

Migration des dispositifs de sécurité de la gamme PIX 500 vers les dispositifs de sécurité adaptatifs dédiés de la gamme ASA 5500

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Configuration matérielle et logicielle requise](#)

[Composants utilisés](#)

[Conventions](#)

[Conversion de configuration manuelle](#)

[Mettre à niveau la version du logiciel PIX vers 7.x](#)

[Mettre à niveau l'appliance de sécurité PIX avec la commande copy tftp flash](#)

[Mettre à niveau le dispositif de sécurité PIX du mode Surveillance](#)

[Convertir les noms d'interface du logiciel Cisco PIX 7.0 au format Cisco ASA](#)

[Copier la configuration de PIX vers ASA](#)

[Méthode 1 : copier/coller manuellement](#)

[Méthode 2 : Télécharger à partir de TFTP/FTP](#)

[Application d'une configuration du logiciel PIX version 6.x au logiciel ASA version 7.x](#)

[Dépannage - Conversion manuelle de la configuration](#)

[Périphérique bloqué dans une boucle de redémarrage](#)

[Message d'erreur](#)

[La configuration ne semble pas correcte](#)

[Certains services, tels que FTP, ne fonctionnent pas](#)

[Impossible d'accéder à Internet lorsque l'appareil de sécurité Cisco PIX est remplacé par l'appareil de sécurité adaptatif Cisco \(ASA\)](#)

[Informations connexes](#)

Introduction

Ce document explique comment migrer des dispositifs de sécurité de la gamme PIX 500 vers des dispositifs de sécurité adaptatifs de la gamme ASA 5500.

Remarque : les PIX 501, PIX 506 et PIX 506E ne prennent pas en charge la version 7 du logiciel.

Il y a deux façons de convertir une configuration PIX en configuration ASA :

- Conversion assistée par outil
- Conversion manuelle

Conversion automatique basée sur outil / assistée par outil

Cisco recommande d'utiliser la conversion assistée par outil afin de convertir les configurations PIX en configurations ASA.

La méthode de conversion assistée par outil est plus rapide et plus évolutive si vous effectuez plusieurs conversions. Cependant, la sortie du processus dans une configuration intermédiaire contient à la fois l'ancienne et la nouvelle syntaxe. Cette méthode repose sur l'installation de la configuration intermédiaire sur le dispositif de sécurité adaptatif cible pour terminer la conversion. Tant qu'il n'est pas installé sur le périphérique cible, vous ne pouvez pas afficher la configuration finale.

Remarque : Cisco a lancé l'outil de migration PIX vers ASA afin d'aider à automatiser le processus de migration vers les nouveaux appareils ASA. Cet outil peut être téléchargé à partir du site de téléchargement du logiciel PIX. Référez-vous à [Migration de la configuration du dispositif de sécurité de la gamme PIX 500 vers les dispositifs de sécurité adaptatifs de la gamme ASA 5500](#) pour plus d'informations.

Conditions préalables

Configuration matérielle et logicielle requise

Vous pouvez mettre à niveau PIX 515, 515E, 525, 535 vers la version 7.0.

Avant de commencer le processus de mise à niveau vers la version 7.x, Cisco recommande que PIX exécute la version 6.2 ou ultérieure. Cela garantit que la configuration actuelle est correctement convertie. En outre, ces exigences matérielles doivent être satisfaites pour la configuration minimale requise de la mémoire vive :

Modèle PIX :	Mémoire RAM requise	
	Restreint (R)	Non restreint (UR) / Basculement uniquement (FO)
PIX-515	64 Mo*	128 Mo*
PIX-515 E	64 Mo*	128 Mo*
PIX-525	128 Mo	256 Mo
PIX-535	512 Mo	1 Go

Émettez la commande show version afin de déterminer la quantité de RAM actuellement installée sur le PIX.

Remarque : les mises à niveau logicielles des PIX 515 et 515E peuvent également nécessiter une mise à niveau de la mémoire :

- Les licences limitées et 32 Mo de mémoire doivent être mis à niveau vers 64 Mo de mémoire.
- Ceux qui disposent de licences illimitées et de 64 Mo de mémoire doivent être mis à niveau

vers 128 Mo de mémoire.

Reportez-vous à ce tableau pour connaître les références dont vous avez besoin pour mettre à niveau la mémoire de ces appliances.

Configuration actuelle de l'appliance		Solution de mise à niveau	
Licence de plate-forme	Mémoire totale (avant la mise à niveau)	Numéro de référence	Mémoire totale (après la mise à niveau)
Restreint (R)	32 Mo	PIX-515-MEM-32=	64 Mo
Non restreint (UR)	32 Mo	PIX-515-MEM-128=	128 Mo
Basculement uniquement (FO)	64 Mo	PIX-515-MEM-128=	128 Mo

Remarque : la référence dépend de la licence installée sur le PIX.

La mise à niveau du logiciel version 6.x vers 7.x est transparente et nécessite un travail manuel, mais ces étapes doivent être terminées avant de commencer :

1. Assurez-vous qu'il n'y a aucune commande conduit ou outbound/apply dans votre configuration actuelle. Ces commandes ne sont plus prises en charge dans 7.x et le processus de mise à niveau les supprime. Utilisez l'outil [Conduit Converter](#) afin de convertir ces commandes en listes d'accès avant de tenter la mise à niveau.
2. Assurez-vous que PIX ne met pas fin aux connexions PPTP (Point to Point Tunneling Protocol). La version 7.x du logiciel ne prend actuellement pas en charge la terminaison PPTP.
3. Copiez tous les certificats numériques pour les connexions VPN sur le PIX avant de commencer le processus de mise à niveau.
4. Lisez ces documents afin de vous assurer que vous connaissez les commandes nouvelles, modifiées et déconseillées :
 - Les notes de version de la version logicielle vers laquelle vous prévoyez d'effectuer la mise à niveau sont disponibles à l'adresse suivante : « Notes de version de l'appliance de sécurité Cisco PIX ».
 - [Guide de mise à niveau des utilisateurs de Cisco PIX 6.2 et 6.3 vers la version 7.0 du logiciel Cisco PIX](#)
5. Planifiez la migration pendant les temps d'arrêt. Bien que la migration soit un processus simple en deux étapes, la mise à niveau de l'appliance de sécurité PIX vers 7.x est un changement majeur qui nécessite un certain temps d'arrêt.
6. Téléchargez le logiciel 7.x à partir de [Cisco Downloads](#) (clients [enregistrés](#) uniquement) .

Composants utilisés

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

- Appareils de sécurité ASA 5500
- Appliance de sécurité PIX 515, 515E, 525 et 535
- Logiciel PIX versions 6.3, 7.0

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 aux [Conventions relatives aux conseils techniques Cisco](#).

Conversion de configuration manuelle

Avec le processus de conversion manuelle, vous utilisez un éditeur de texte pour parcourir votre configuration ligne par ligne et convertir les commandes spécifiques à PIX en commandes ASA.

La conversion manuelle de la configuration PIX en configuration ASA vous donne le plus de contrôle sur le processus de conversion. Cependant, le processus prend du temps et n'évolue pas bien si vous devez effectuer plusieurs conversions.

Ces trois étapes doivent être effectuées afin de migrer de PIX vers ASA :

1. Mettez à niveau la version du logiciel PIX vers 7.x.
2. Convertissez les noms d'interface du logiciel Cisco PIX 7.0 au format Cisco ASA.
3. Copiez la configuration du logiciel PIX 7.0 sur Cisco ASA 5500.

Mettre à niveau la version du logiciel PIX vers 7.x

Avant de commencer le processus de mise à niveau proprement dit, procédez comme suit :

1. Émettez la commande `show running-config` ou `write net` afin d'enregistrer la configuration actuelle de PIX dans un fichier texte ou un serveur TFTP.
2. Émettez la commande `show version` afin de vérifier les exigences, telles que la mémoire vive. Enregistrez également le résultat de cette commande dans un fichier texte. Si vous devez revenir à une version antérieure du code, vous pouvez éventuellement avoir besoin de la clé d'activation d'origine.

Si le PIX a une version du système d'entrée-sortie (BIOS) de base antérieure à 4.2 ou si vous prévoyez de mettre à niveau un PIX 515 ou un PIX 535 avec un PDM déjà installé, alors vous devez compléter la procédure de mise à niveau en Mode de surveillance au lieu d'avec la méthode copy tftp flash. Afin d'afficher la version du BIOS, redémarrez le PIX, et avec un câble de console attaché, lisez les messages au démarrage.

La version du BIOS est répertoriée dans un message, tel que :

```
<#root>
```

```
Rebooting....
```

```
CISCO SYSTEMS PIX FIREWALL
```

```
Embedded BIOS Version 4.3.207
```

```
01/02/02 16:12:22.73
```

```
Compiled by morlee
```

```
64 MB RAM
```

Remarque : les commandes 6.x sont automatiquement converties en commandes 7.x lors de la mise à niveau. La conversion automatique des commandes entraîne une modification de votre configuration. Vous devez revoir les modifications de configuration après le démarrage du logiciel 7.x afin de vérifier que les modifications automatiques sont satisfaisantes. Enregistrez ensuite la configuration dans la mémoire flash afin de vous assurer que le système ne la convertira pas de nouveau au prochain démarrage de l'apppliance de sécurité.

Remarque : une fois le système mis à niveau vers 7.x, il est important de ne pas utiliser l'utilitaire de disque np version 6.x du logiciel, tel que la récupération de mot de passe, car il corrompt l'image logicielle 7.x et vous oblige à redémarrer votre système à partir du mode Surveillance. Cela peut également vous faire perdre votre configuration précédente, votre noyau de sécurité et vos informations clés.

Mettre à niveau l'apppliance de sécurité PIX avec la commande copy tftp flash

Procédez comme suit afin de mettre à niveau le PIX avec l'utilisation de la commande copy tftp flash.

1. Copiez l'image binaire de l'apppliance PIX, par exemple, pix701.bin, dans le répertoire racine du serveur TFTP.
2. À partir de l'invite enable, émettez la commande copy tftp flash.

```
<#root>
```

```
pixfirewall>
```

```
enable
```

Password:

```
pixfirewall#
```

```
copy tftp flash
```

3. Saisissez l'adresse IP du serveur TFTP.

```
<#root>
```

```
Address or name of remote host [0.0.0.0]?
```

4. Saisissez le nom du fichier sur le serveur TFTP que vous souhaitez charger. Il s'agit du nom de fichier de l'image binaire PIX.

```
<#root>
```

```
Source file name [cdisk]?
```

5. Lorsque vous êtes invité à démarrer la copie TFTP, tapez yes.

```
<#root>
```

```
copying tftp://172.18.173.123/pix701.bin to flash:image  
[yes|no|again]?
```

```
yes
```

6. L'image est maintenant copiée du serveur TFTP vers la mémoire Flash.

Ce message s'affiche et indique que le transfert a réussi, que l'ancienne image binaire dans


```
Received 5124096 bytes
Erasing current image
Writing 5066808 bytes of image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image installed
pixfirewall#
pixfirewall#

reload

Proceed with reload? [confirm]
```

Rebooting...

```
CISCO SYSTEMS PIX FIREWALL
Embedded BIOS Version 4.3.207 01/02/02 16:12:22.73
Compiled by morlee
128 MB RAM
```

```
PCI Device Table.
Bus Dev Func VendID DevID Class Irq
00 00 00 8086 7192 Host Bridge
00 07 00 8086 7110 ISA Bridge
00 07 01 8086 7111 IDE Controller
00 07 02 8086 7112 Serial Bus 9
00 07 03 8086 7113 PCI Bridge
00 0D 00 8086 1209 Ethernet 11
00 0E 00 8086 1209 Ethernet 10
00 13 00 11D4 2F44 Unknown Device 5
```

```
Cisco Secure PIX Firewall BIOS (4.2) #0: Mon Dec 31 08:34:35 PST 2001
Platform PIX-515E
System Flash=E28F128J3 @ 0xffff00000
```

```
Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Reading 5063168 bytes of image from flash.
```

```
#####
#####
128MB RAM
```

```
Total NICs found: 2
mcwa i82559 Ethernet at irq 11 MAC: 0009.4360.ed44
mcwa i82559 Ethernet at irq 10 MAC: 0009.4360.ed43
BIOS Flash=am29f400b @ 0xd8000
Old file system detected. Attempting to save data in flash
```

*!--- This output indicates that the Flash file
!--- system is formatted. The messages are normal.*

```
Initializing flashfs...
flashfs[7]: Checking block 0...block number was (-27642)
```

flashfs[7]: erasing block 0...done.
flashfs[7]: Checking block 1...block number was (-30053)
flashfs[7]: erasing block 1...done.
flashfs[7]: Checking block 2...block number was (-1220)
flashfs[7]: erasing block 2...done.
flashfs[7]: Checking block 3...block number was (-22934)
flashfs[7]: erasing block 3...done.
flashfs[7]: Checking block 4...block number was (2502)
flashfs[7]: erasing block 4...done.
flashfs[7]: Checking block 5...block number was (29877)
flashfs[7]: erasing block 5...done.
flashfs[7]: Checking block 6...block number was (-13768)
flashfs[7]: erasing block 6...done.
flashfs[7]: Checking block 7...block number was (9350)
flashfs[7]: erasing block 7...done.
flashfs[7]: Checking block 8...block number was (-18268)
flashfs[7]: erasing block 8...done.
flashfs[7]: Checking block 9...block number was (7921)
flashfs[7]: erasing block 9...done.
flashfs[7]: Checking block 10...block number was (22821)
flashfs[7]: erasing block 10...done.
flashfs[7]: Checking block 11...block number was (7787)
flashfs[7]: erasing block 11...done.
flashfs[7]: Checking block 12...block number was (15515)
flashfs[7]: erasing block 12...done.
flashfs[7]: Checking block 13...block number was (20019)
flashfs[7]: erasing block 13...done.
flashfs[7]: Checking block 14...block number was (-25094)
flashfs[7]: erasing block 14...done.
flashfs[7]: Checking block 15...block number was (-7515)
flashfs[7]: erasing block 15...done.
flashfs[7]: Checking block 16...block number was (-10699)
flashfs[7]: erasing block 16...done.
flashfs[7]: Checking block 17...block number was (6652)
flashfs[7]: erasing block 17...done.
flashfs[7]: Checking block 18...block number was (-23640)
flashfs[7]: erasing block 18...done.
flashfs[7]: Checking block 19...block number was (23698)
flashfs[7]: erasing block 19...done.
flashfs[7]: Checking block 20...block number was (-28882)
flashfs[7]: erasing block 20...done.
flashfs[7]: Checking block 21...block number was (2533)
flashfs[7]: erasing block 21...done.
flashfs[7]: Checking block 22...block number was (-966)
flashfs[7]: erasing block 22...done.
flashfs[7]: Checking block 23...block number was (-22888)
flashfs[7]: erasing block 23...done.
flashfs[7]: Checking block 24...block number was (-9762)
flashfs[7]: erasing block 24...done.
flashfs[7]: Checking block 25...block number was (9747)
flashfs[7]: erasing block 25...done.
flashfs[7]: Checking block 26...block number was (-22855)
flashfs[7]: erasing block 26...done.
flashfs[7]: Checking block 27...block number was (-32551)
flashfs[7]: erasing block 27...done.
flashfs[7]: Checking block 28...block number was (-13355)
flashfs[7]: erasing block 28...done.
flashfs[7]: Checking block 29...block number was (-29894)
flashfs[7]: erasing block 29...done.
flashfs[7]: Checking block 30...block number was (-18595)
flashfs[7]: erasing block 30...done.
flashfs[7]: Checking block 31...block number was (22095)

flashfs[7]: erasing block 31...done.
flashfs[7]: Checking block 32...block number was (1486)
flashfs[7]: erasing block 32...done.
flashfs[7]: Checking block 33...block number was (13559)
flashfs[7]: erasing block 33...done.
flashfs[7]: Checking block 34...block number was (24215)
flashfs[7]: erasing block 34...done.
flashfs[7]: Checking block 35...block number was (21670)
flashfs[7]: erasing block 35...done.
flashfs[7]: Checking block 36...block number was (-24316)
flashfs[7]: erasing block 36...done.
flashfs[7]: Checking block 37...block number was (29271)
flashfs[7]: erasing block 37...done.
flashfs[7]: Checking block 125...block number was (0)
flashfs[7]: erasing block 125...done.
flashfs[7]: inconsistent sector list, fileid 7, parent_fileid 0
flashfs[7]: inconsistent sector list, fileid 12, parent_fileid 0
flashfs[7]: 5 files, 3 directories
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 16128000
flashfs[7]: Bytes used: 5128192
flashfs[7]: Bytes available: 10999808
flashfs[7]: flashfs fsck took 59 seconds.
flashfs[7]: Initialization complete.

Saving the configuration

!
Saving a copy of old configuration as downgrade.cfg
!

Saved the activation key from the flash image
Saved the default firewall mode (single) to flash
Saving image file as image.bin

!!
!!

Upgrade process complete
Need to burn loader...
Erasing sector 0...[OK]
Burning sector 0...[OK]

Licensed features for this platform:
Maximum Physical Interfaces : 6
Maximum VLANs : 25
Inside Hosts : Unlimited
Failover : Active/Active
VPN-DES : Enabled
VPN-3DES-AES : Enabled
Cut-through Proxy : Enabled
Guards : Enabled
URL Filtering : Enabled
Security Contexts : 2
GTP/GPRS : Disabled
VPN Peers : Unlimited

This platform has an Unrestricted (UR) license.

Encryption hardware device : VAC (IRE2141 with 2048KB, HW:1.0, CGXROM:1.9, FW:6.5)

. .
| |
||| |||
.|| ||. .|| ||.
.:||| | |||:..:||| | |||:.

Cisco PIX Security Appliance Software Version 7.0(1)

***** Warning *****

This product contains cryptographic features and is subject to United States and local country laws governing, import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return the enclosed items immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

***** Warning *****

Copyright (c) 1996-2005 by Cisco Systems, Inc.

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

!--- These messages are printed for any deprecated commands.

ERROR: This command is no longer needed. The LOCAL user database is always enabled.
*** Output from config line 50, "aaa-server LOCAL protoco..."
ERROR: This command is no longer needed. The 'floodguard' feature is always enabled.
*** Output from config line 55, "floodguard enable"

Cryptochecksum(unchanged): 9fa48219 950977b6 dbf6bea9 4dc97255

!--- All current fixups are converted to the new Modular Policy Framework.

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 http 80' 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.
pixfirewall>
```

Remarque : émettez la commande `show version` afin de vérifier que le PIX exécute maintenant la version du logiciel 7.x.

Remarque : afin d'examiner les erreurs qui se sont produites pendant la migration de la configuration, émettez la commande `show startup-config errors`. Les erreurs apparaissent dans ce résultat après le premier démarrage du PIX pour la première fois.

Mettre à niveau le dispositif de sécurité PIX du mode Surveillance

Passez en mode Surveillance

Complétez ces étapes afin d'entrer en Mode Surveillance sur le PIX.

1. Connectez un câble de console au port de console sur le PIX avec l'utilisation de ces paramètres de communication :
 - 9600 bits par seconde
 - 8 bits de données
 - aucune parité
 - 1 bit d'arrêt
 - aucun contrôle de flux
2. Éteignez et rallumez ou rechargez le PIX. Pendant le démarrage, vous êtes invité à utiliser `BREAK` ou `ESC` afin d'interrompre le démarrage Flash. Vous avez dix secondes pour interrompre le processus de démarrage normal.
3. Appuyez sur la touche `ESC` ou envoyez un caractère `BREAK` afin d'entrer en mode Monitor.
 - Si vous utilisez Windows Hyper Terminal, vous pouvez appuyer sur la touche Échap ou appuyer sur `Ctrl+Pause` afin d'envoyer un caractère `BREAK`.
 - Si vous établissez une connexion Telnet via un serveur de terminal afin d'accéder au port de console du PIX, vous devez appuyer sur `Ctrl+] (Contrôle + crochet droit)` afin d'accéder à l'invite de commande Telnet. Ensuite, émettez la commande `send break`.
4. L'invite `monitor>` s'affiche.

5. Passez à la section [Mise à niveau du PIX à partir du mode de surveillance](#).

Mettre à niveau le PIX à partir du mode Surveillance

Complétez ces étapes afin de mettre à niveau votre PIX à partir du mode de surveillance.

1. Copiez l'image binaire de l'apppliance PIX, par exemple, pix701.bin, dans le répertoire racine du serveur TFTP.
2. Passez en mode Surveillance sur le PIX. Si vous n'êtes pas sûr de la façon de le faire, consultez [Enter Monitor Mode](#).

Remarque : une fois en mode Surveillance, vous pouvez utiliser la touche ? pour afficher la liste des options disponibles.

3. Saisissez le numéro d'interface auquel le serveur TFTP est connecté ou l'interface la plus proche du serveur TFTP. Il s'agit par défaut de l'interface 1 (à l'intérieur).

```
<#root>  
monitor>  
interface
```

Remarque : en mode Surveillance, l'interface négocie toujours automatiquement la vitesse et le mode duplex. Les paramètres d'interface ne peuvent pas être codés en dur. Par conséquent, si l'interface PIX est connectée à un commutateur qui est codé en dur pour la vitesse/le duplex, reconfigurez-le pour la négociation automatique lorsque vous êtes en mode Surveillance. Notez également que le périphérique PIX ne peut pas initialiser une interface Gigabit Ethernet à partir du mode Surveillance. Vous devez utiliser une interface Fast Ethernet à la place.

4. Entrez l'adresse IP de l'interface définie à l'étape 3.

```
<#root>  
monitor>  
address
```

5. Saisissez l'adresse IP du serveur TFTP.

```
<#root>  
monitor>  
server
```

6. (Facultatif) Saisissez l'adresse IP de votre passerelle. Une adresse de passerelle est requise si l'interface du PIX n'est pas sur le même réseau que le serveur TFTP.

```
<#root>  
monitor>  
gateway
```

7. Saisissez le nom du fichier sur le serveur TFTP que vous souhaitez charger. Il s'agit du nom de fichier de l'image binaire PIX.

```
<#root>  
monitor>  
file
```

8. Envoyez une requête ping du PIX au serveur TFTP afin de vérifier la connectivité IP.

Si les requêtes ping échouent, vérifiez à nouveau les câbles, l'adresse IP de l'interface PIX et du serveur TFTP, ainsi que l'adresse IP de la passerelle (si nécessaire). Les requêtes ping doivent aboutir avant de continuer.

```
<#root>
monitor>
ping
```

9. Tapez tftp afin de démarrer le téléchargement TFTP.

```
<#root>
monitor>
tftp
```

10. Le PIX télécharge l'image dans la RAM et l'amorce automatiquement.

Au cours du processus de démarrage, le système de fichiers est converti en même temps que votre configuration actuelle. Cependant, vous n'avez pas encore terminé. Notez ce message d'avertissement après le démarrage et passez à l'étape 11 :

```
*****
**                                                                 **
**   *** WARNING *** WARNING *** WARNING *** WARNING *** WARNING *** **
**                                                                 **
**           ----> Current image running from RAM only! <---- **
**                                                                 **
** When the PIX was upgraded in Monitor mode the boot image was not **
** written to Flash. Please issue "copy tftp: flash:" to load and **
** save a bootable image to Flash. Failure to do so will result in **
** a boot loop the next time the PIX is reloaded. **
**                                                                 **
*****
```

11. Une fois démarré, passez en mode enable et copiez de nouveau la même image sur le PIX. Cette fois, émettez la commande copy tftp flash.

L'image est alors enregistrée dans le système de fichiers Flash. Si vous ne complétez pas cette étape, une boucle de démarrage se produira lors du prochain rechargement du PIX.

```
<#root>
pixfirewall>
```

```
enable
pixfirewall#
copy tftp flash
```

Remarque : Pour obtenir des instructions détaillées sur la façon de copier l'image à l'aide de la commande `copy tftp flash`, consultez la section [Mettre à niveau l'appliance de sécurité PIX avec la commande `copy tftp flash`](#).

12. Une fois l'image copiée avec la commande `copy tftp flash`, le processus de mise à niveau est terminé.

Exemple de configuration - Mise à niveau du dispositif de sécurité PIX du mode Surveillance

```
<#root>
monitor>
interface 1
0: i8255X @ PCI(bus:0 dev:13 irq:10)
1: i8255X @ PCI(bus:0 dev:14 irq:7 )
2: i8255X @ PCI(bus:1 dev:0 irq:11)
3: i8255X @ PCI(bus:1 dev:1 irq:11)
4: i8255X @ PCI(bus:1 dev:2 irq:11)
5: i8255X @ PCI(bus:1 dev:3 irq:11)

Using 1: i82559 @ PCI(bus:0 dev:14 irq:7 ), MAC: 0050.54ff.4d81
monitor>
address 10.1.1.2

address 10.1.1.2
monitor>
server 172.18.173.123

server 172.18.173.123
monitor>
gateway 10.1.1.1

gateway 10.1.1.1
monitor>
file pix701.bin

file pix701.bin
monitor>
ping 172.18.173.123

Sending 5, 100-byte 0xa014 ICMP Echoes to 172.18.173.123, timeout is 4 seconds:
!!!!
Success rate is 100 percent (5/5)
```

monitor>

tftp

tftp pix701.bin@172.18.173.123.....
Received 5124096 bytes

Cisco PIX Security Appliance admin loader (3.0) #0: Mon Mar 7 17:39:03 PST 2005

128MB RAM

Total NICs found: 6
mcwa i82559 Ethernet at irq 10 MAC: 0050.54ff.4d80
mcwa i82559 Ethernet at irq 7 MAC: 0050.54ff.4d81
mcwa i82558 Ethernet at irq 11 MAC: 00e0.b600.2014
mcwa i82558 Ethernet at irq 11 MAC: 00e0.b600.2015
mcwa i82558 Ethernet at irq 11 MAC: 00e0.b600.2016
mcwa i82558 Ethernet at irq 11 MAC: 00e0.b600.2017
BIOS Flash=AT29C257 @ 0xfffd8000
Old file system detected. Attempting to save data in flash

*!--- This output indicates that the Flash file
!--- system is formatted. The messages are normal.*

Initializing flashfs...
flashfs[7]: Checking block 0...block number was (-10627)
flashfs[7]: erasing block 0...done.
flashfs[7]: Checking block 1...block number was (-14252)
flashfs[7]: erasing block 1...done.
flashfs[7]: Checking block 2...block number was (-15586)
flashfs[7]: erasing block 2...done.
flashfs[7]: Checking block 3...block number was (5589)
flashfs[7]: erasing block 3...done.
flashfs[7]: Checking block 4...block number was (4680)
flashfs[7]: erasing block 4...done.
flashfs[7]: Checking block 5...block number was (-21657)
flashfs[7]: erasing block 5...done.
flashfs[7]: Checking block 6...block number was (-28397)
flashfs[7]: erasing block 6...done.
flashfs[7]: Checking block 7...block number was (2198)
flashfs[7]: erasing block 7...done.
flashfs[7]: Checking block 8...block number was (-26577)
flashfs[7]: erasing block 8...done.
flashfs[7]: Checking block 9...block number was (30139)
flashfs[7]: erasing block 9...done.
flashfs[7]: Checking block 10...block number was (-17027)
flashfs[7]: erasing block 10...done.
flashfs[7]: Checking block 11...block number was (-2608)
flashfs[7]: erasing block 11...done.
flashfs[7]: Checking block 12...block number was (18180)
flashfs[7]: erasing block 12...done.
flashfs[7]: Checking block 13...block number was (0)
flashfs[7]: erasing block 13...done.
flashfs[7]: Checking block 14...block number was (29271)
flashfs[7]: erasing block 14...done.
flashfs[7]: Checking block 15...block number was (0)
flashfs[7]: erasing block 15...done.
flashfs[7]: Checking block 61...block number was (0)
flashfs[7]: erasing block 61...done.
flashfs[7]: inconsistent sector list, fileid 9, parent_fileid 0

flashfs[7]: inconsistent sector list, fileid 10, parent_fileid 0
flashfs[7]: 9 files, 3 directories
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 15988976
flashfs[7]: Bytes used: 10240
flashfs[7]: Bytes available: 15988736
flashfs[7]: flashfs fsck took 58 seconds.
flashfs[7]: Initialization complete.

Saving the datafile

!

Saving a copy of old datafile for downgrade

!

Saving the configuration

!

Saving a copy of old configuration as downgrade.cfg

!

Saved the activation key from the flash image

Saved the default firewall mode (single) to flash

The version of image file in flash is not bootable in the current version of software.

Use the downgrade command first to boot older version of software.

The file is being saved as image_old.bin anyway.

!!

Upgrade process complete

Need to burn loader....

Erasing sector 0...[OK]

Burning sector 0...[OK]

Erasing sector 64...[OK]

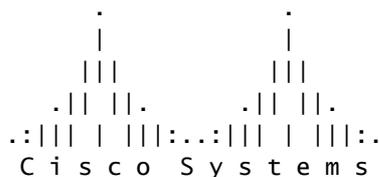
Burning sector 64...[OK]

Licensed features for this platform:

Maximum Physical Interfaces	: 6
Maximum VLANs	: 25
Inside Hosts	: Unlimited
Failover	: Active/Active
VPN-DES	: Enabled
VPN-3DES-AES	: Enabled
Cut-through Proxy	: Enabled
Guards	: Enabled
URL Filtering	: Enabled
Security Contexts	: 2
GTP/GPRS	: Disabled
VPN Peers	: Unlimited

This platform has an Unrestricted (UR) license.

Encryption hardware device : VAC+ (Crypto5823 revision 0x1)



Cisco PIX Security Appliance Software Version 7.0(1)

***** Warning *****

This product contains cryptographic features and is subject to United States and local country laws governing, import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return the enclosed items immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

***** Warning *****

Copyright (c) 1996-2005 by Cisco Systems, Inc.

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

!--- These messages are printed for any deprecated commands.

.ERROR: This command is no longer needed. The LOCAL user database is always enabled.
*** Output from config line 71, "aaa-server LOCAL protoco..."
ERROR: This command is no longer needed. The 'floodguard' feature is always enabled.
*** Output from config line 76, "floodguard enable"

Cryptochecksum(unchanged): 8c224e32 c17352ad 6f2586c4 6ed92303

*!--- All current fixups are converted to the
!--- new Modular Policy Framework.*

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 http 80' to MPF commands
INFO: converting 'fixup protocol ils 389' 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
*****
**
**   *** WARNING *** WARNING *** WARNING *** WARNING *** WARNING ***   **
**
**   ----> Current image running from RAM only! <----   **
**
**   When the PIX was upgraded in Monitor mode the boot image was not   **
**   written to Flash. Please issue "copy tftp: flash:" to load and   **
**   save a bootable image to Flash. Failure to do so will result in   **
**   a boot loop the next time the PIX is reloaded.   **
**
*****
```

Type help or '?' for a list of available commands.

```
pixfirewall>
pixfirewall>
```

enable

Password:

```
pixfirewall#
pixfirewall#
```

copy tftp flash

Address or name of remote host []?

172.18.173.123

Source filename []?

pix701.bin

Destination filename [pix701.bin]?

```
Accessing tftp://172.18.173.123/pix701.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file flash:/pix701.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
5124096 bytes copied in 139.790 secs (36864 bytes/sec)
pixfirewall#
```

Convertir les noms d'interface du logiciel Cisco PIX 7.0 au format Cisco ASA

L'étape suivante du processus consiste à modifier hors ligne la configuration du logiciel Cisco PIX 7.0 nouvellement convertie.

La convention d'attribution de noms d'interface Cisco ASA étant différente de celle des appareils de sécurité Cisco PIX, vous devez modifier la configuration Cisco PIX avant de la copier/la télécharger sur votre appareil de sécurité Cisco ASA 5500.

Complétez ces étapes afin d'effectuer les changements de nom d'interface sur la configuration PIX :

1. Copiez la nouvelle configuration du logiciel Cisco PIX 7.0 hors ligne. Pour ce faire, téléchargez la configuration sur un serveur TFTP/FTP ou copiez la configuration d'une session de console vers un éditeur de texte.

Afin de télécharger la configuration PIX vers un serveur TFTP/FTP, à partir de la console, émettez cette commande :

```
copy startup^'config tftp://n.n.n.n/PIX7cfg.txt  
or  
copy startup^'config ftp://n.n.n.n/PIX7cfg.txt
```

2. Une fois que le fichier de configuration basé sur le logiciel Cisco PIX 7.0 est téléchargé avec succès sur le serveur TFTP/FTP (ou est collé/copié dans un éditeur de texte), ouvrez le Bloc-notes/WordPad ou tout éditeur de texte favori afin de modifier les noms d'interface sur la configuration PIX.

Les appareils de sécurité Cisco PIX numérotent les interfaces de 0 à n. Les appareils de sécurité Cisco ASA 5500 numérotent les interfaces en fonction de leur emplacement/emplacement. Les interfaces intégrées sont numérotées de 0/0 à 0/3 et l'interface de gestion est Management 0/0. Les interfaces du module 4GE SSM sont numérotées de 1/0 à 1/3.

Cisco ASA 5510 avec une licence de base qui exécute 7.0 dispose de trois ports Fast Ethernet (0/0 à 0/2) plus l'interface Management 0/0 disponible. Cisco ASA 5510 avec une licence Security Plus dispose des cinq interfaces Fast Ethernet disponibles. Les modèles Cisco ASA 5520 et 5540 sont dotés de quatre ports Gigabit Ethernet et d'un port de gestion Fast Ethernet. Le Cisco ASA 5550 est doté de huit ports Gigabit Ethernet et d'un port Fast Ethernet.

Modifiez les noms d'interface sur la configuration PIX au format d'interface ASA.

Exemple :

```
<#root>
```

```
Ethernet0 ==> Ethernet
```

```
0/0
```

```
Ethernet1 ==> Ethernet
```

```
0/1
```

```
GigabitEthernet0 ==> GigabitEthernet
```

```
0/0
```

Référez-vous à la section « Configuration des paramètres d'interface » du [Guide de configuration de la ligne de commande du dispositif de sécurité Cisco, version 7.0](#) pour plus d'informations.

Copier la configuration de PIX vers ASA

À ce stade, vous disposez d'une configuration basée sur le logiciel Cisco PIX 7.0 avec les noms d'interface modifiés prêts à être copiés ou téléchargés sur votre Cisco ASA 5500. Il existe deux façons de charger la configuration basée sur le logiciel Cisco PIX 7.0 sur l'appareil Cisco ASA 5500.

Suivez les étapes de la [Méthode 1 : Copier/Coller manuel](#) ou de la [Méthode 2 : Télécharger à partir de TFTP/FTP](#).

Méthode 1 : copier/coller manuellement

Copiez la configuration via la méthode copier/coller à partir de la console PIX :

1. Connectez-vous à la gamme Cisco ASA 5500 via la console et émettez la commande `clear config all` afin d'effacer la configuration avant de coller la configuration modifiée du logiciel Cisco PIX 7.0.

```
<#root>
```

```
ASA#config t
```

```
ASA(config)#clear config all
```

2. Copiez et collez la configuration sur la console ASA, puis enregistrez la configuration.

Remarque : vérifiez que toutes les interfaces sont à l'état `no shutdown` avant de commencer le test.

Méthode 2 : Télécharger à partir de TFTP/FTP

La deuxième méthode consiste à télécharger la configuration basée sur le logiciel Cisco PIX 7.0 à partir d'un serveur TFTP/FTP. Pour cette étape, vous devez configurer l'interface de gestion sur l'appareil de la gamme Cisco ASA 5500 pour le téléchargement TFTP/FTP :

1. À partir de la console ASA, émettez ceci :

```
<#root>
```

```
ASA#config t
ASA(config)#interface management 0
ASA(config)#nameif management
ASA(config)#ip add
```

```
ASA(config)#no shut
```

Remarque : (facultatif) gestion de la route <ip> <mask> <next-hop>

2. Une fois l'interface de gestion configurée, vous pouvez télécharger la configuration PIX sur l'ASA :

```
<#root>
```

```
ASA(Config)#copy tftp://
```

```
/PIX7cfg.txt running-config
```

3. Enregistrez la configuration.

Application d'une configuration du logiciel PIX version 6.x au logiciel ASA version 7.x

La conversion d'une configuration PIX 6.2 ou 6.3 en un nouvel appareil de sécurité ASA est un processus manuel. L'administrateur ASA/PIX doit convertir la syntaxe PIX 6.x pour qu'elle corresponde à la syntaxe ASA et taper les commandes dans la configuration ASA. Vous pouvez copier et coller certaines commandes telles que la commande `access-list`. Assurez-vous de comparer étroitement la configuration PIX 6.2 ou 6.3 à la nouvelle configuration ASA afin de vous assurer qu'aucune erreur n'est faite dans la conversion.

Remarque : [Cisco CLI Analyzer](#) (clients [enregistrés](#) uniquement) peut être utilisé pour convertir certaines commandes plus anciennes, non prises en charge, telles que `apply`, `outbound` ou `conduit` vers la liste d'accès appropriée. Les déclarations converties doivent être examinées en détail. Il est nécessaire de vérifier que la conversion correspond aux stratégies de sécurité.

Remarque : le processus de mise à niveau vers une nouvelle appliance ASA est différent d'une mise à niveau vers une nouvelle appliance PIX. Une tentative de mise à niveau vers un ASA avec le processus PIX génère un certain nombre d'erreurs de configuration sur l'ASA.

Dépannage - Conversion manuelle de la configuration

Périphérique bloqué dans une boucle de redémarrage

- Après avoir utilisé la méthode `copy tftp flash` afin de mettre à niveau le PIX, et redémarrer, il est bloqué dans cette boucle de redémarrage :

```
<#root>
```

```
Cisco Secure PIX Firewall BIOS (4.0)
```

```
#0:
```

```
Thu Mar 2 22:59:20 PST 2000
```

```
Platform PIX-515
```

```
Flash=i28F640J5 @ 0x300
```

```
Use BREAK or ESC to interrupt flash boot.
```

```
Use SPACE to begin flash boot immediately.
```

```
Reading 5063168 bytes of image from flash.
```

Les appliances PIX avec des versions du BIOS antérieures à 4.2 ne peuvent pas être mises à niveau à l'aide de la commande `copy tftp flash`. Vous devez les mettre à niveau avec la méthode Monitor Mode.

- Une fois que le PIX exécute 7.x et redémarre, il est bloqué dans cette boucle de

redémarrage :

```
<#root>
```

```
Rebooting....
```

```
Cisco Secure PIX Firewall BIOS (4.0) #0: Thu Mar 2 22:59:20 PST 2000  
Platform PIX-515  
Flash=i28F640J5 @ 0x300
```

```
Use BREAK or ESC to interrupt flash boot.  
Use SPACE to begin flash boot immediately.  
Reading 115200 bytes of image from flash.
```

```
PIX Flash Load Helper
```

```
Initializing flashfs...  
flashfs[0]: 10 files, 4 directories  
flashfs[0]: 0 orphaned files, 0 orphaned directories  
flashfs[0]: Total bytes: 15998976  
flashfs[0]: Bytes used: 1975808  
flashfs[0]: Bytes available: 14023168  
flashfs[0]: Initialization complete.
```

```
Unable to locate boot image configuration
```

```
Booting first image in flash
```

```
No bootable image in flash. Please download  
an image from a network server in the monitor mode
```

```
Failed to find an image to boot
```

Si le PIX est mis à niveau du Mode Surveillance vers 7.0, mais que l'image 7.0 n'est pas recopiée dans Flash après le premier démarrage de 7.0, alors quand le PIX est rechargé, il devient bloqué dans une boucle de redémarrage.

La résolution est de charger à nouveau l'image à partir du mode Surveillance. Après le démarrage, vous devez copier l'image une fois de plus avec l'utilisation de la méthode copy tftp flash.

Message d'erreur

Lorsque vous effectuez une mise à niveau avec la méthode copy tftp flash, le message d'erreur suivant s'affiche :

```
<#root>
```

```
pixfirewall#
```

```
copy tftp flash
```

```
Address or name of remote host [0.0.0.0]? 172.18.173.123
```

```
Source file name [cdisk]? pix701.bin
copying tftp://172.18.173.123/pix701.bin to flash:image
[yes|no|again]? y
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Received 5124096 bytes
Erasing current image

Insufficient flash space available for this request:

Size info: request:5066808 current:1966136 delta:3100672 free:2752512
Image not installed
pixfirewall#
```

Ce message apparaît généralement quand le PIX 515 ou un PIX 535 avec PDM déjà installé est mis à niveau avec la méthode copy tftp flash.

Effectuez une mise à niveau avec la méthode Monitor Mode afin de résoudre ce problème.

La configuration ne semble pas correcte

Après avoir mis à niveau le PIX de 6.x à 7.x, une partie de la configuration ne migre pas correctement.

Le résultat de la commande show startup-config errors montre toutes les erreurs qui se sont produites pendant la migration de la configuration. Les erreurs apparaissent dans ce résultat après le premier démarrage du PIX pour la première fois. Examinez ces erreurs et essayez de les résoudre.

Certains services, tels que FTP, ne fonctionnent pas

Parfois, certains services tels que FTP ne fonctionnent pas après une mise à niveau.

L'inspection de ces services n'est pas activée après la mise à niveau. Activez l'inspection pour les services appropriés. Pour ce faire, ajoutez-les à la stratégie d'inspection par défaut/globale ou créez une stratégie d'inspection distincte pour le service souhaité.

Référez-vous à la section « Application de l'inspection de protocole de couche application » du [Guide de configuration de la ligne de commande du dispositif de sécurité Cisco, version 7.0](#) pour plus d'informations sur les politiques d'inspection.

Impossible d'accéder à Internet lorsque l'appareil de sécurité Cisco PIX est remplacé par l'appareil de sécurité adaptatif Cisco (ASA)

Utilisez cette section si vous ne parvenez pas à accéder à Internet après avoir remplacé le dispositif de sécurité Cisco PIX par le dispositif de sécurité adaptatif Cisco (ASA).

Lorsque vous débranchez le PIX du réseau et reliez l'ASA sur le réseau avec une adresse IP d'interface externe qui est la même que l'interface externe du PIX, le routeur en amont a toujours l'adresse mac pour le PIX correspondant à l'adresse IP d'interface externe. Par conséquent, il ne

peut pas renvoyer les paquets de réponse à l'ASA. Pour que l'ASA fonctionne, vous devez effacer l'entrée ARP sur le routeur en amont afin qu'il apprenne l'entrée nouvelle/correcte d'adresse MAC. Si vous videz les entrées ARP lorsque vous prévoyez de remplacer le PIX par ASA, cela résout le problème de connectivité Internet. L'effacement de l'entrée ARP doit être effectué par le FAI à leur extrémité.

Informations connexes

- [Appareils de sécurité de la gamme Cisco PIX 500 - Introduction](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.