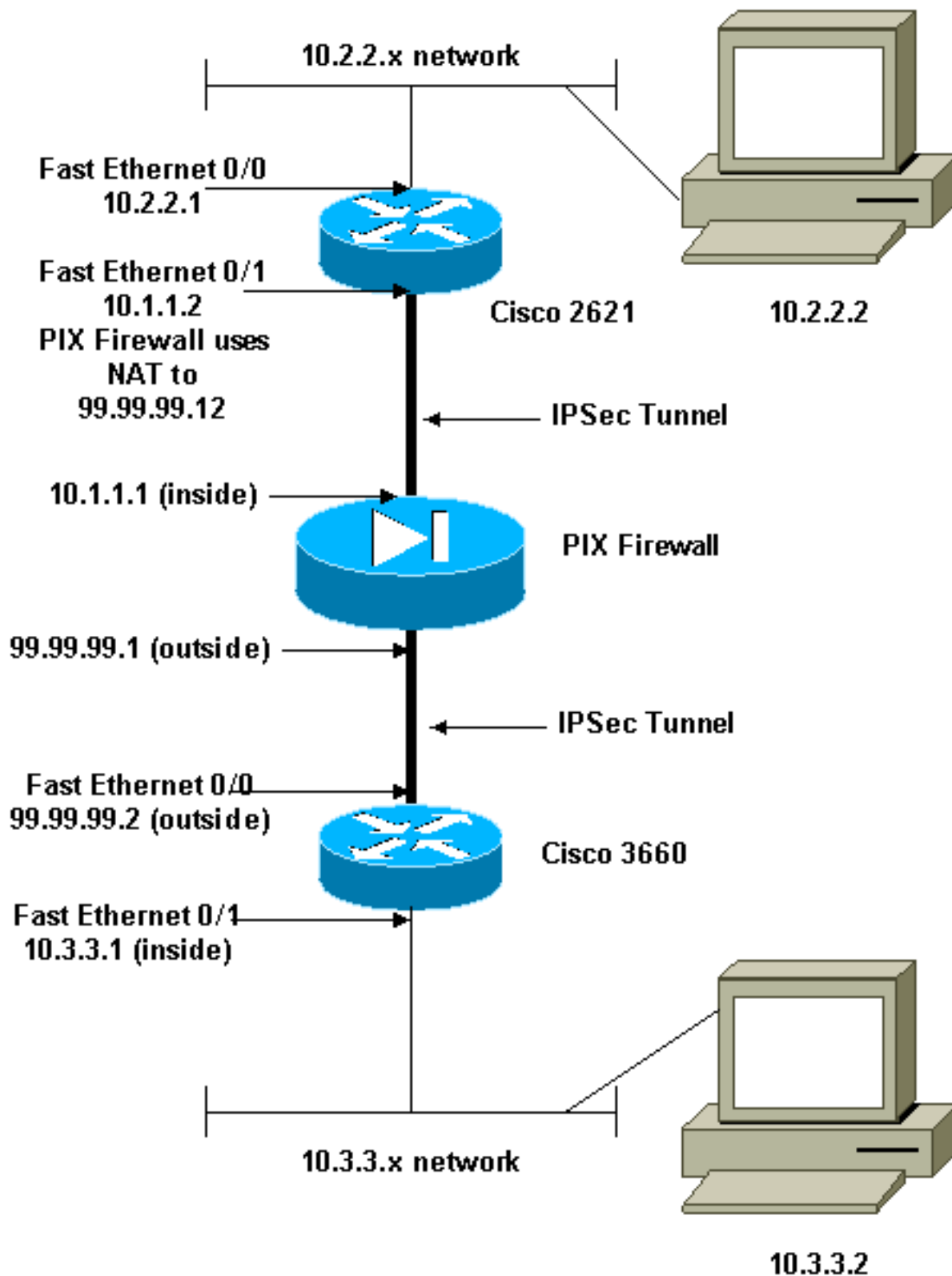
## [Configurez](#)

Cette section vous présente avec les informations que vous pouvez employer pour configurer les caractéristiques ce document décrit.

**Note:** Afin de trouver des informations complémentaires sur les commandes que ce document utilise, veuillez utiliser le [Command Lookup Tool](#) (clients [enregistrés](#) seulement).

## Diagramme du réseau

Ce document utilise la configuration réseau suivante :



## Configurations

Ce document utilise les configurations suivantes :

- [Configuration de Cisco 2621](#)
- [Configuration de Cisco 3660](#)
- [Dispositifs de sécurité et configuration de liste d'accès PIX Configuration GUI de gestionnaire de périphériques de sécurité avancée \(ASDM\) Configuration de l'interface de ligne de commande \(CLI\)](#)
- [Dispositifs de sécurité PIX et configuration MPF \(cadre de stratégie modulaire\)](#)

### Cisco 2621

Current configuration:

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname goss-2621  
!  
ip subnet-zero  
!  
ip audit notify log  
ip audit po max-events 100  
isdn voice-call-failure 0  
cns event-service server  
!  
!--- The IKE policy. crypto isakmp policy 10  
  hash md5  
  authentication pre-share  
crypto isakmp key cisco123 address 99.99.99.2  
!  
crypto ipsec transform-set myset esp-des esp-md5-hmac  
!  
crypto map mymap local-address FastEthernet0/1  
  
!--- IPsec policy. crypto map mymap 10 ipsec-isakmp  
  set peer 99.99.99.2  
  set transform-set myset  
  
!--- Include the private-network-to-private-network  
traffic !--- in the encryption process. match address  
101  
!  
controller T1 1/0  
!  
interface FastEthernet0/0  
  ip address 10.2.2.1 255.255.255.0  
  no ip directed-broadcast  
  duplex auto  
  speed auto  
!  
interface FastEthernet0/1  
  ip address 10.1.1.2 255.255.255.0  
  no ip directed-broadcast  
  duplex auto  
  speed auto
```

```
!--- Apply to the interface. crypto map mymap
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
no ip http server

!--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
line con 0
  transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end
```

## Cisco 3660

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname goss-3660
!
ip subnet-zero
!
cns event-service server
!

!--- The IKE policy. crypto isakmp policy 10
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 99.99.99.12
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/0

!--- The IPsec policy. crypto map mymap 10 ipsec-isakmp
  set peer 99.99.99.12
  set transform-set myset

!--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
!
interface FastEthernet0/0
  ip address 99.99.99.2 255.255.255.0
  no ip directed-broadcast
  ip nat outside
  duplex auto
  speed auto

!--- Apply to the interface. crypto map mymap
!
interface FastEthernet0/1
  ip address 10.3.3.1 255.255.255.0
  no ip directed-broadcast
  ip nat inside
  duplex auto
```

```

speed auto
!
interface Ethernet3/0
  no ip address
  no ip directed-broadcast
  shutdown
!
interface Serial3/0
  no ip address
  no ip directed-broadcast
  no ip mroute-cache
  shutdown
!
interface Ethernet3/1
  no ip address
  no ip directed-broadcast
interface Ethernet4/0
  no ip address
  no ip directed-broadcast
  shutdown
!
interface TokenRing4/0
  no ip address
  no ip directed-broadcast
  shutdown
  ring-speed 16
!

!--- The pool from which inside hosts translate to !---
the globally unique 99.99.99.0/24 network. ip nat pool
OUTSIDE 99.99.99.70 99.99.99.80 netmask 255.255.255.0

!--- Except the private network from the NAT process. ip
nat inside source route-map nonat pool OUTSIDE
  ip classless
  ip route 0.0.0.0 0.0.0.0 99.99.99.1
  no ip http server
  !

!--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
  access-list 101 deny ip 10.3.3.0 0.0.0.255 any

!--- Except the private network from the NAT process.
access-list 110 deny ip 10.3.3.0 0.0.0.255 10.2.2.0
0.0.0.255
  access-list 110 permit ip 10.3.3.0 0.0.0.255 any
  route-map nonat permit 10
  match ip address 110
  !
line con 0
  transport input none
line aux 0
line vty 0 4
!
end

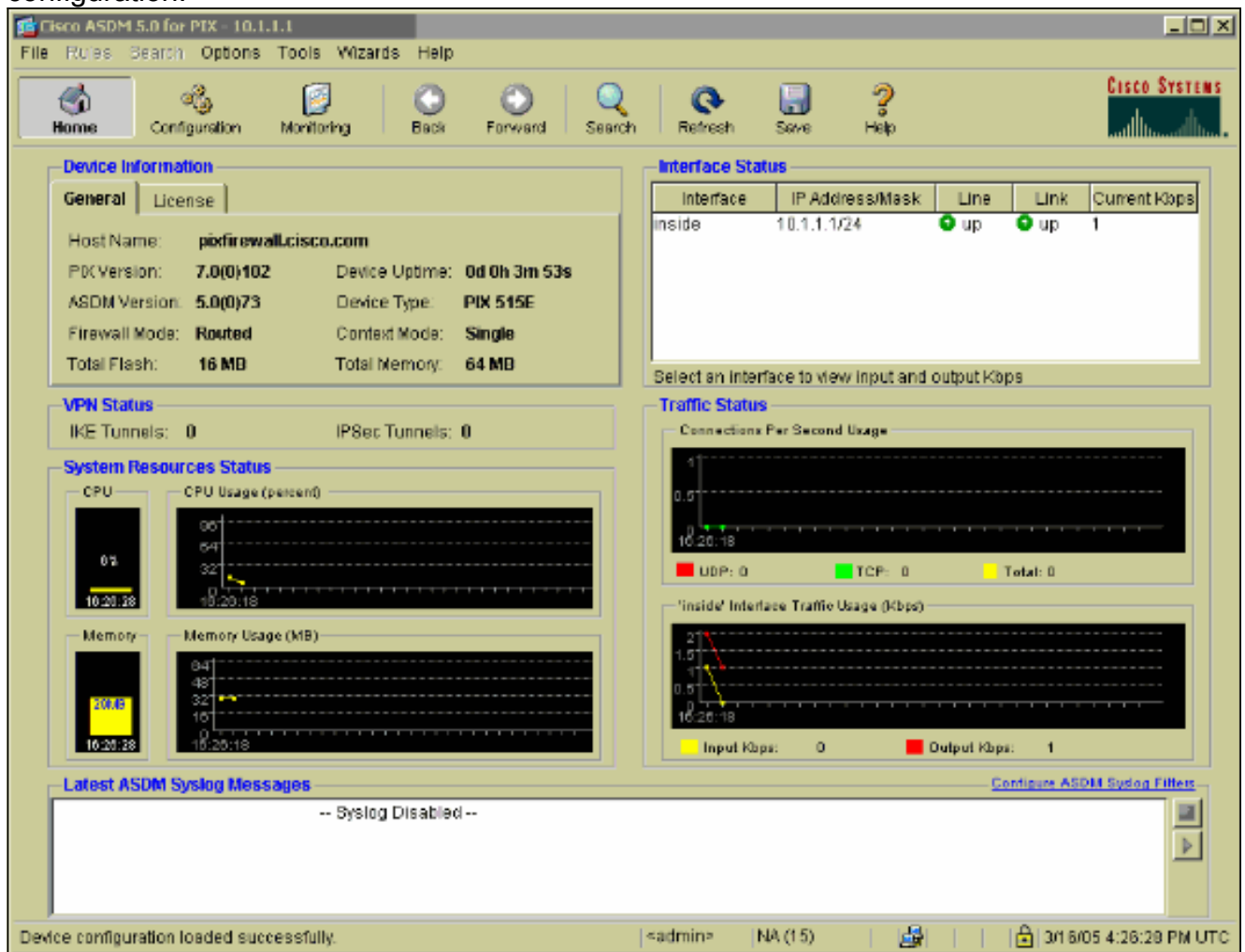
```

## [Dispositifs de sécurité et configuration de liste d'accès PIX](#)

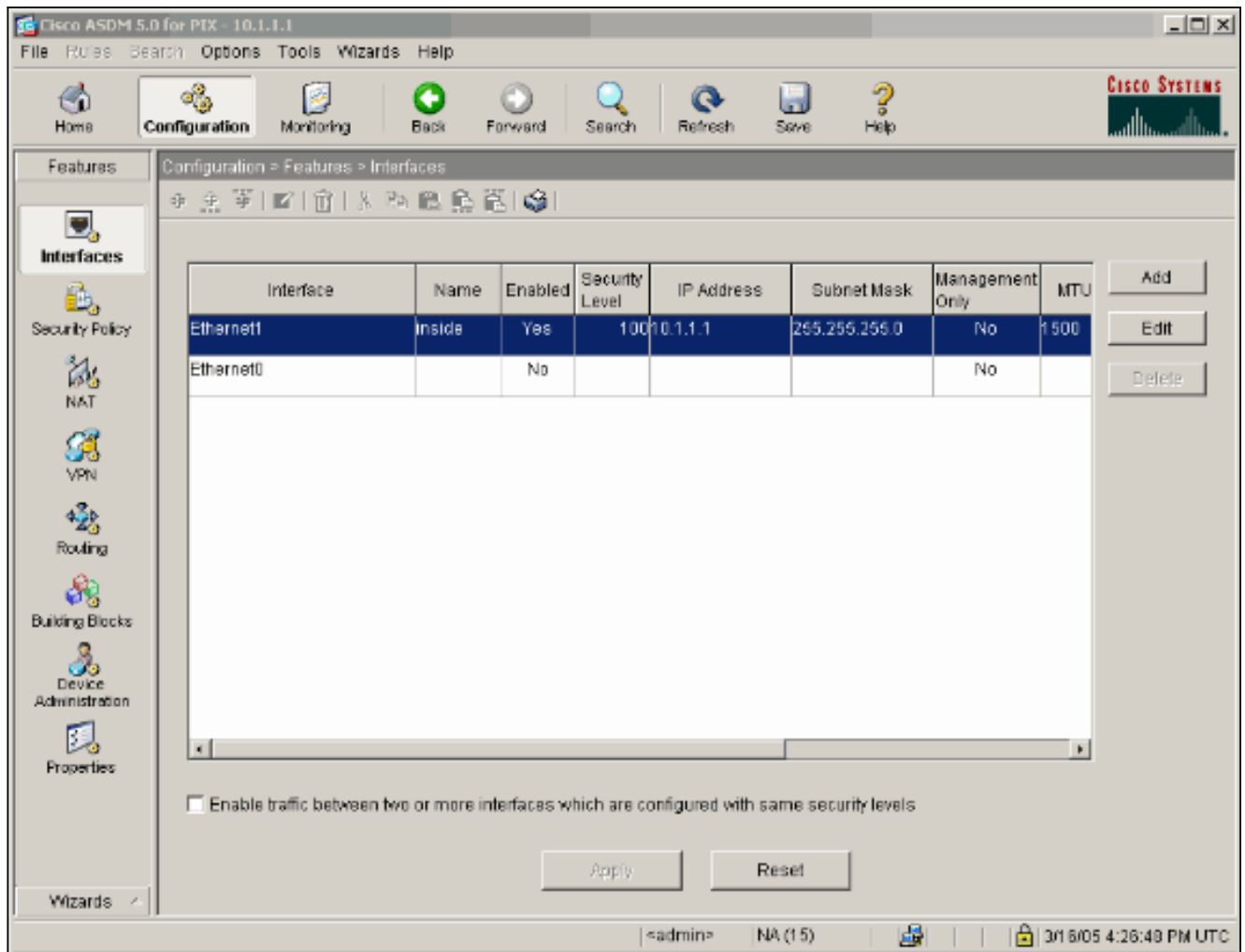
### [Configuration ASDM 5.0](#)

Terminez-vous ces étapes afin de configurer la version 7.0 de Pare-feu PIX utilisant l'ASDM.

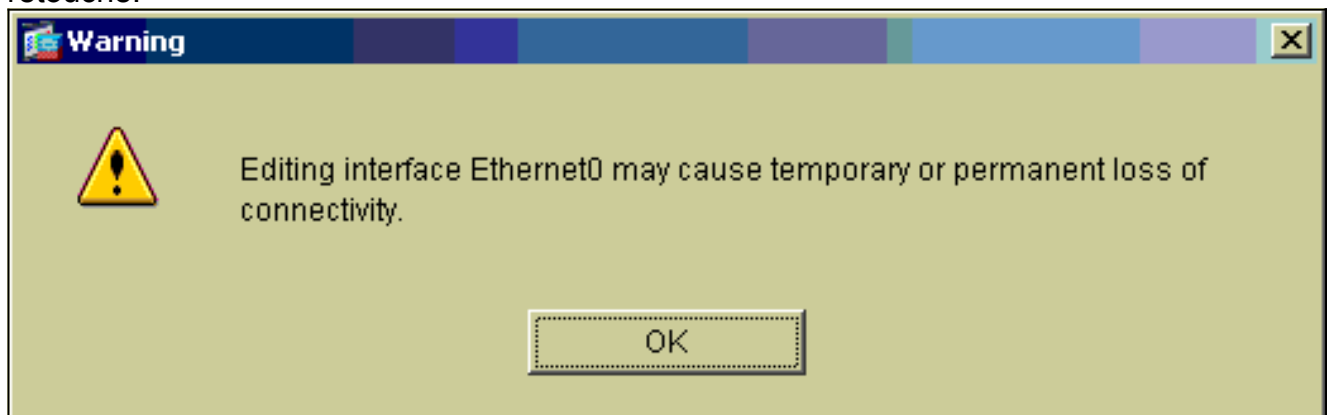
1. Console dans le PIX. D'une configuration effacée, employez les demandes interactives pour activer **GUI de gestionnaire de périphériques de sécurité avancée (ASDM)** pour la Gestion du PIX du poste de travail 10.1.1.3.
2. Du poste de travail 10.1.1.3, ouvrez un navigateur Web et utilisez ASDM (dans cet exemple, <https://10.1.1.1>).
3. Choisissez **oui** sur les demandes et la procédure de connexion de certificat avec le mot de passe d'enable comme configuré dans la [configuration de bootstrap du Pare-feu ASDM PIX](#).
4. Si c'est la première fois l'ASDM est exécuté sur le PC, il vous incite si utiliser le lanceur ASDM, ou utiliser l'ASDM comme app de Javas. Dans cet exemple, le lanceur ASDM est sélectionné et installe ces demandes.
5. Poursuivez dans la fenêtre d'accueil ASDM et sélectionnez l'onglet de configuration.



6. Mettez en valeur l'**interface d'Ethernet 0** et cliquez sur Edit afin de configurer l'interface extérieure.



7. Cliquez sur OK à la demande d'interface de retouche.



8. Écrivez les détails d'interface et cliquez sur OK quand vous êtes fait.



Hardware Port: **Ethernet0** Configure Hardware Properties...

Enable Interface  Dedicate this interface to management only

Interface Name:

Security Level:

IP Address

Use Static IP  Obtain Address via DHCP

IP Address:


Subnet Mask:

MTU:

Description:

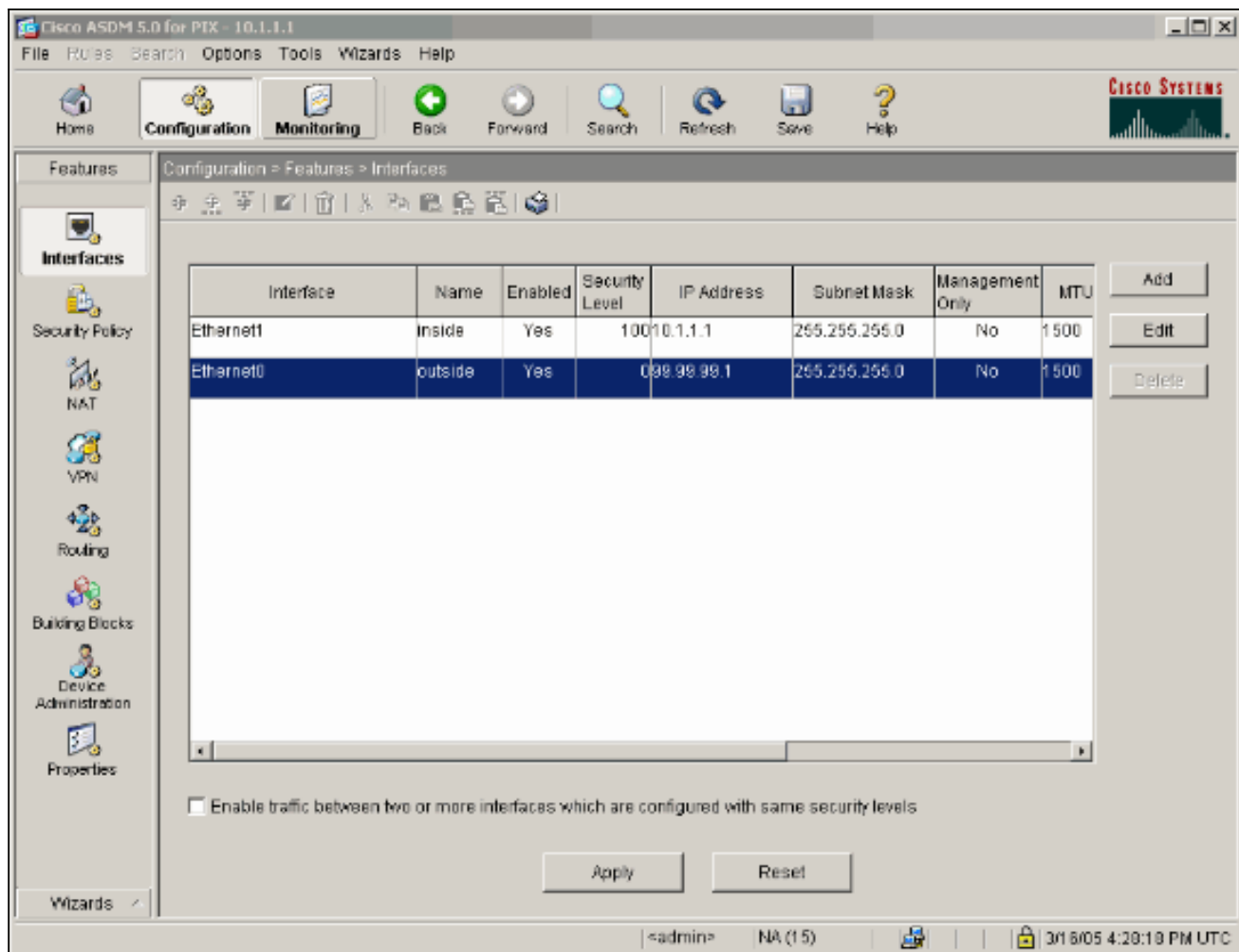
OK Cancel Help

9. Cliquez sur OK à changer une demande d'interface.

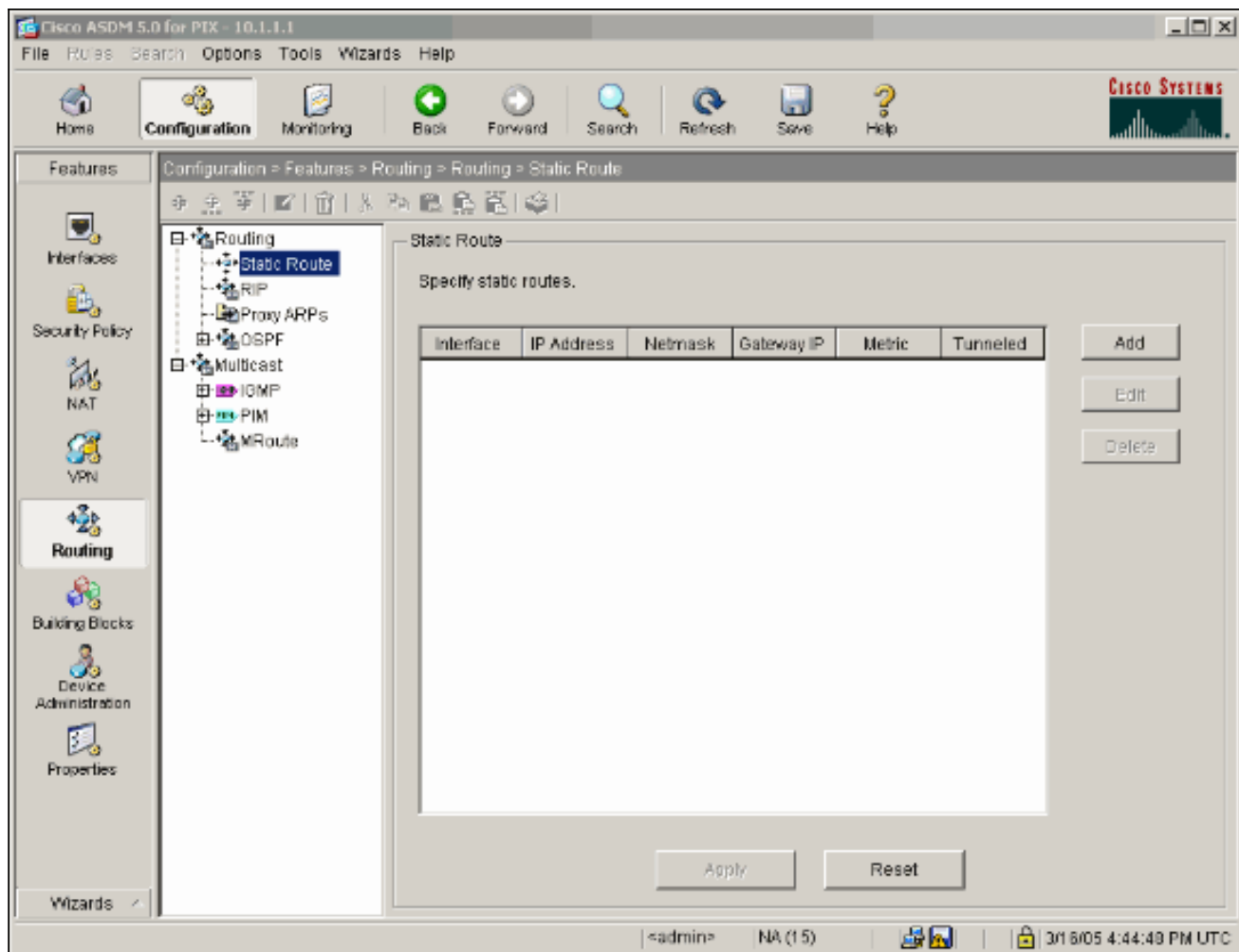
 Changing an interface's security level may cause your PIX configuration to become invalid, causing the PIX to drop legal traffic or allow illegal traffic to pass through. Do you still wish to proceed?

OK Cancel

10. Cliquez sur Apply afin de recevoir la configuration d'interface. La configuration obtient également poussé sur le PIX. Cet exemple utilise les artères statiques.



11. Cliquez sur Routing sous les caractéristiques onglet, mettez en valeur l'artère statique, et cliquez sur Add.



12. Configurez la passerelle par défaut et cliquez sur

OK.

13. Cliquez sur Add et ajoutez les artères aux réseaux

**Add Static Route**

Interface Name:

IP Address:

Mask:

Gateway IP:

Metric

Tunneled (Used only for default route)

OK Cancel Help

intérieurs.

14. Confirmez que les artères correctes sont configurées et cliquez sur Apply.

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

Features

Configuration = Features > Routing > Routing > Static Route

Routing

- Static Route
- RIP
- Proxy ARP's
- OSPF
- Multicast
- IGMP
- PIM
- MRoute

Static Route

Specify static routes.

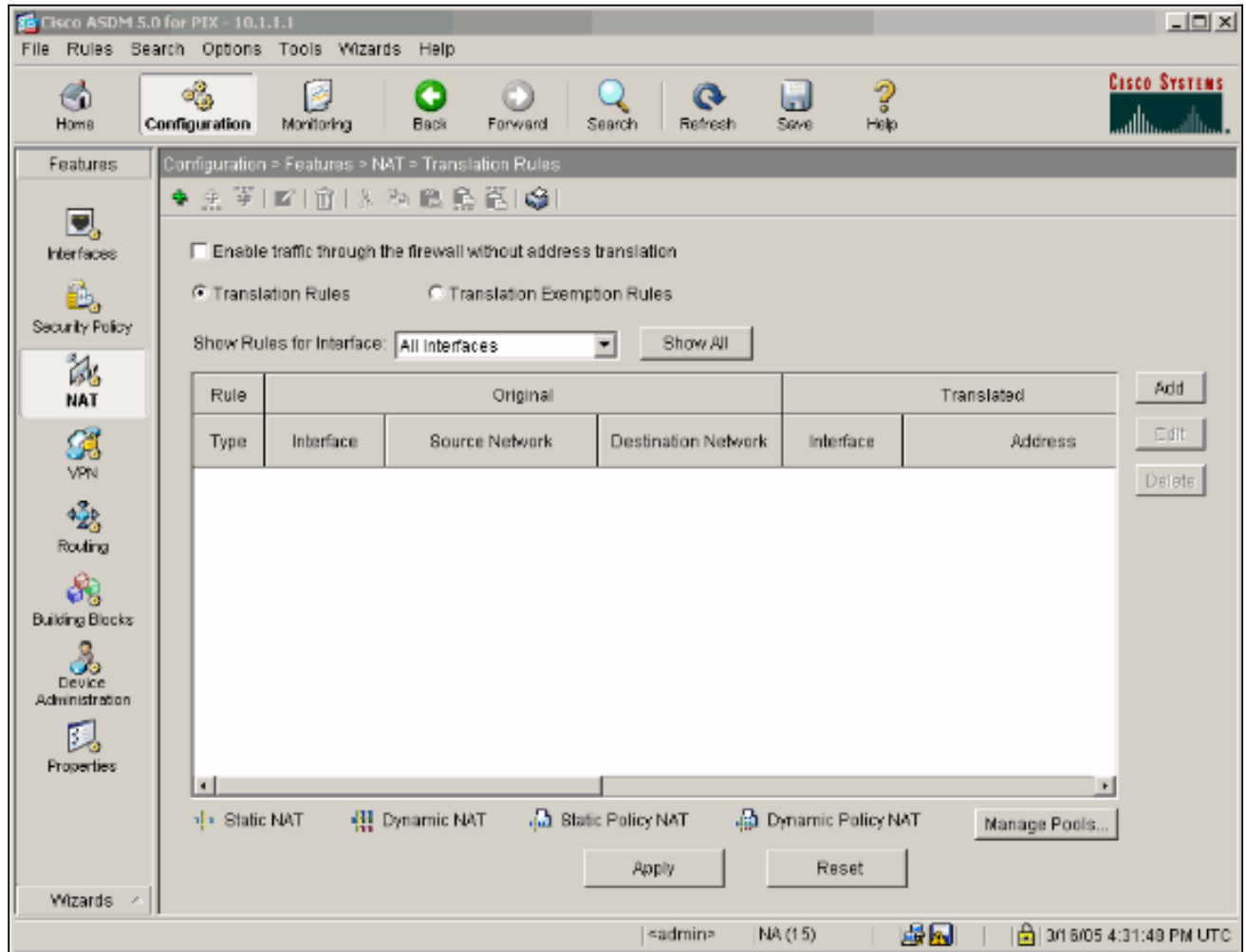
Interface	IP Address	Netmask	Gateway IP	Metric	Tunneled
outside	0.0.0.0	0.0.0.0	99.99.99.2	1	No
inside	10.2.2.0	255.255.2...	10.1.1.2	1	N/A

Add Edit Delete

Apply Reset

<admin> NA (15) 3/1 6/05 4:46:49 PM UTC

15. Dans cet exemple, NAT est utilisé. Retirez le contrôle sur la case pour l'**Enable traffic through the firewall without address translation** et cliquez sur Add afin de configurer la règle NAT.



16. Configurez le réseau de source (cet exemple use). Cliquez sur alors **parviennent des groupes** afin de définir PAT.

**Add Address Translation Rule**

Use NAT       Use Policy NAT

Source Host/Network


Interface:

IP Address:

Mask:


Translate Address on Interface:

Translate Address To

 **Static**      IP Address:

Redirect port

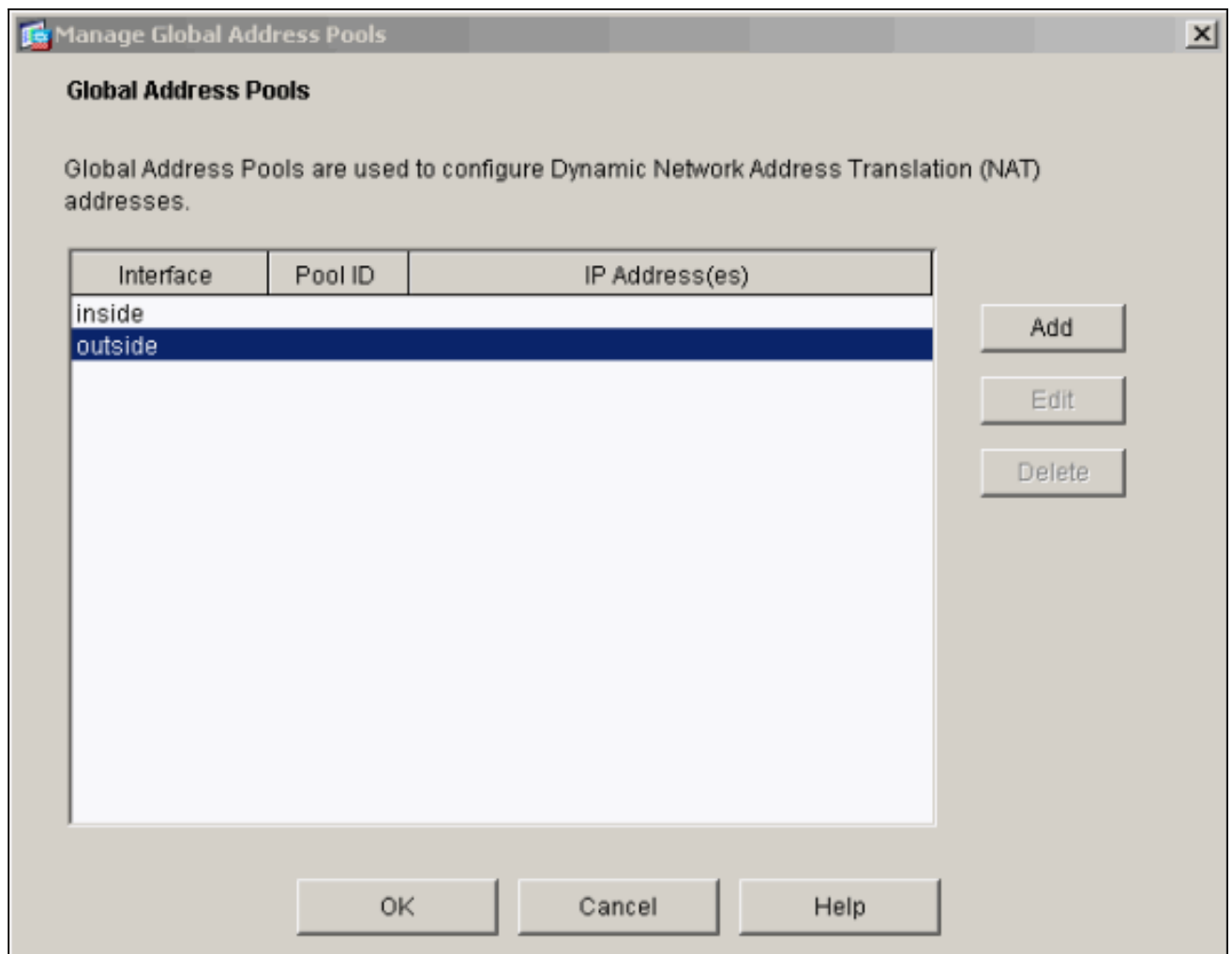
TCP      Original port:       Translated port: 
  
 UDP

 **Dynamic**      Address Pool:      

Pool ID	Address
N/A	No address pool defined

17. Sélectionnez l'interface **extérieure** et cliquez sur Add.



Cet exemple utilise PAT utilisant l'adresse IP de l'interface.

**Add Global Pool Item**

Interface:  Pool ID:

Range

Port Address Translation (PAT)

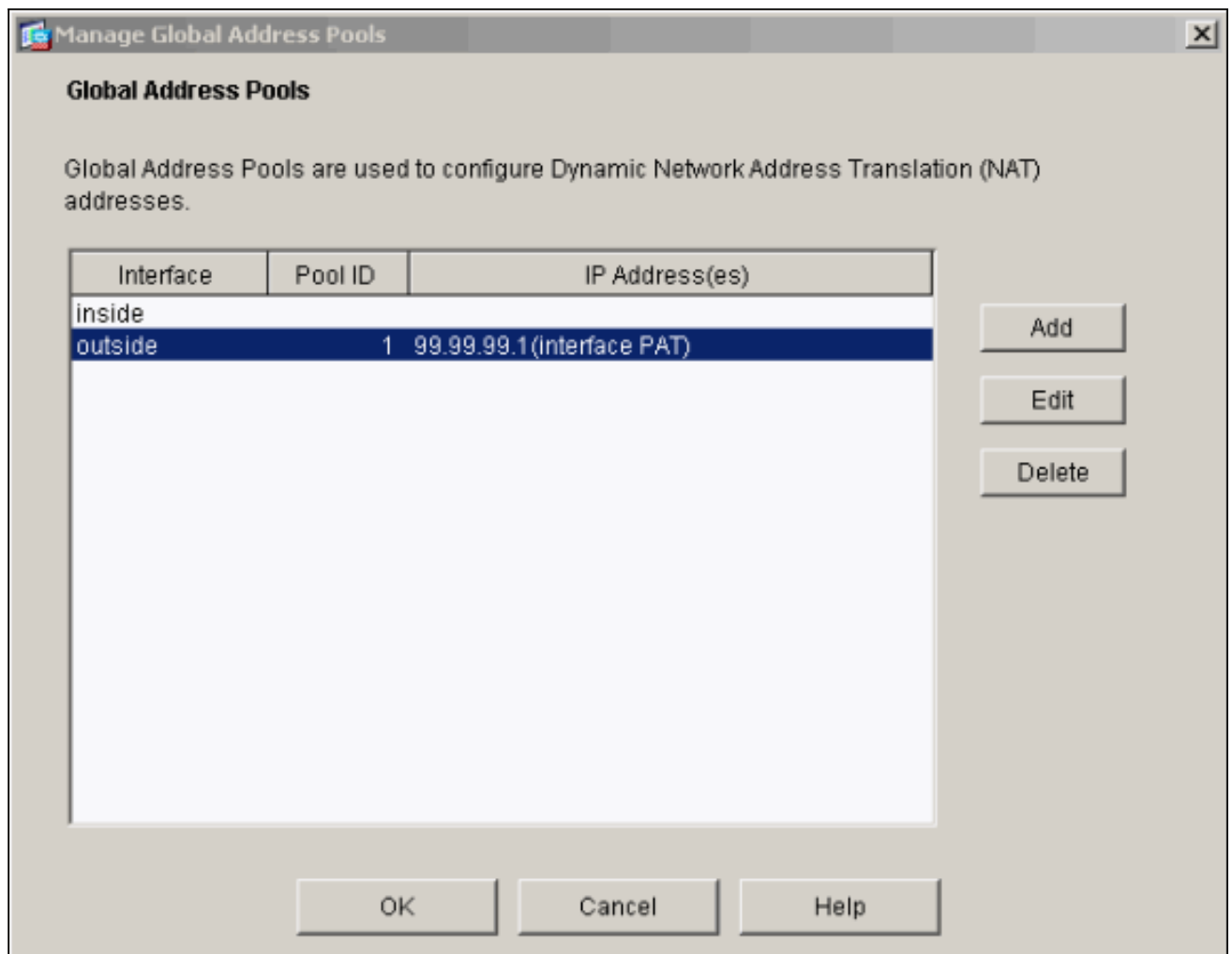
Port Address Translation (PAT) using the IP address of the interface

IP Address:  -

Network Mask (optional):

18. Cliquez sur OK quand PAT est configuré.





19. Cliquez sur Add afin de configurer la traduction statique.

**Add Address Translation Rule**

Use NAT   
 Use Policy NAT

Source Host/Network

Interface:

IP Address:

Mask:

Translate Address on Interface:

Translate Address To

Static    IP Address:

Redirect port

TCP    Original port:     Translated port:

UDP

Dynamic    Address Pool:    

Pool ID	Address
1	99.99.99.1 (interface PAT)

20. Sélectionnez l'intérieur sur le déroulant d'interface, puis écrivez l'adresse IP 10.1.1.2, masque de sous-réseau 255.255.255.255, choisissez la charge statique et dans l'adresse 99.99.99.12 d'extérieur de type de champ IP Address. Cliquez sur OK quand vous avez terminé.

**Add Address Translation Rule**

Use NAT    
 Use Policy NAT

Source Host/Network


Interface:

IP Address:

Mask:


Translate Address on Interface:

Translate Address To

 Static    
IP Address:

Redirect port

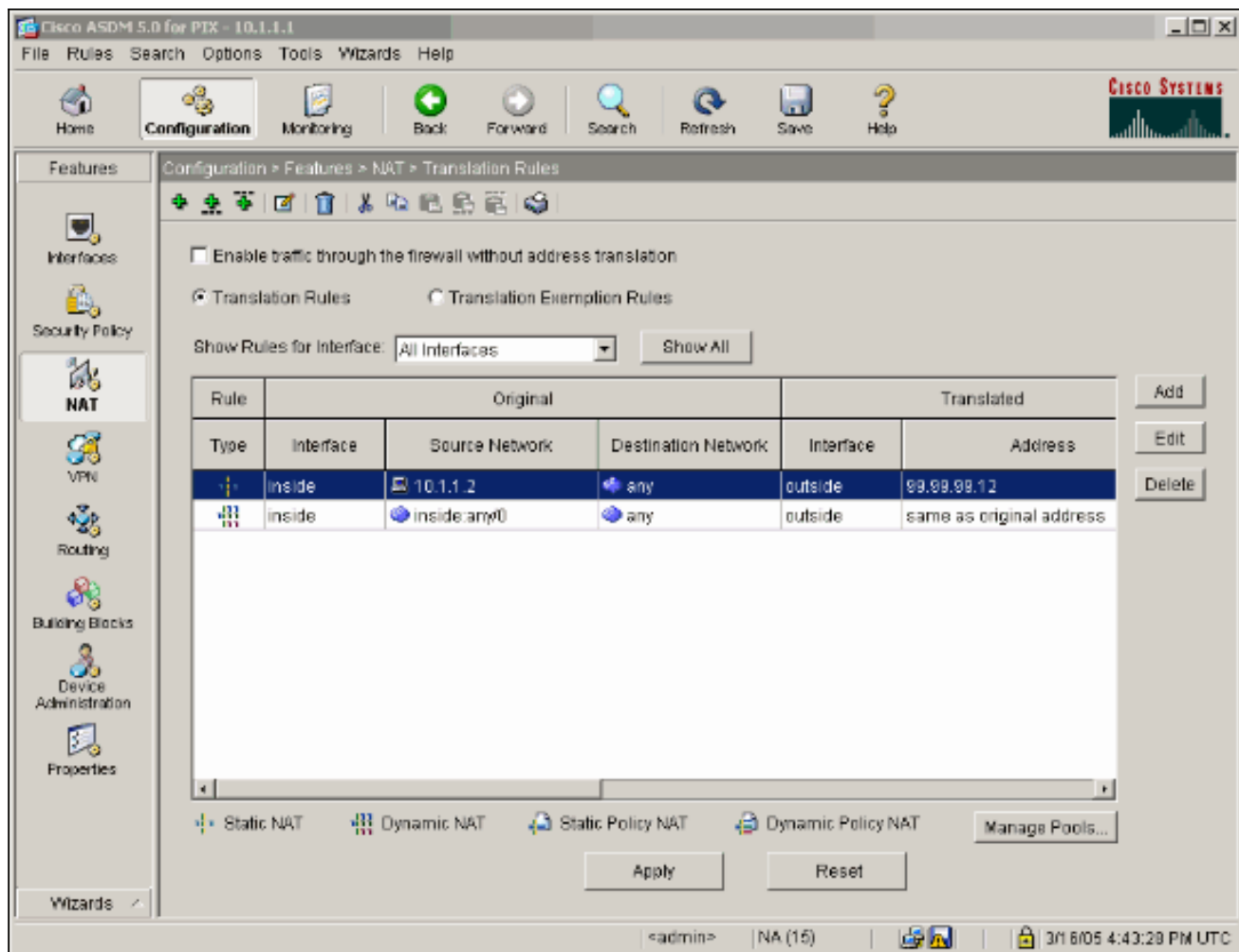
TCP    
Original port:     
Translated port:

 Dynamic    
Address Pool:     

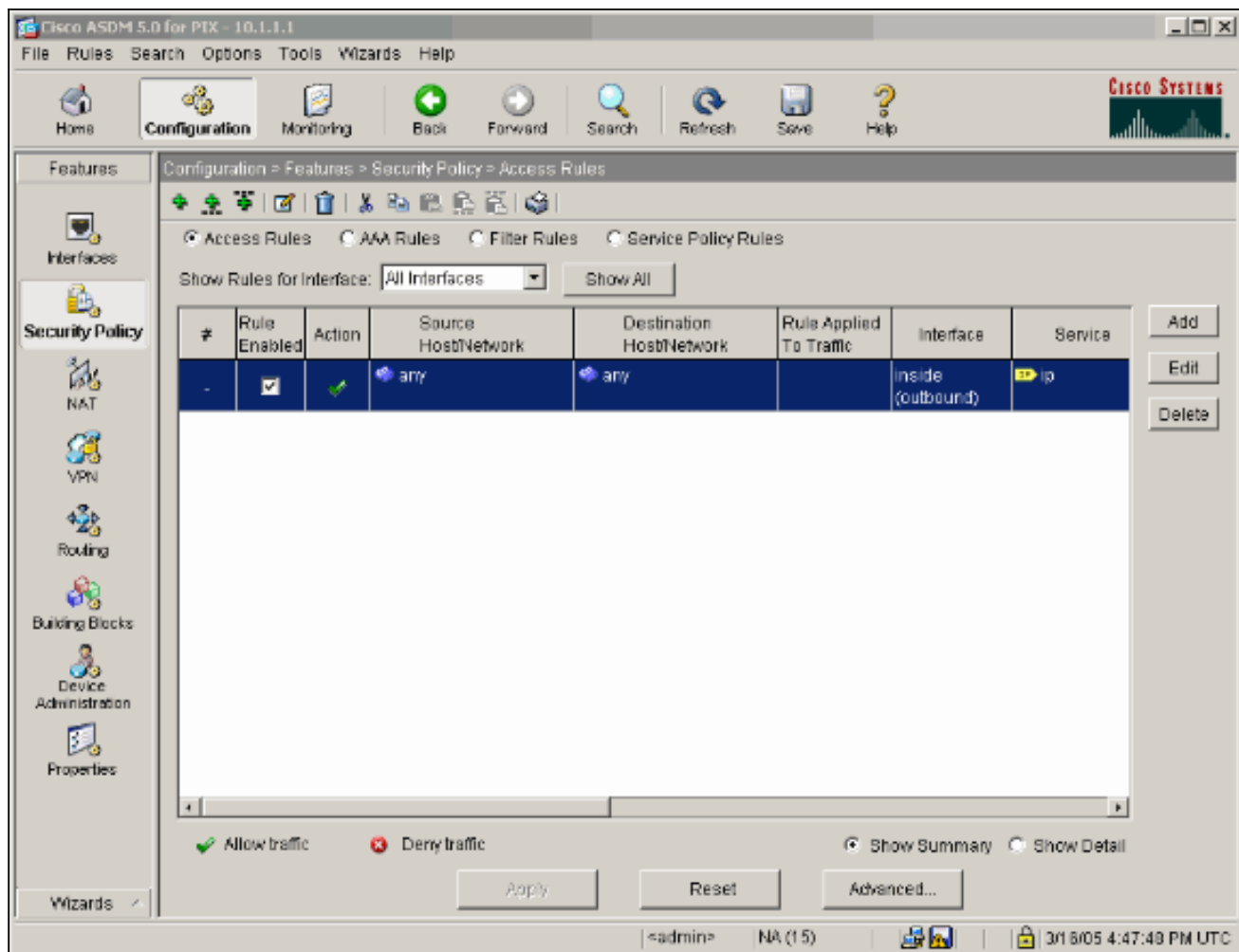
Pool ID	Address

21. Cliquez sur Apply pour recevoir la configuration d'interface. La configuration obtient également poussé sur le PIX.



22. **Stratégie de sécurité** choisie sous l'onglet de caractéristiques afin de configurer la règle de stratégie de sécurité.




23. Cliquez sur Add pour permettre le trafic de l'ESP et pour cliquer sur OK afin de continuer.

**Add Access Rule**

Action  
 Select an action:   
 Apply to Traffic:

Source Host/Network  
 IP Address  Name  Group  
 Interface:   
 IP address:  ...  
 Mask:

Destination Host/Network  
 IP Address  Name  Group  
 Interface:   
 IP address:  ...  
 Mask:

Rule Flow Diagram  
 Rule applied to traffic incoming to source interface  
  
 99.99.99.2      outside      inside      99.99.99.12  
 Allow traffic

Protocol and Service  
 TCP  UDP  ICMP  IP   
 IP Protocol  
 IP protocol:  ...

Please enter the description below (optional):

24. Cliquez sur Add afin de permettre le trafic d'ISAKMP et cliquer sur OK afin de continuer.

**Edit Access Rule**

**Action**  
 Select an action:   
 Apply to Traffic:

**Source Host/Network**  
 IP Address  Name  Group  
 Interface:   
 IP address:  ...  
 Mask:

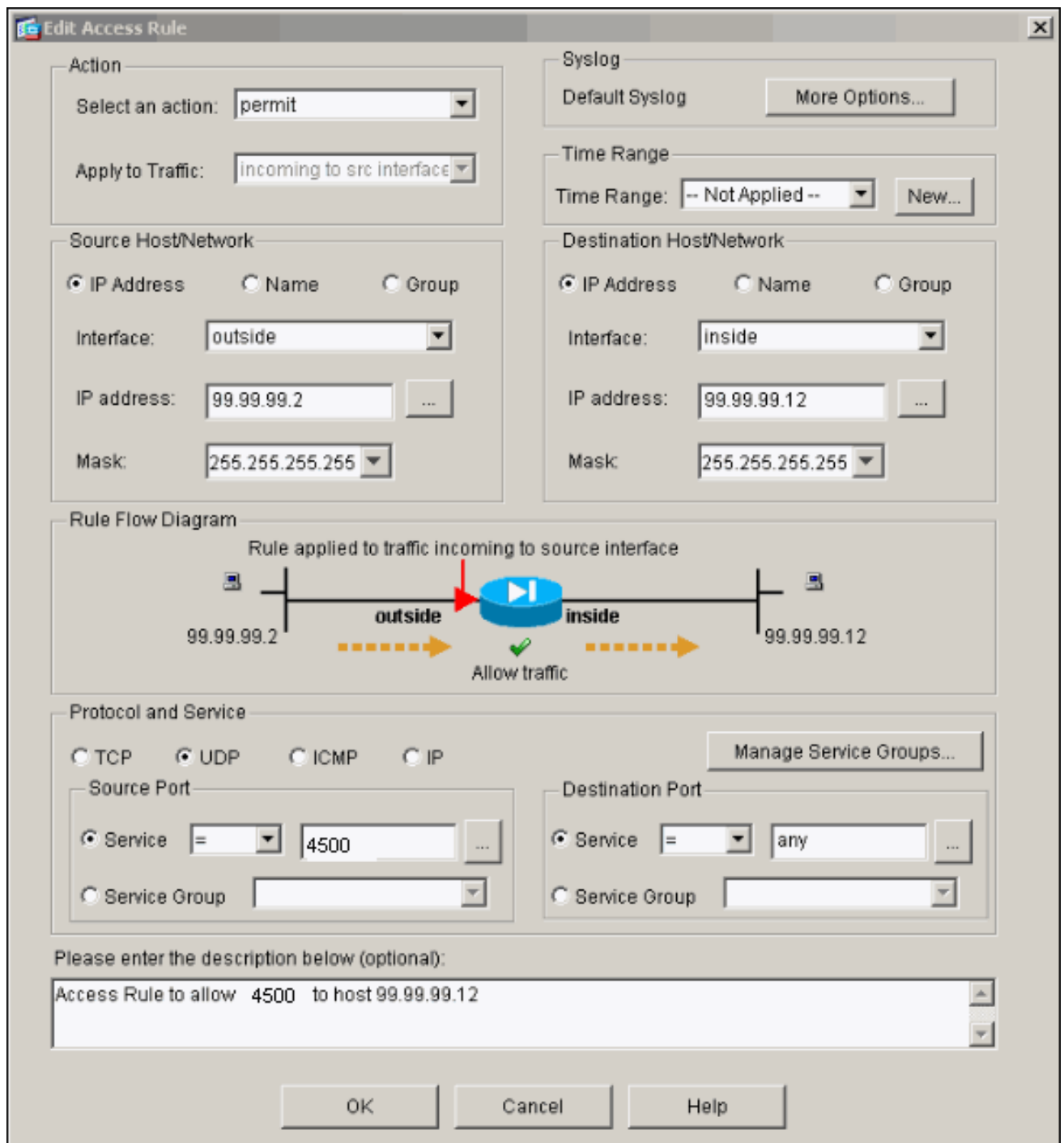
**Destination Host/Network**  
 IP Address  Name  Group  
 Interface:   
 IP address:  ...  
 Mask:

**Rule Flow Diagram**  
 Rule applied to traffic incoming to source interface  
  
 99.99.99.2      outside      inside      99.99.99.12  
 Allow traffic

**Protocol and Service**  
 TCP  UDP  ICMP  IP        
**Source Port**  
 Service =  ...  
 Service Group   
**Destination Port**  
 Service =  ...  
 Service Group

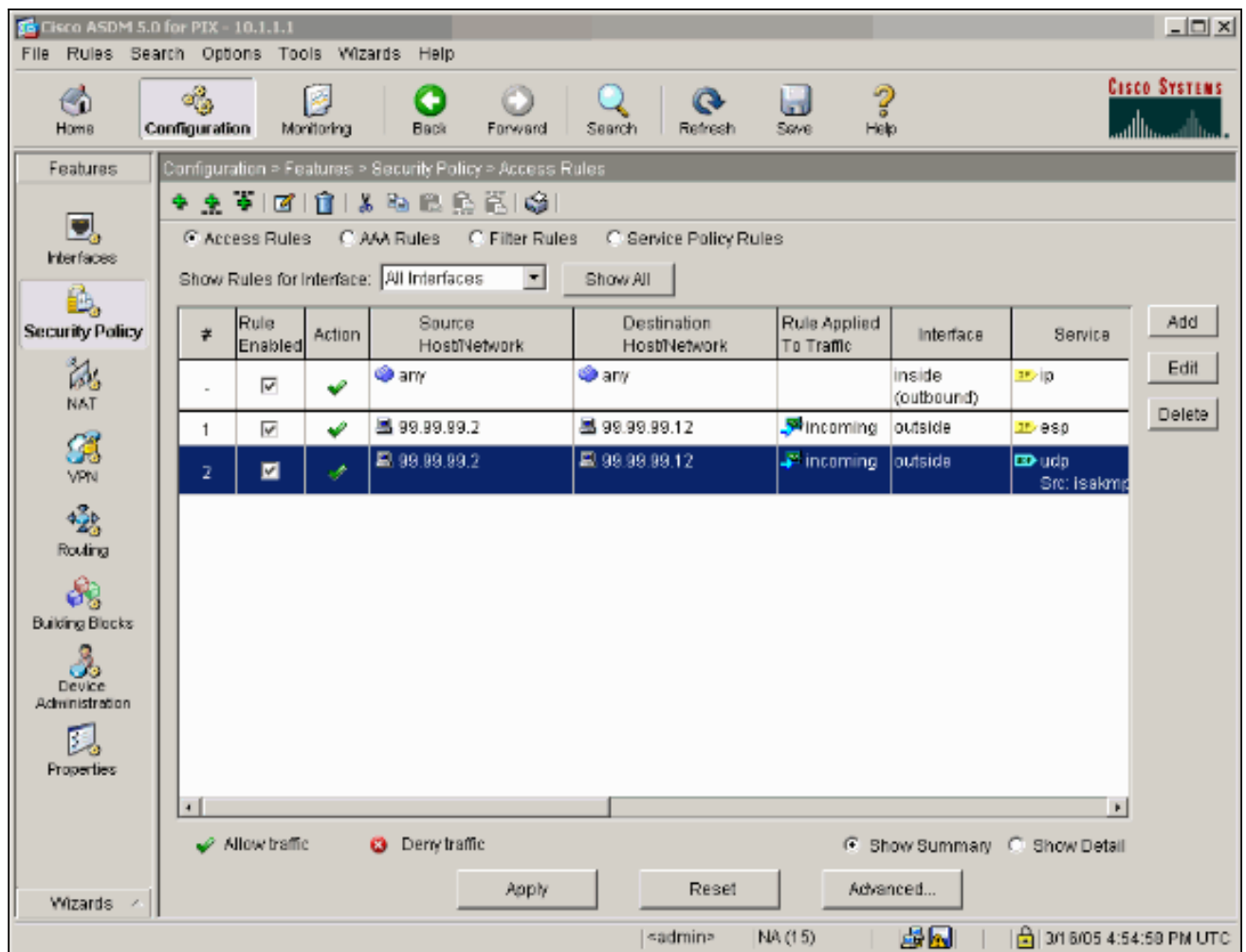
Please enter the description below (optional):

25. Cliquez sur Add afin de permettre le trafic du port UDP 4500 pour NAT-T et cliquer sur OK afin de continuer.

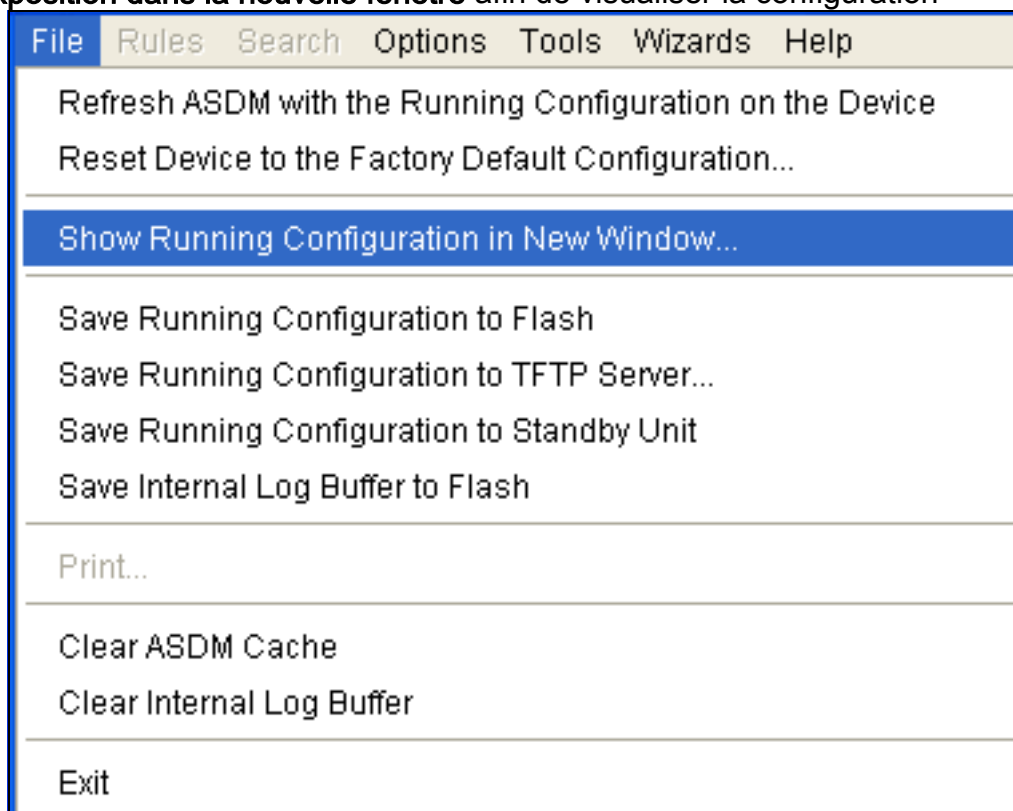


26. Cliquez sur Apply afin de recevoir la configuration d'interface. La configuration obtient également poussé sur le PIX.





27. La configuration est maintenant complète. Choisissez la **configuration en cours de fichier > d'exposition dans la nouvelle fenêtre** afin de visualiser la configuration



CLI.

## Pare-feu PIX

```
.
pixfirewall# show run
: Saved
:
PIX Version 7.0(0)102
names
↓
interface Ethernet0
  nameif outside
  security-level 0
  ip address 99.99.99.1 255.255.255.0
↓
interface Ethernet1
  nameif inside
  security-level 100
  ip address 10.1.1.1 255.255.255.0
↓
enable password 2KFOnbNIdI.2KYOU encrypted
passwd 2KFOnbNIdI.2KYOU encrypted
hostname pixfirewall
domain-name cisco.com
ftp mode passive
.
access-list outside access in remark Access Rule to
Allow ESP traffic
access-list outside access in
_____ extended permit esp host 99.99.99.2 host
99.99.99.12
.
access-list outside access in
_____ remark Access Rule to allow ISAKMP to host
99.99.99.12
access-list outside access in
_____ extended permit udp host 99.99.99.2 eq
isakmp host 99.99.99.12
.
.
access-list outside access in
_____ remark Access Rule to allow port 4500 (NAT-
T) to host 99.99.99.12
access-list outside access in
_____ extended permit udp host 99.99.99.2
eq 4500 host 99.99.99.12
pager lines 24
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 0.0.0.0 0.0.0.0
static (inside,outside) 99.99.99.12 10.1.1.2 netmask
255.255.255.255
access-group outside access in in interface outside
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1
route outside 0.0.0.0 0.0.0.0 99.99.99.2 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 mcp 0:05:00
mcp-pat
0:05:00 sip 0:30:00 sip media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 10.1.1.3 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
↓
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
↓
service-policy asa global fw policy global
Cryptochecksum:0a12956036ce4e7a97f351cde61fba7e
: end

```

## Dispositifs de sécurité PIX et configuration MPF (cadre de stratégie modulaire)

Au lieu de la liste d'accès, utilisez la commande **examiner ipsec-passage-à travers** dans MPF (cadre de stratégie modulaire) afin de passer le trafic d'IPsec par les dispositifs de sécurité PIX/ASA.

Cette inspection est configurée pour ouvrir des trous d'épingle pour le trafic de l'ESP. On permet tous les flux de données de l'ESP quand un écoulement en avant existe, et il n'y a aucune limite sur le nombre maximal de connexions qui peut être laissé. OH n'est pas laissé. Le délai d'attente de veille par défaut pour des flux de données de l'ESP est par l'ensemble par défaut à 10 minutes. Cette inspection peut être appliquée dans tous les emplacements que d'autres inspections peuvent être appliquées, qui inclut des modes de classe et de commande match. IPSec traversent l'inspection d'application fournit la traversée commode du trafic de l'ESP (protocole 50 IP) associé avec une connexion du port UDP 500 d'IKE. Il évite la configuration de liste d'accès prolongée pour permettre le trafic de l'ESP et fournit également à la Sécurité le délai d'attente et les connexions maximum. Employez le **class-map**, le **policy-map**, et les commandes de **service-stratégie** afin de définir une classe du trafic, s'appliquer la commande d'examiner à la classe, et s'appliquer la stratégie à un ou plusieurs interfaces. Une fois activé, l'**examiner IPSec-passage-à travers** la commande permet le trafic illimité de l'ESP avec un délai d'attente de 10 minutes, qui n'est pas configurable. On permet le trafic NAT et non-NAT.

```
hostname(config)#access-list test-udp-acl extended permit udp any any eq 500
hostname(config)#class-map test-udp-class
hostname(config-cmap)#match access-list test-udp-acl
hostname(config)#policy-map test-udp-policy
hostname(config-pmap)#class test-udp-class
hostname(config-pmap-c)#inspect ipsec-pass-thru
hostname(config)#service-policy test-udp-policy interface outside
```

## Vérifiez

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) ([clients enregistrés](#) uniquement), qui vous permet de voir 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.
- **active de connexions de show crypto engine** — Affiche les paquets chiffrés et déchiffrés.

## Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

### Commandes de dépannage pour le routeur IPsec

**Note:** Reportez-vous à [Informations importantes sur les commandes de débogage](#) avant d'émettre des commandes **debug**.

- **debug crypto engine** — Affiche le trafic qui est chiffré.
- **debug crypto ipsec** — Affiche les négociations IPsec de la phase 2.
- **debug crypto isakmp** — Affiche les négociations de Protocole ISAKMP (Internet Security Association and Key Management Protocol) de la phase 1.

### Effacer les associations de sécurité.

- **clear crypto isakmp** — Associations de sécurité d'Échange de clés Internet (IKE) d'espaces libres.
- **clear crypto ipsec sa** — Associations de sécurité d'IPsec d'espaces libres.

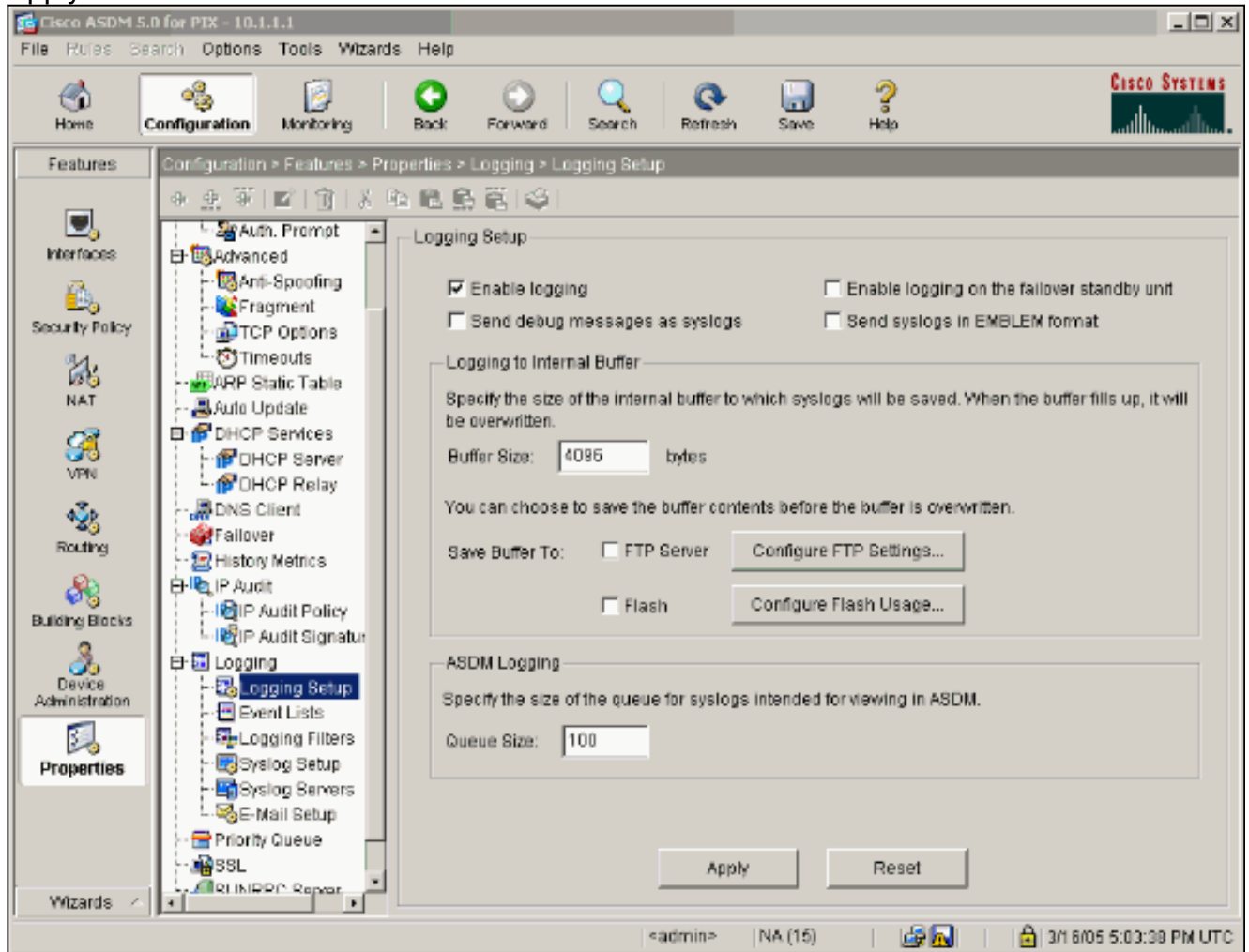
### Commandes de dépannage pour PIX

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) ([clients enregistrés](#) uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

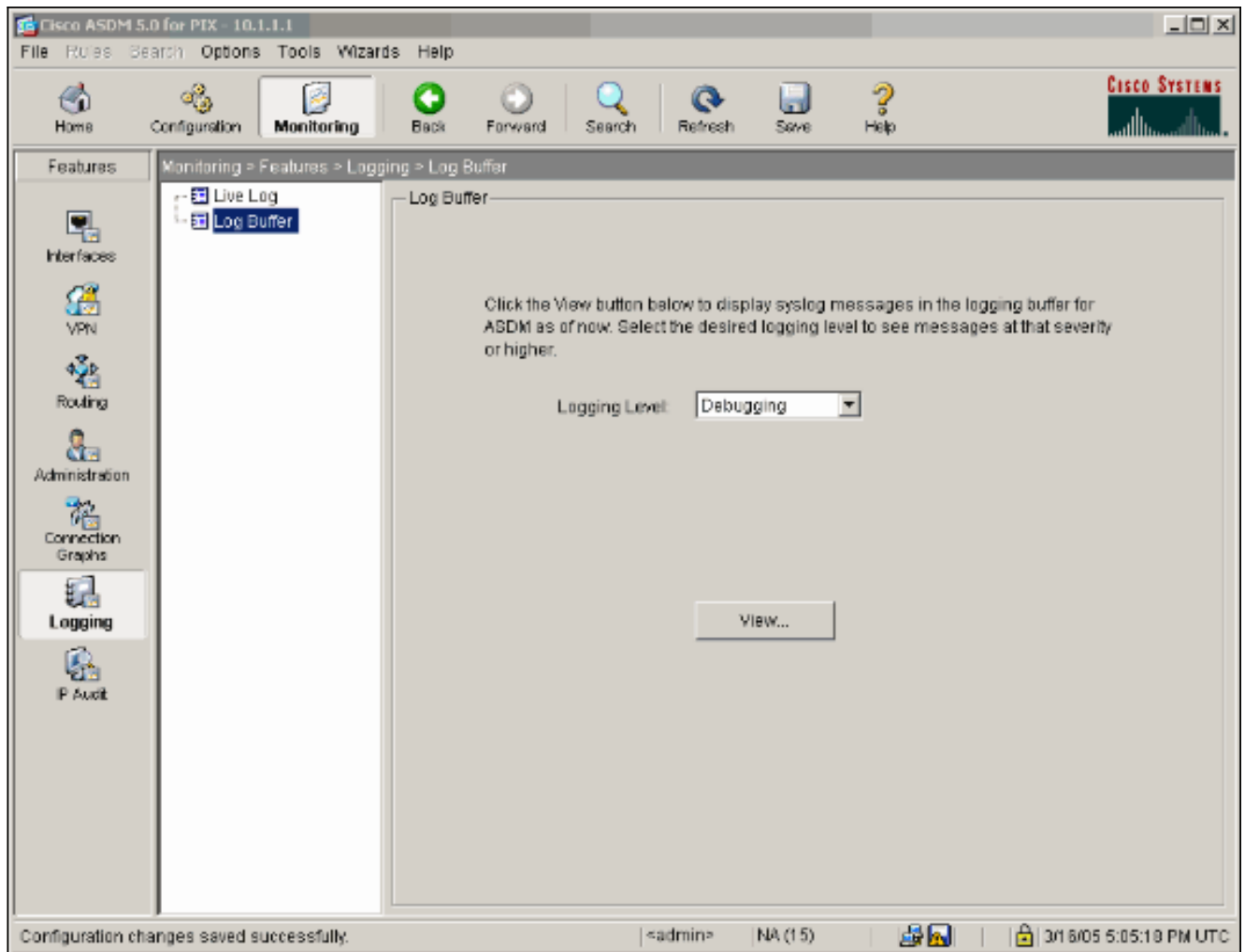
**Note:** Reportez-vous à [Informations importantes sur les commandes de débogage](#) avant d'émettre des commandes **debug**.

- **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 la sortie peut être vue utilisant le **show log command**.
- L'ASDM peut être utilisé pour activer se connecter et pour visualiser également les logs suivant les indications de ces étapes.

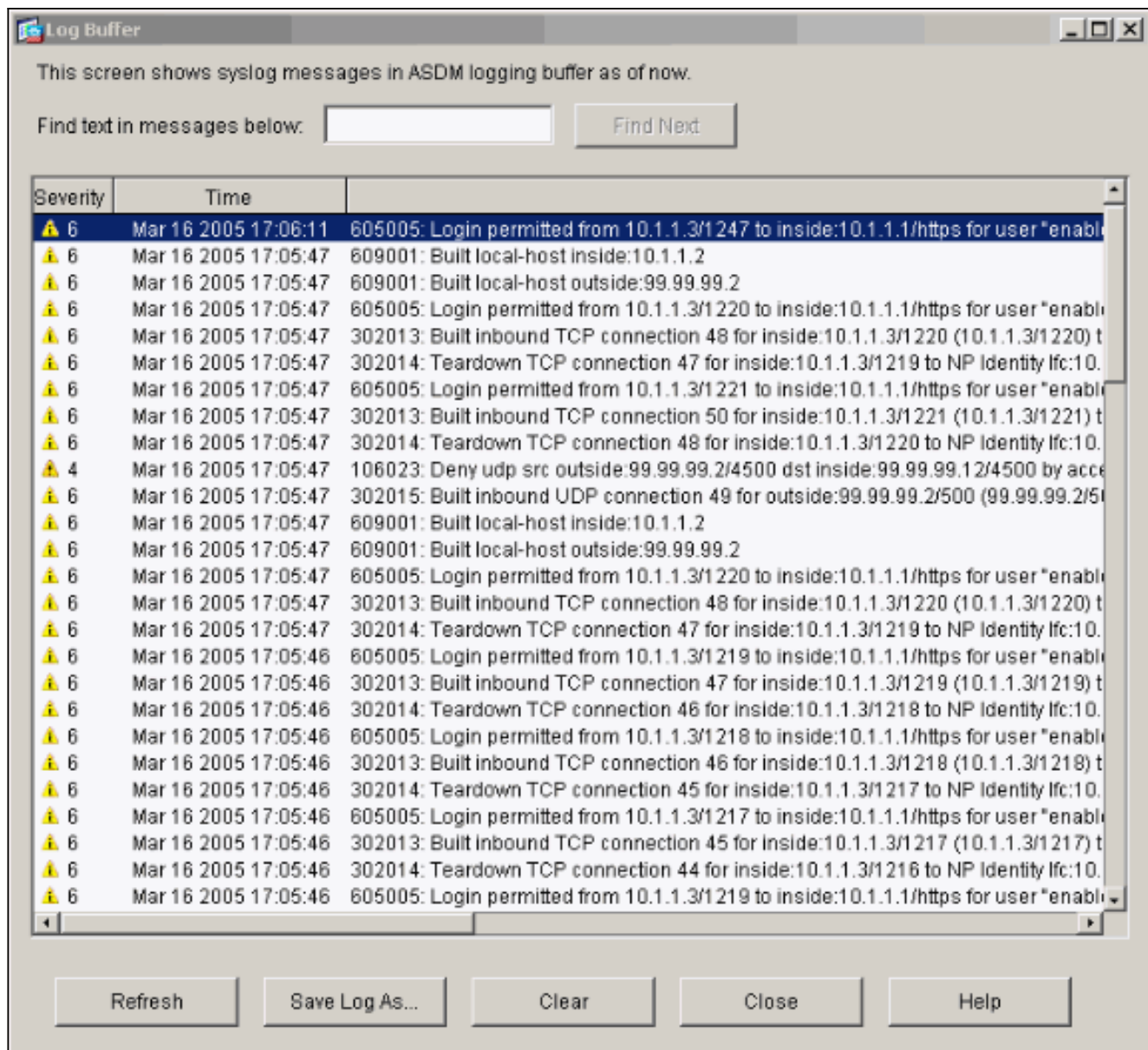
1. Choisissez la **configuration > le Properties > en se connectant > en se connectant l'installation > l'enable se connectant** et puis cliquez sur **Apply**.



2. Choisissez la **surveillance > en se connectant > mémoire tampon de log > sur se connecter le niveau > le tampon de journalisation**, puis cliquez sur la **vue**.



C'est un exemple de la mémoire tampon de log.



## [Informations connexes](#)

- [Page de support de la négociation IPSec/des protocoles IKE](#)
- [Page de support PIX](#)
- [Références des commandes du pare-feu PIX](#)
- [Page de support NAT](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)