

PIX/ASA 7.x et plus tard : Exemple de configuration de la connexion de plusieurs réseaux internes à Internet

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Produits connexes](#)

[Conventions](#)

[Configurez](#)

[Informations générales](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration PIX utilisant l'ASDM](#)

[Configuration PIX utilisant le CLI](#)

[Vérifiez](#)

[Dépannez](#)

[Dépannage des commandes](#)

[Procédure de dépannage](#)

[Incapable d'accéder à des sites Web de nom](#)

[Informations connexes](#)

Introduction

Ce document présente un exemple de configuration pour les versions 7.x et ultérieures des dispositifs de sécurité PIX/ASA dotés de plusieurs réseaux internes connectés à Internet (ou à un réseau externe) à l'aide de l'interface en ligne de commande (CLI) ou des versions 5.x et ultérieures d'Adaptive Security Device Manager (ASDM).

Référez-vous [établissent et dépannent la Connectivité par l'appliance de sécurité Cisco](#) pour les informations sur la façon dont établir et dépanner la Connectivité par PIX/ASA.

Référez-vous [utilisant nat, global, statique, conduit, et commandes access-list et Port Redirection\(Forwarding\) sur PIX](#) pour des informations sur des commandes communes PIX.

Remarque: Quelques options dans d'autres versions ASDM peuvent sembler différentes des options dans ASDM 5.1. Référez-vous à [Document ASDM](#) pour plus d'informations.

Conditions préalables

Conditions requises

Quand vous ajoutez plus d'un réseau interne derrière un Pare-feu PIX, maintenez ces points dans l'esprit :

- Le PIX ne prend en charge pas l'adressage secondaire.
- Un routeur doit être utilisé derrière le PIX afin de réaliser le routage entre le réseau existant et le réseau nouvellement ajouté.
- La passerelle par défaut de tous les hôtes doit indiquer le routeur interne.
- Ajoutez un default route sur le routeur interne ces points au PIX.
- Effacez le cache de Protocole ARP (Address Resolution Protocol) sur le routeur interne.

Référez-vous à [Permettre l'accès HTTPS pour ASDM](#) afin de permettre au périphérique d'être configuré par ASDM.

Composants utilisés

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

- Appliance 515E de Sécurité PIX avec la version de logiciel 7.1
- ASDM 5.1
- Routeurs de Cisco avec la version de logiciel 12.3(7)T de Cisco IOS®

Remarque: Ce document recertifié avec la version de logiciel 8.x PIX/ASA et la version du logiciel Cisco IOS 12.4.

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.

Produits connexes

Cette configuration peut également être utilisée avec la version 7.x et ultérieures d'appareils de Sécurité de Cisco ASA.

Conventions

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

Configurez

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.

Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Informations générales

Dans ce scénario, il y a trois réseaux internes (10.1.1.0/24, 10.2.1.0/24 et 10.3.1.0/24) à connecter à l'Internet (ou à un réseau externe) par PIX. Les réseaux internes sont connectés à l'interface interne de PIX. La connexion Internet est par un routeur qui est connecté à l'interface extérieure de PIX. Le PIX a l'adresse IP 172.16.1.1/24.

Les artères statiques sont utilisées pour conduire les paquets des réseaux internes à l'Internet et vice versa. Au lieu d'à l'aide des artères de charge statique, vous pouvez également utiliser un protocole de routage dynamique tel que le Protocole RIP (Routing Information Protocol) ou le Protocole OSPF (Open Shortest Path First).

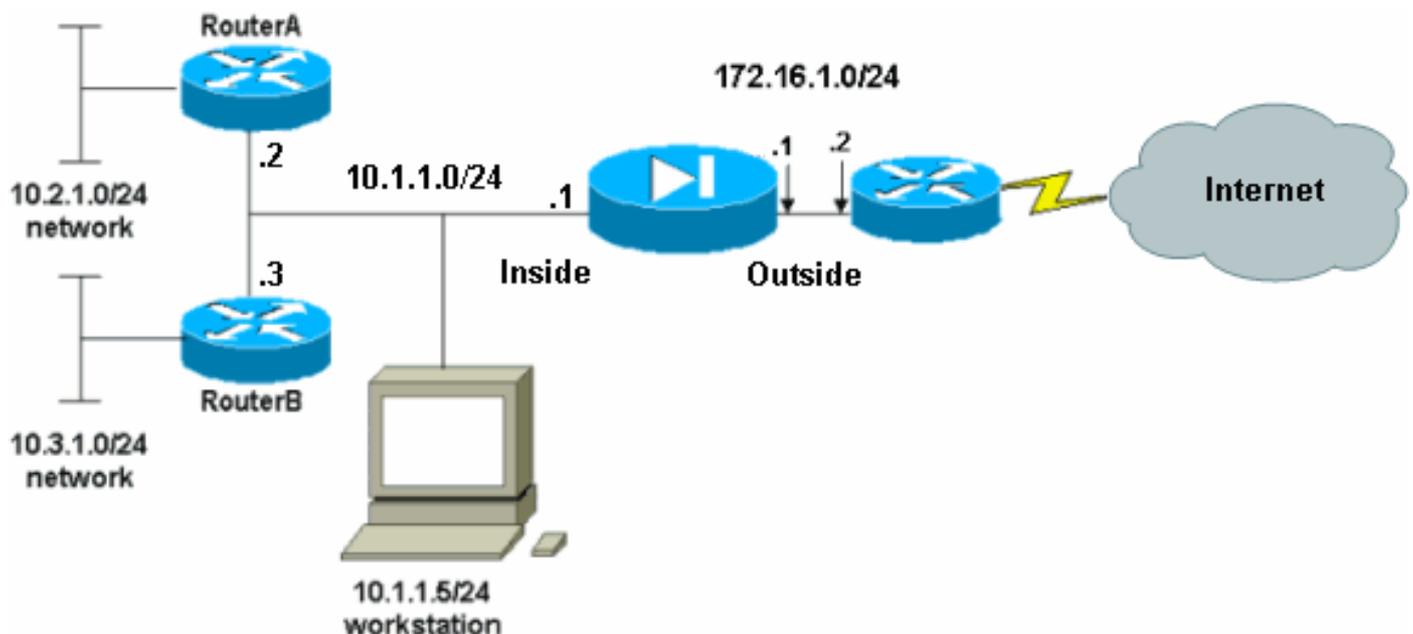
Les hôtes internes communiquent avec l'Internet en traduisant les réseaux internes sur PIX utilisant NAT dynamique (groupe d'adresses IP - 172.16.1.5 à 172.16.1.10). Si le groupe d'adresses IP est épuisé, le PIX TAPOTERA (utilisant adresse IP 172.16.1.4) les hôtes internes pour atteindre l'Internet.

Référez-vous à [PIX/ASA 7.x NAT et TAPOTEZ les déclarations](#) pour plus d'informations sur NAT/PAT.

Remarque: Si la NAT statique utilise l'adresse IP externe (global_IP) à traduire, alors cela peut entraîner une traduction. Par conséquent, utilisez le mot clé **interface** au lieu de l'adresse IP dans la traduction statique.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



La passerelle par défaut des hôtes sur le réseau de 10.1.1.0 indique le RouterA. On ajoute un

default route sur le RouterB qui indique le RouterA. Le RouterA a un default route ces points à l'interface interne PIX.

[Configurations](#)

Ce document utilise les configurations suivantes :

- [Configuration de RouterA](#)
- [Configuration de RouterB](#)
- [Configuration des dispositifs de sécurité 7.1 PIX Configuration PIX utilisant l'ASDM Configuration CLI de dispositifs de sécurité PIX](#)

Configuration de RouterA

```
RouterA#show running-config Building configuration...
Current configuration : 1151 bytes ! version 12.4
service config service timestamps debug uptime service
timestamps log uptime no service password-encryption !
hostname RouterA ! interface Ethernet2/0 ip address
10.2.1.1 255.255.255.0 half-duplex ! interface
Ethernet2/1 ip address 10.1.1.2 255.255.255.0 half-
duplex ! ip classless ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3 ! ! line con 0
line aux 0 line vty 0 4 ! end RouterA#
```

Configuration de RouterB

```
RouterB#show running-config Building configuration...
Current configuration : 1132 bytes ! version 12.4
service config service timestamps debug datetime msec
service timestamps log datetime msec no service
password-encryption ! hostname RouterB ! interface
FastEthernet0/0 ip address 10.1.1.3 255.255.255.0 speed
auto ! interface Ethernet1/0 ip address 10.3.1.1
255.255.255.0 half-duplex ! ip classless ip route
0.0.0.0 0.0.0.0 10.1.1.2 ! control-plane ! ! line con 0
line aux 0 line vty 0 4 ! end RouterB#
```

Si vous voulez utiliser l'ASDM pour la configuration des dispositifs de sécurité PIX, mais n'avez pas amorcé le périphérique, terminez-vous ces étapes :

1. Console dans le PIX.
2. D'une configuration effacée, employez les demandes interactives afin d'activer l'ASDM pour la Gestion du PIX du poste de travail 10.1.1.5.

Configuration des dispositifs de sécurité 7.1 PIX

```
Pre-configure Firewall now through interactive prompts
[yes]? yes
Firewall Mode [Routed]:
Enable password [<use current password>]: cisco
Allow password recovery [yes]?
Clock (UTC):
  Year [2005]:
  Month [Mar]:
  Day [15]:
  Time [05:40:35]: 14:45:00
Inside IP address: 10.1.1.1
Inside network mask: 255.255.255.0
Host name: OZ-PIX
```

```
Domain name: cisco.com
IP address of host running Device Manager: 10.1.1.5

The following configuration will be used:
  Enable password: cisco
  Allow password recovery: yes
  Clock (UTC): 14:45:00 Mar 15 2005
  Firewall Mode: Routed
  Inside IP address: 10.1.1.1
  Inside network mask: 255.255.255.0
  Host name: OZ-PIX
  Domain name: cisco.com
  IP address of host running Device Manager:
10.1.1.5

Use this configuration and write to flash? yes
  INFO: Security level for "inside" set to 100 by
default.
  Cryptochecksum: a0bff9bb aa3d815f c9fd269a
3f67fef5

965 bytes copied in 0.880 secs
  INFO: converting 'fixup protocol dns maximum-
length 512' to MPF commands
  INFO: converting 'fixup protocol ftp 21' to MPF
commands
  INFO: converting 'fixup protocol h323_h225
1720' to MPF commands
  INFO: converting 'fixup protocol h323_ras 1718-
1719' to MPF commands
  INFO: converting 'fixup protocol netbios 137-
138' to MPF commands
  INFO: converting 'fixup protocol rsh 514' to
MPF commands
  INFO: converting 'fixup protocol rtsp 554' to
MPF commands
  INFO: converting 'fixup protocol sip 5060' to
MPF commands
  INFO: converting 'fixup protocol skinny 2000'
to MPF commands
  INFO: converting 'fixup protocol smtp 25' to
MPF commands
  INFO: converting 'fixup protocol sqlnet 1521'
to MPF commands
  INFO: converting 'fixup protocol sunrpc_udp
111' to MPF commands
  INFO: converting 'fixup protocol tftp 69' to
MPF commands
  INFO: converting 'fixup protocol sip udp 5060'
to MPF commands
  INFO: converting 'fixup protocol xdmcp 177' to
MPF commands

Type help or '?' for a list of available commands.
OZ-PIX>
```

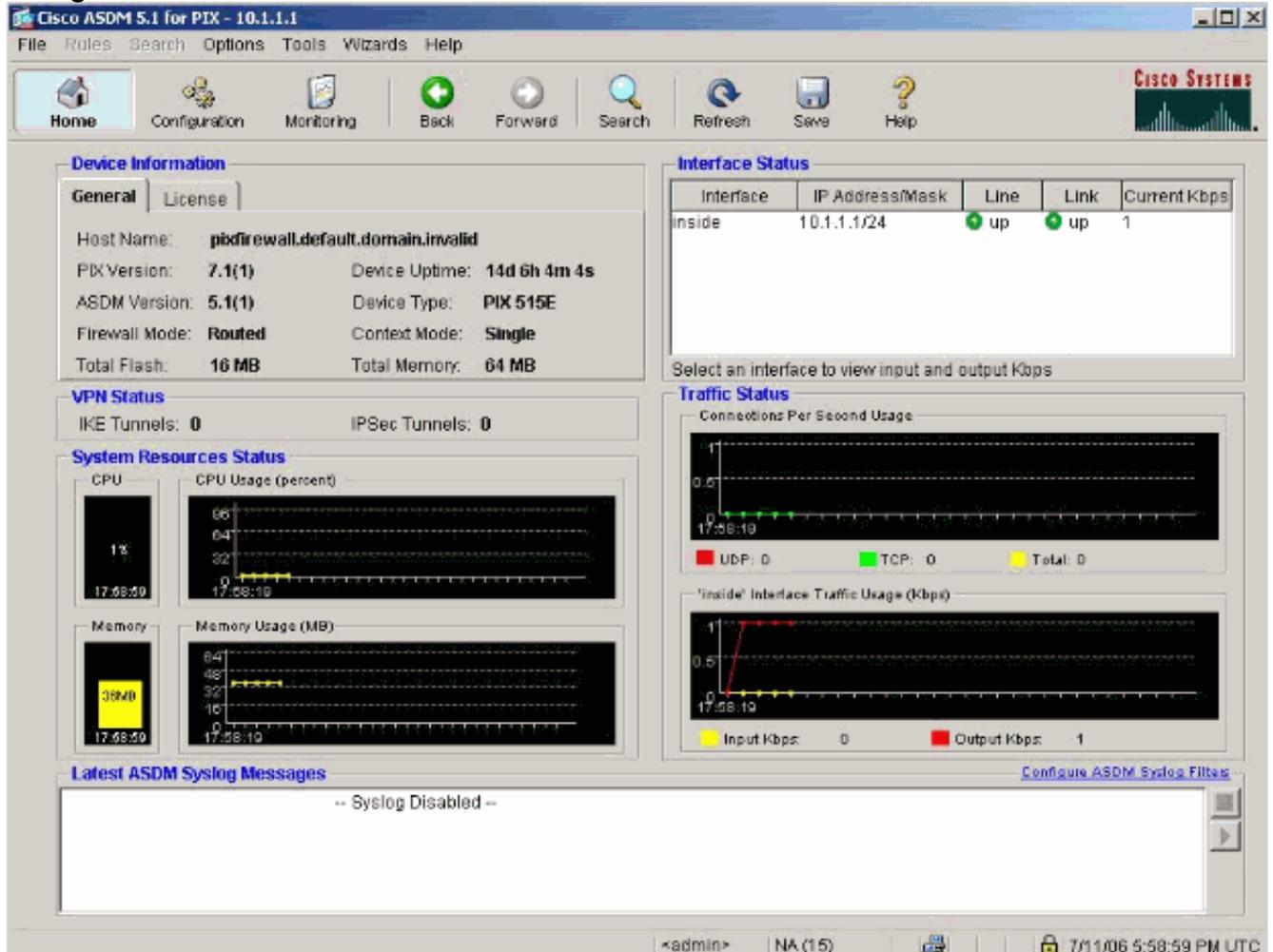
[Configuration PIX utilisant l'ASDM](#)

Terminez-vous ces étapes afin de configurer par l'intermédiaire du GUI ASDM :

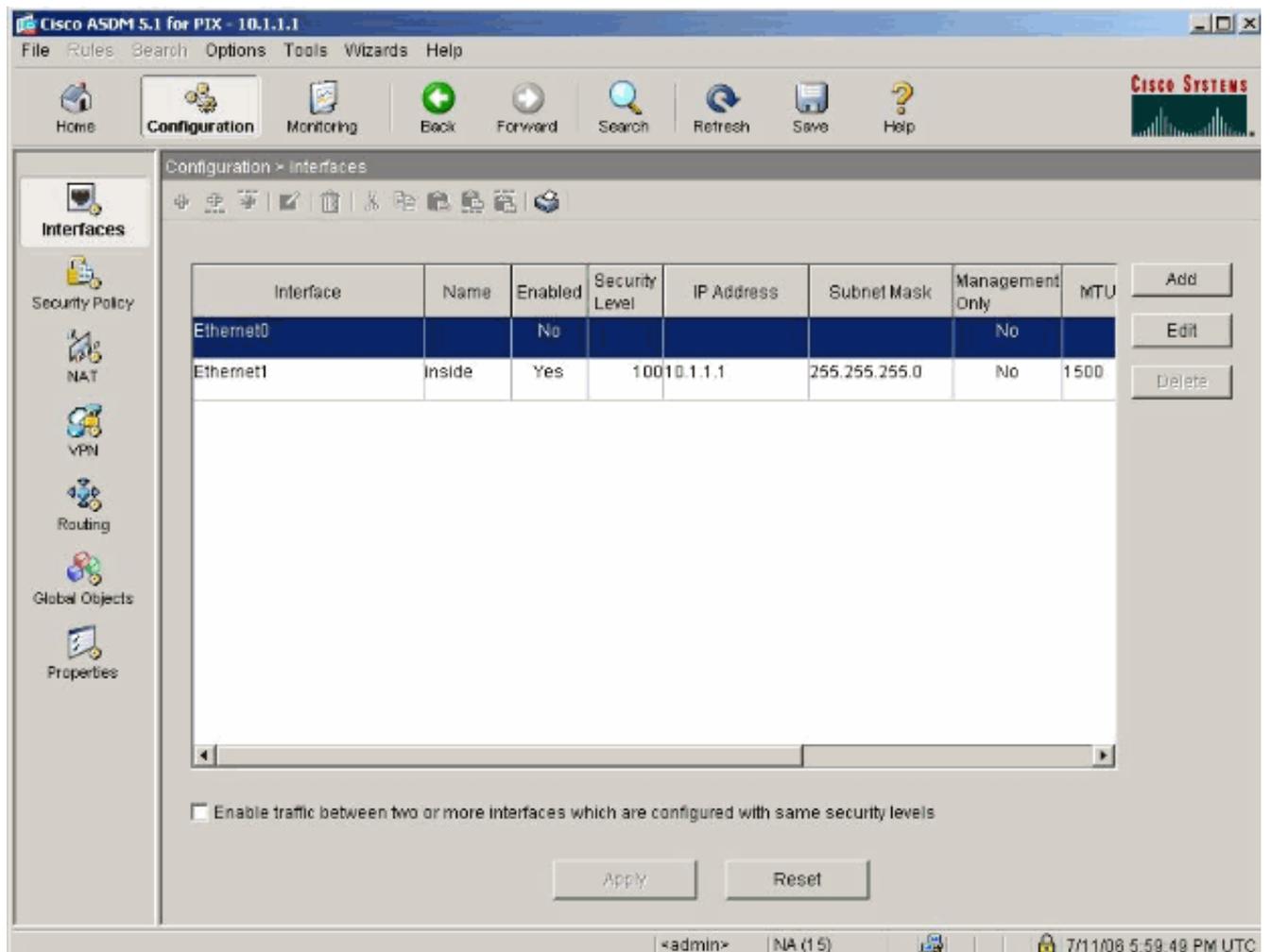
1. Du poste de travail 10.1.1.5, ouvrez un navigateur Web pour utiliser ASDM (dans cet

exemple, https://10.1.1.1).

2. Clic **oui** sur les demandes de certificat.
3. Ouvrez une session avec le mot de passe d'enable, comme précédemment configuré.
4. Si c'est la première fois l'ASDM est exécuté sur le PC, vous êtes incité à utiliser le lanceur ASDM ou l'ASDM comme app de Javas. Dans cet exemple, le lanceur ASDM est sélectionné et installé.
5. Allez dans la fenêtre d'accueil ASDM et cliquez sur la **configuration**.



6. Choisissez l'interface > éditez afin de configurer l'interface extérieure.



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

Edit Interface

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:

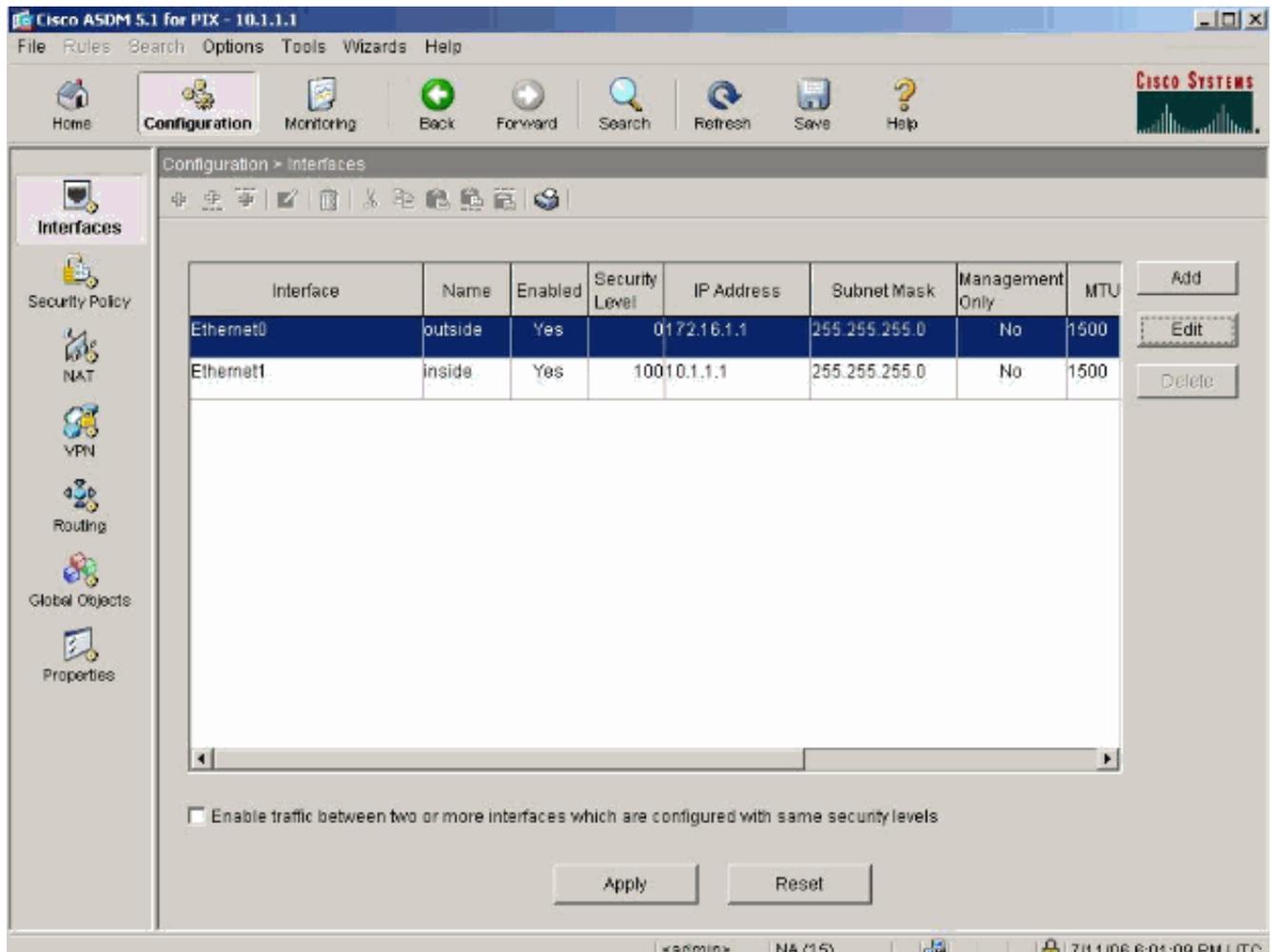
Description:

8. Cliquez sur OK sur la boîte de dialogue de modification de niveau de Sécurité.

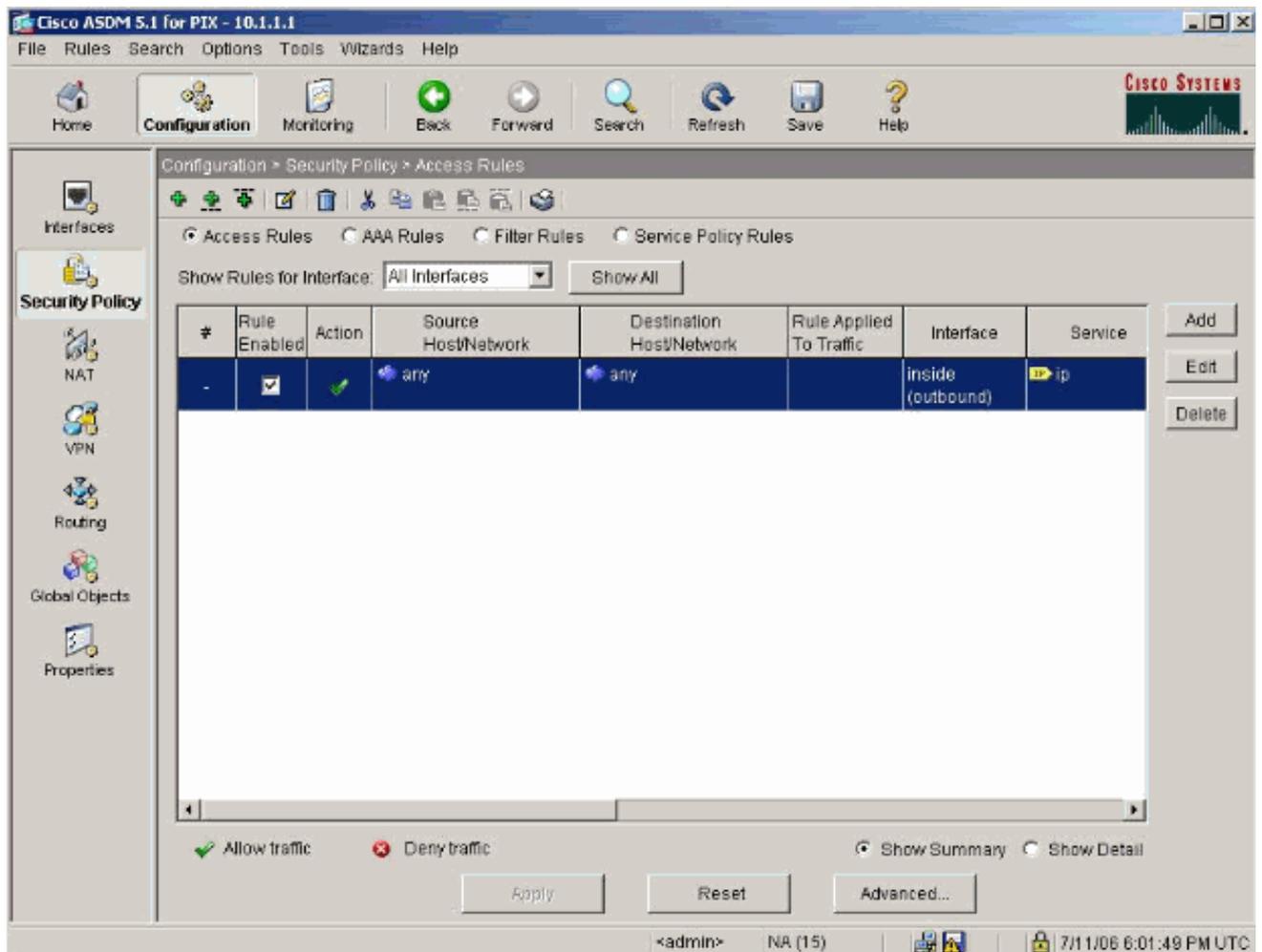
Security Level Change

 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?

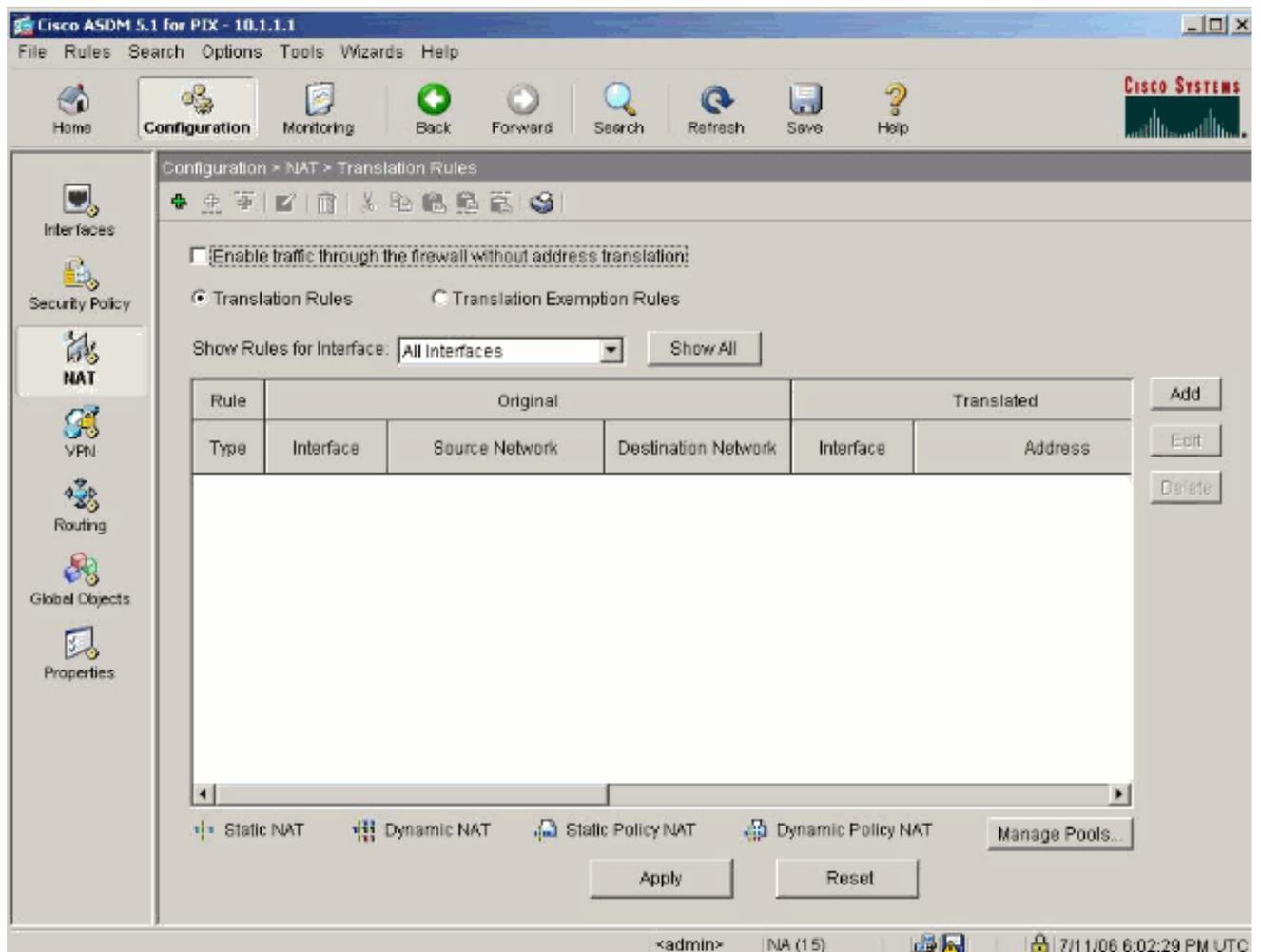
9. Cliquez sur Apply pour recevoir la configuration d'interface. La configuration obtient également poussé sur le PIX.



10. Choisissez la **stratégie de sécurité** sur l'onglet de caractéristiques afin de passer en revue la règle de stratégie de sécurité utilisée. Dans cet exemple, la règle d'intérieur de par défaut est utilisée.



11. Dans cet exemple, NAT est utilisé. Décochez la case d'**Enable traffic through the firewall without address translation** et cliquez sur Add afin de configurer la règle NAT.



12. Configurez le réseau de source. Dans cet exemple, 10.0.0.0 est utilisé pour l'adresse IP, et 255.0.0.0 est utilisé pour le masque. Cliquez sur **Manage Pools** afin de définir le pool d'adresses NAT.

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

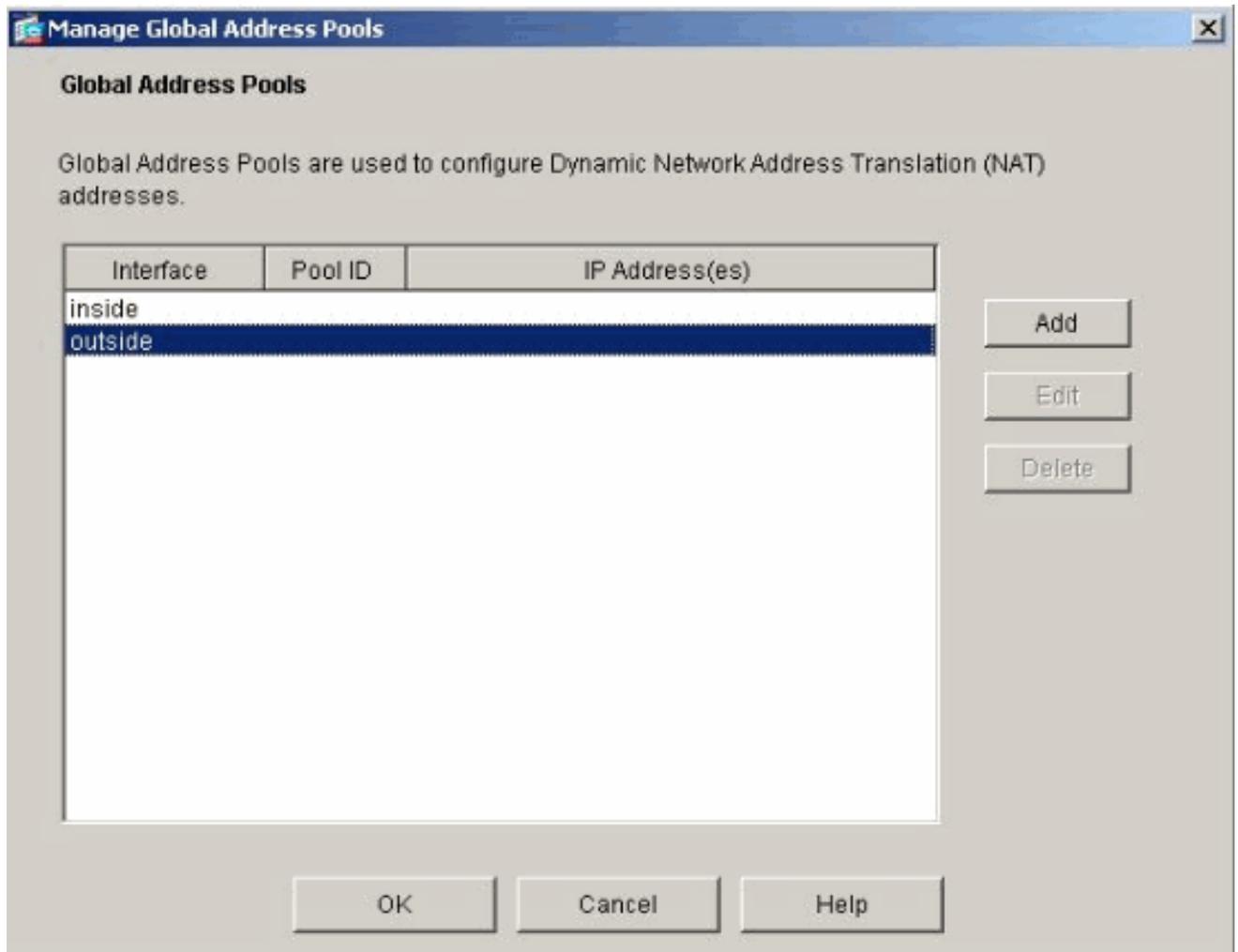
TCP Original port: Translated port:

 UDP

 Dynamic Address Pool:

Pool ID	Address
N/A	No address pool defined

13. Sélectionnez l'interface extérieure et cliquez sur Add.



14. Dans cet exemple, une plage et un pool d'adresses de PAT sont configurés. Configurez l'adresse NAT de groupe de plage et cliquez sur OK.

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):

15. Sélectionnez l'interface extérieure dans l'étape 13 afin de configurer l'adresse de PAT.
Cliquez sur
OK

Add Global Pool Item

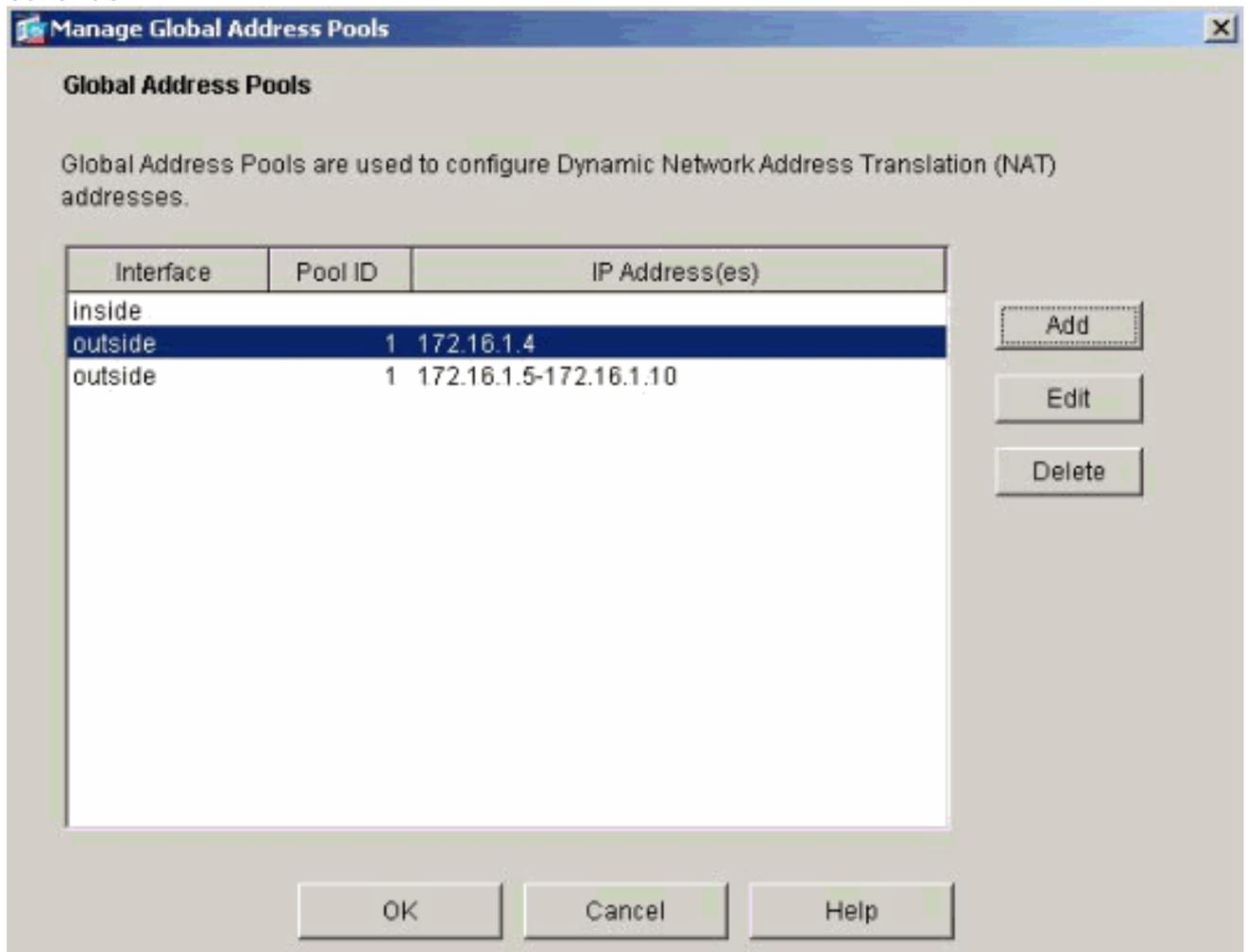
Interface: Pool ID:

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

IP Address: —

Network Mask (optional):

Cliquez sur OK afin de continuer.



16. Sur la fenêtre de règle de traduction d'adresses d'éditer, sélectionnez l'ID de groupe à utiliser par le réseau de source configuré. Cliquez sur **OK**.

Edit 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	172.16.1.4 172.16.1.5-172.16.1.10

17. Cliquez sur Apply afin de pousser la règle NAT configurée au PIX.

Cisco ASDM 5.1 for PIX - 10.1.1.1

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Back Forward Search Refresh Save Help

Configuration > NAT > Translation Rules

Enable traffic through the firewall without address translation

Translation Rules Translation Exemption Rules

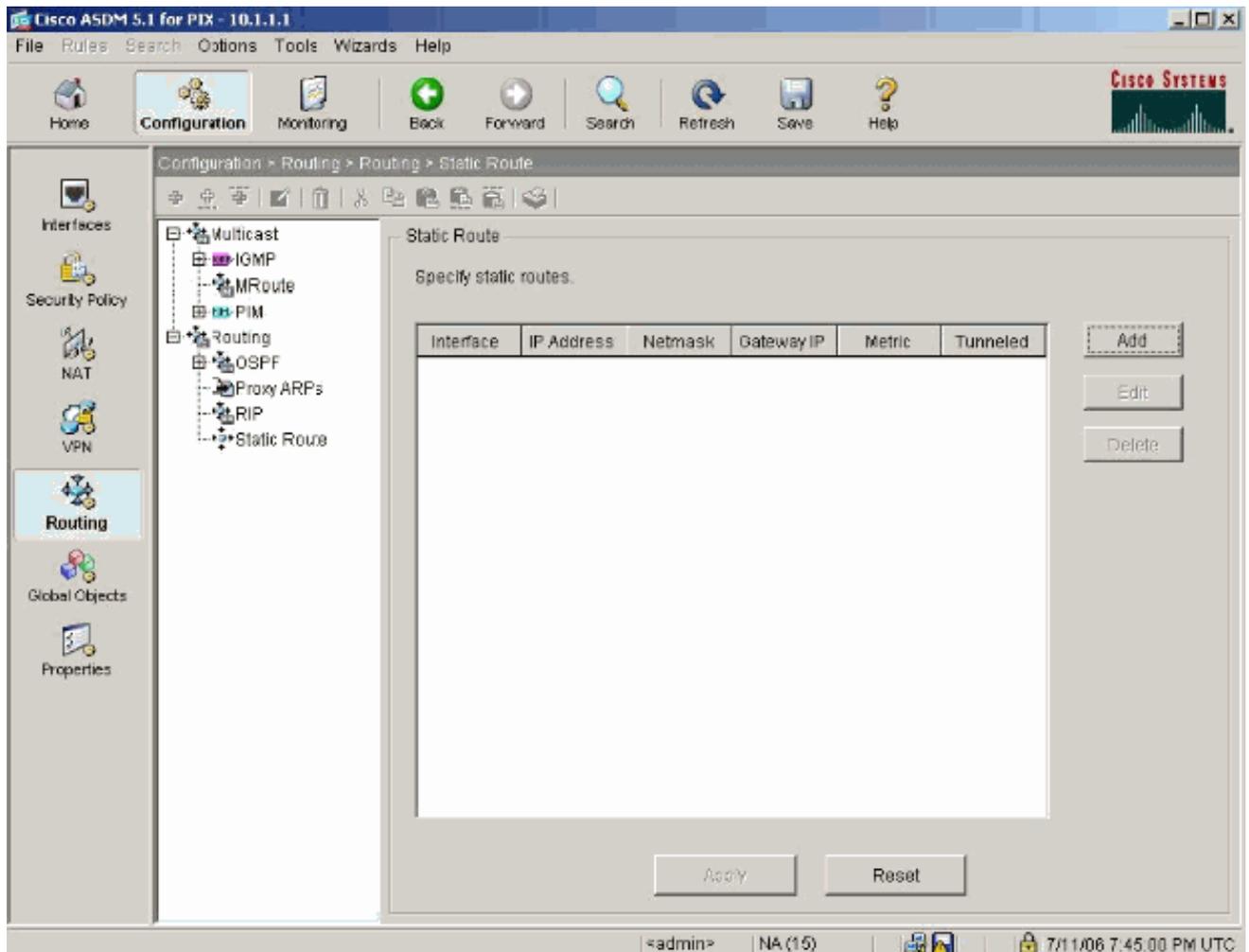
Show Rules for Interface: All Interfaces

Rule	Original			Translated		Add	Edit	Delete
	Type	Interface	Source Network	Destination Network	Interface			
		inside	10.0.0.0/8	any	outside	172.16.1.4 172.16.1.5-172.16.1.10		

Static NAT
 Dynamic NAT
 Static Policy NAT
 Dynamic Policy NAT

Device configuration loaded successfully. <admin> NA (15) 7/11/08 7:44:00 PM UTC

18. Dans cet exemple, des artères statiques sont utilisées. Cliquez sur Routing, choisissez l'artère statique et cliquez sur Add.



19. Configurez la passerelle par défaut et cliquez sur



OK.

20. 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.

Add Static Route

Interface Name:

IP Address:

Mask:

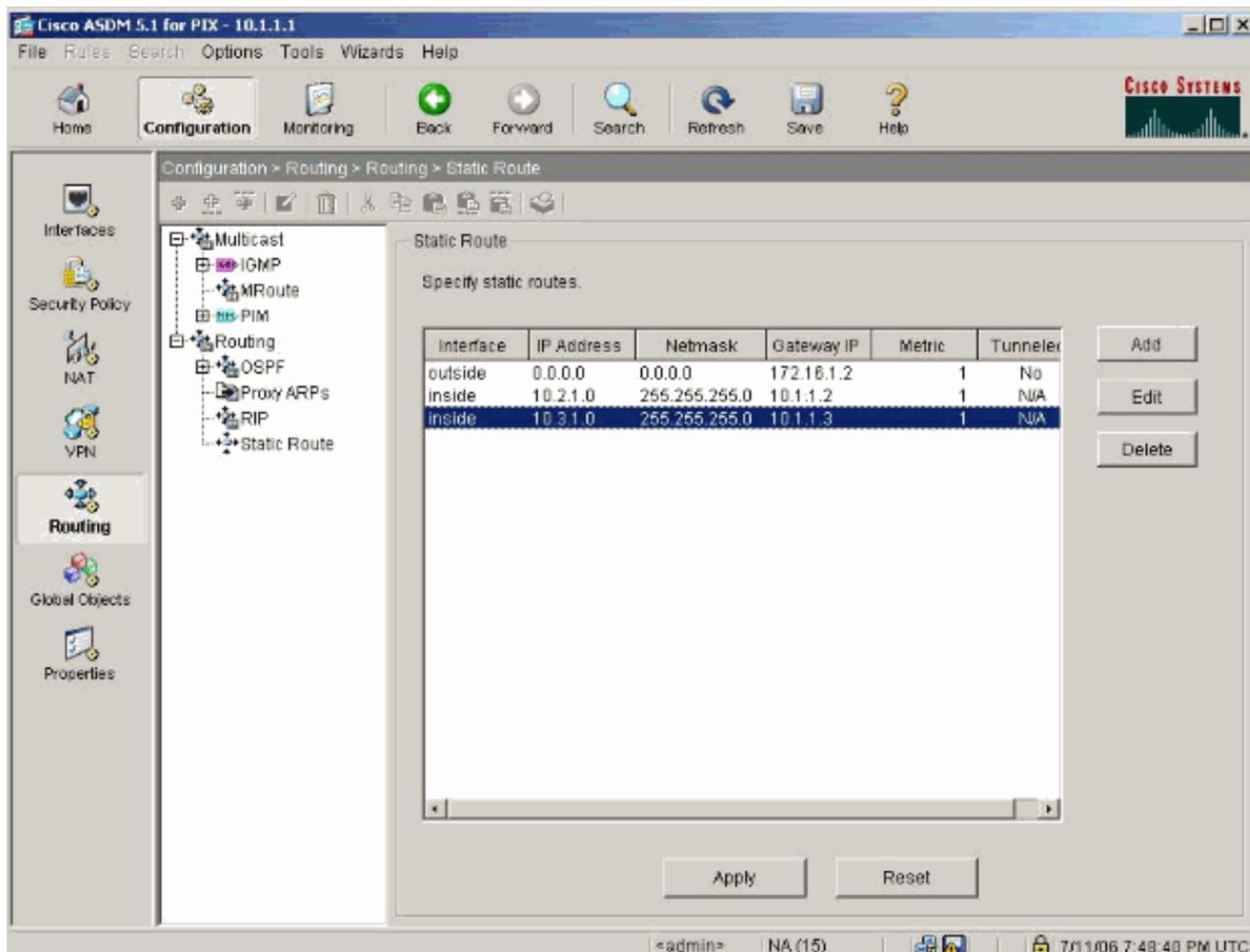
Gateway IP:

Metric

Tunneled (Used only for default route)

OK Cancel Help

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



Configuration PIX utilisant le CLI

La configuration par l'intermédiaire du GUI ASDM est maintenant complète.

Vous pouvez voir cette configuration par l'intermédiaire du CLI :

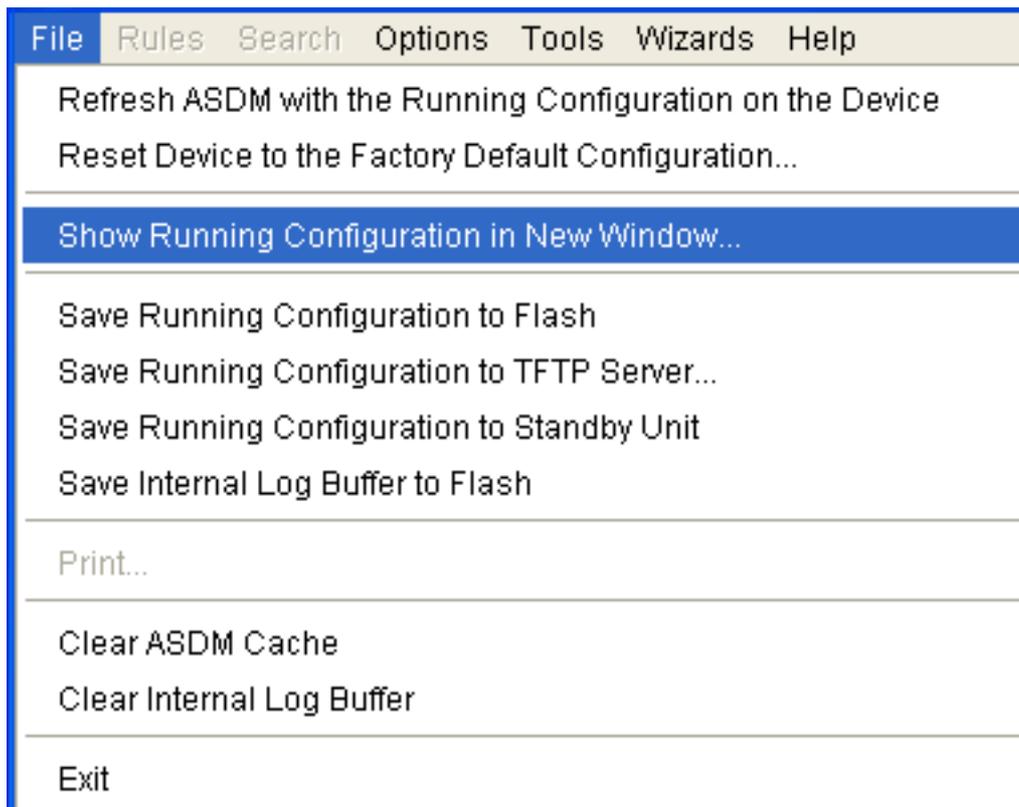
```

Dispositifs de sécurité CLI PIX
pixfirewall(config)#write terminal PIX Version 7.0(0)102
names ! interface Ethernet0 nameif outside security-
level 0 ip address 172.16.1.1 255.255.255.0 ! interface
Ethernet1 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 !--- Assign name and IP address
to the interfaces enable password 2KFQnbNIdI.2KYOU
encrypted passwd 2KFQnbNIdI.2KYOU encrypted asdm image
flash:/asdmfile.50073 no asdm history enable arp timeout
14400 nat-control !--- Enforce a strict NAT for all the
traffic through the Security appliance global (outside)
1 172.16.1.5-172.16.1.10 netmask 255.255.255.0 !---
Define a pool of global addresses 172.16.1.5 to
172.16.1.10 with !--- NAT ID 1 to be used for NAT global
(outside) 1 172.16.1.4 netmask 255.255.255.0 !--- Define
a single IP address 172.16.1.4 with NAT ID 1 to be used
for PAT nat (inside) 1 10.0.0.0 255.0.0.0 !--- Define
the inside networks with same NAT ID 1 used in the
global command for NAT route inside 10.3.1.0
255.255.255.0 10.1.1.3 1 route inside 10.2.1.0
255.255.255.0 10.1.1.2 1 !--- Configure static routes
for routing the packets towards the internal network
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1 !---

```

```
Configure static route for routing the packets towards
the Internet (or External network) 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 http server
enable !--- Enable the HTTP server on PIX for ASDM
access http 10.1.1.5 255.255.255.255 inside !--- Enable
HTTP access from host 10.1.1.5 to configure PIX using
ASDM (GUI) ! !--- Output suppressed ! !
Cryptochecksum:a0bff9bbaa3d815fc9fd269a3f67fef5 : end
```

Choisissez la **configuration en cours de fichier > d'exposition** dans la nouvelle fenêtre afin de visualiser la configuration CLI dans l'ASDM.



Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

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.

- **mettez au point le suivi d'ICMP** — Affiche si les demandes d'ICMP des hôtes atteignent le

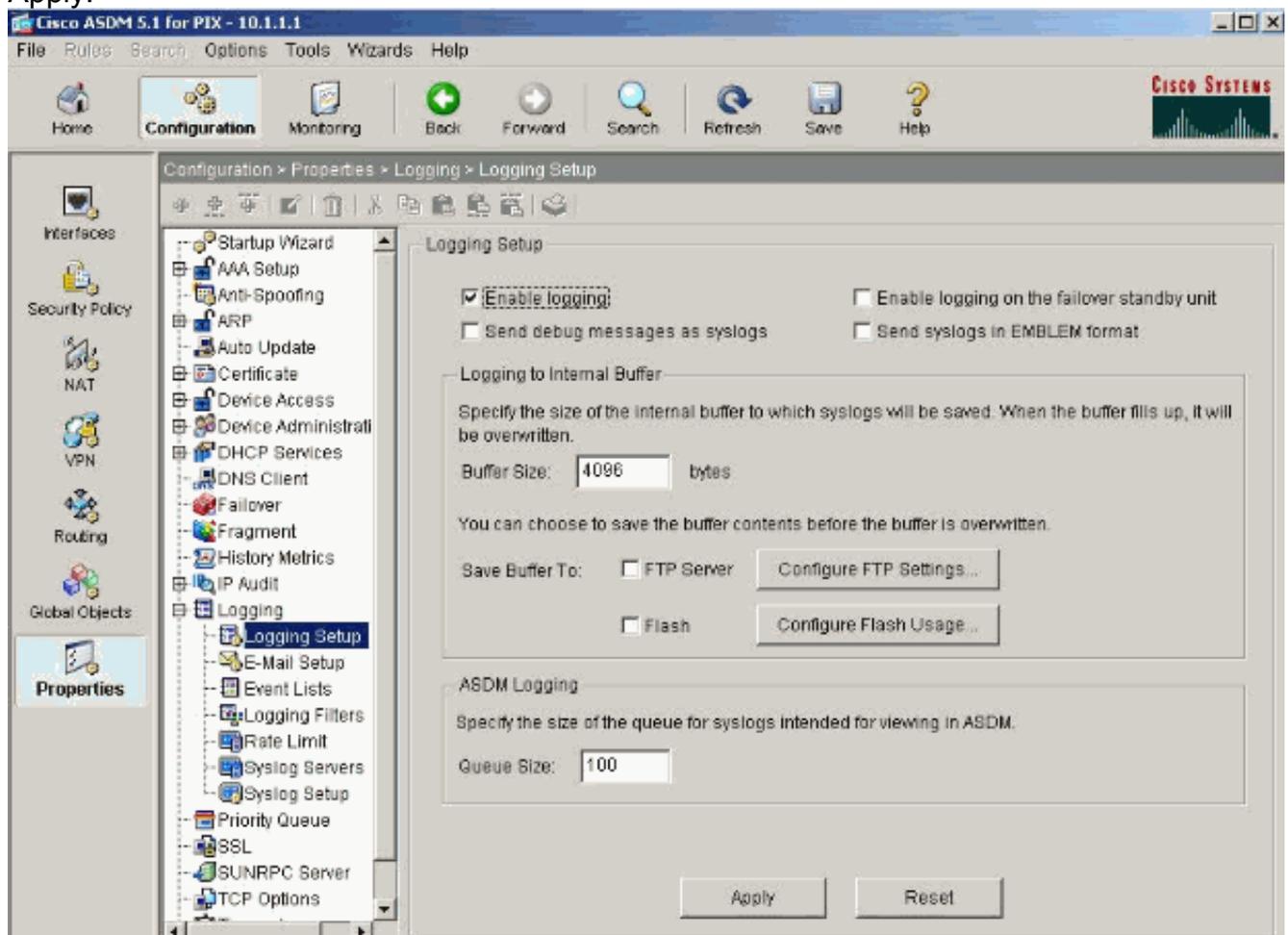
PIX. Afin d'exécuter ceci mettez au point, vous doivent ajouter la **commande access-list** de permettre l'ICMP dans votre configuration.

- **élimination des imperfections de tampon de journalisation** — Affiche les connexions qui sont 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**.

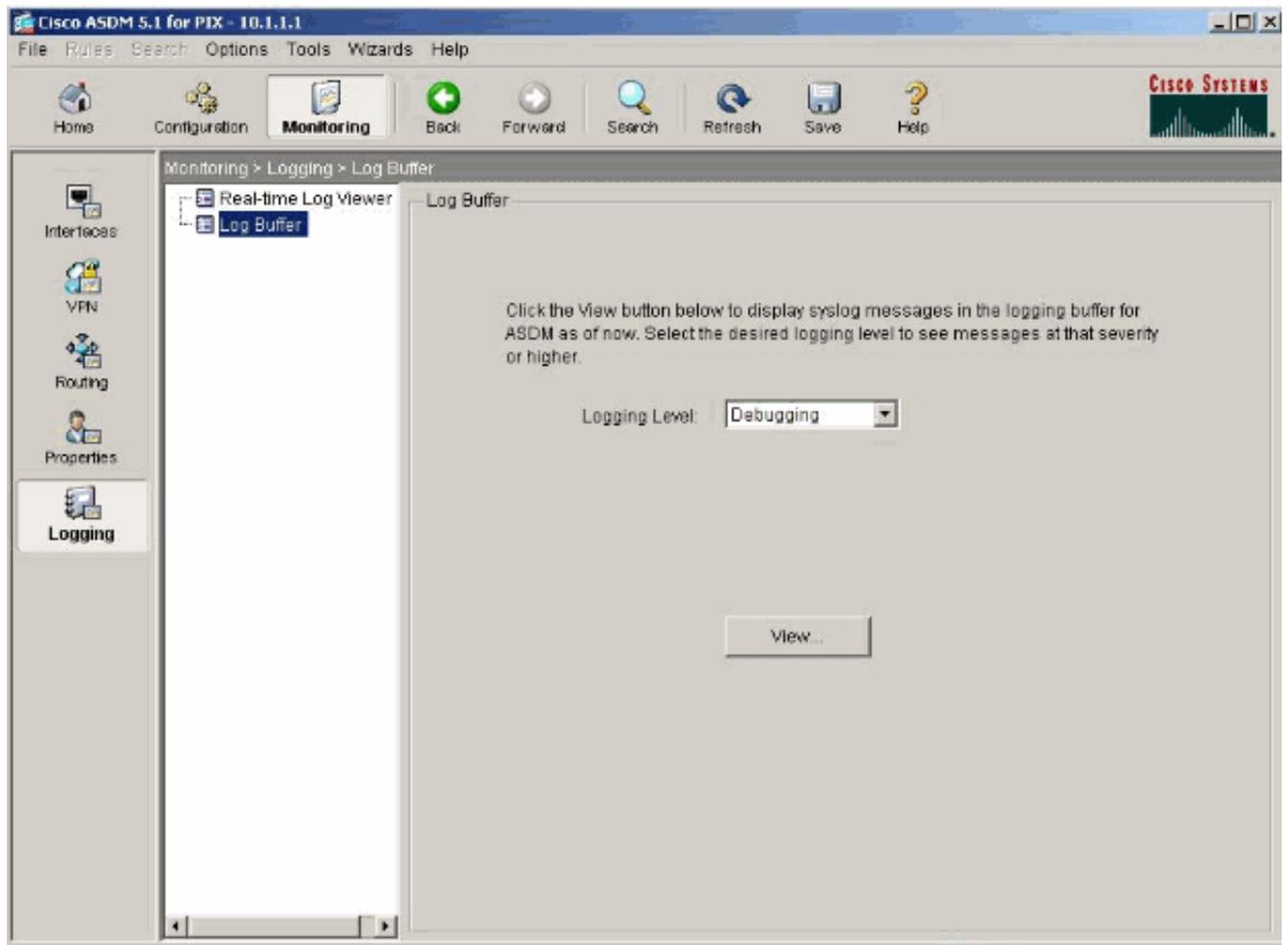
Procédure de dépannage

L'ASDM peut être utilisé pour activer se connecter, et pour visualiser également les logs :

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



2. Choisissez la **surveillance > en se connectant > mémoire tampon de log > en se connectant de niveau** et choisissez le **tampon de journalisation** de la liste déroulante. **Vue de clic**.



3. Voici un exemple de la mémoire tampon de log
:

This table shows syslog messages in ASDM logging buffer as of now.

Severity	Time	Message ID: Description
6	Jul 12 2006 13:08:11	805005: Login permitted from 10.1.1.5/1136 to inside:10.1.1.1/https for user "enable_15"
6	Jul 12 2006 13:08:11	725002: Device completed SSL handshake with client inside:10.1.1.5/1136
6	Jul 12 2006 13:08:11	725003: SSL client inside:10.1.1.5/1136 request to resume previous session.
6	Jul 12 2006 13:08:11	725001: Starting SSL handshake with client inside:10.1.1.5/1136 for TLSv1 session.
6	Jul 12 2006 13:08:11	302013: Built inbound TCP connection 545 for inside:10.1.1.5/1136 (10.1.1.5/1136) to NP Identity Ifc:10.
6	Jul 12 2006 13:08:10	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:10	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:10	110001: No route to 171.71.179.143 from 10.1.1.5
6	Jul 12 2006 13:08:09	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:09	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:08	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:08	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:07	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:07	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:06	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:06	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:05	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:05	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:04	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:04	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:03	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:03	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:02	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:02	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:01	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:01	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0

Legend: Emergencies Alerts Critical Errors Warnings Notifications Informational Debugging

[Incapable d'accéder à des sites Web de nom](#)

Dans certains scénarios, les réseaux internes ne peuvent pas accéder aux sites Web d'Internet à l'aide du nom (travaux avec l'adresse IP) dans le navigateur Web. Cette question est commune et se produit habituellement si le serveur DNS n'est pas défini, particulièrement dans les cas où PIX/ASA est le serveur DHCP. En outre, ceci peut se produire dans des cas si le PIX/ASA ne peut pas pousser le serveur DNS ou si le serveur DNS n'est pas accessible.

[Informations connexes](#)

- [Dispositifs de sécurité de la gamme Cisco PIX 500](#)
- [Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500](#)
- [Références des commandes du pare-feu Cisco Secure PIX](#)
- [Cisco Adaptive Security Device Manager](#)
- [Dépannage et alertes de Cisco Adaptive Security Device Manager \(ASDM\)](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)