

從PIX 500系列安全裝置遷移到ASA 5500系列自適應安全裝置

目錄

[簡介](#)

[必要條件](#)

[硬體和軟體要求](#)

[採用元件](#)

[慣例](#)

[手動配置轉換](#)

[將PIX軟體版本升級到7.x](#)

[使用copy tftp flash命令升級PIX安全裝置](#)

[從監控模式升級PIX安全裝置](#)

[將介面名稱從Cisco PIX軟體7.0轉換為Cisco ASA格式](#)

[將配置從PIX複製到ASA](#)

[方法1:手動複製/貼上](#)

[方法2:從TFTP/FTP下載](#)

[將PIX軟體版本6.x配置應用於ASA軟體版本7.x](#)

[故障排除 — 手動配置轉換](#)

[裝置停滯在重新啟動環路中](#)

[錯誤消息](#)

[配置似乎不正確](#)

[某些服務 \(例如FTP \) 無法正常工作](#)

[將Cisco PIX安全裝置替換為Cisco Adaptive Security Appliance\(ASA\)時，無法訪問網際網路](#)

[相關資訊](#)

簡介

本文檔介紹如何從PIX 500系列安全裝置遷移到ASA 5500系列自適應安全裝置。

註：PIX 501、PIX 506和PIX 506E不支援軟體版本7。

將PIX配置轉換為ASA配置有兩種方法：

- 工具輔助轉換
- 手動轉換

基於工具的自動轉換/工具輔助轉換

Cisco建議您使用工具輔助轉換，以便將PIX配置轉換為ASA配置。

如果進行多次轉換，工具輔助轉換方法會更快且更具可擴充性。但是，中間配置中進程的輸出包含舊語法和新語法。此方法依靠在目標自適應安全裝置上安裝中間配置來完成轉換。在目標裝置上安裝之前，您無法檢視最終配置。

注意：思科已發佈PIX到ASA遷移工具，以幫助自動遷移到新的ASA裝置的過程。此工具可從PIX軟體下載站點下載。有關詳細資訊，請參閱[將PIX 500系列安全裝置的配置遷移到ASA 5500系列自適應安全裝置](#)。

必要條件

硬體和軟體要求

您可以將PIX 515、515E、525、535升級到7.0版。

在開始升級到版本7.x之前，Cisco建議PIX運行版本6.2或更高版本。這可確保正確轉換當前配置。此外，必須滿足以下硬體要求才能達到最低RAM要求：

PIX型號	RAM要求
	受限(R) 非受限(UR)/僅故障轉移(FO)
PIX-515	64 MB* 128 MB*
PIX-515 E	64 MB* 128 MB*
PIX-525	128 MB 256 MB
PIX-535	512 MB 1 GB

發出**show version**命令，以確定當前在PIX上安裝的RAM大小。

註：PIX 515和515E軟體升級也可能需要記憶體升級：

- 許可證受限且32 MB記憶體的客戶端必須升級到64 MB記憶體。
- 那些具有不受限制的許可證和64 MB記憶體的許可證必須升級到128 MB記憶體。

請參閱下表，瞭解升級這些裝置上的記憶體所需的部件號。

當前裝置配置	升級解決方案
平台許可證	總記憶體 (升級前) 部件號 總記憶體 (升級後)
受限(R)	32 MB PIX-515-MEM-32= 64 MB
非受限(UR)	32 MB PIX-515-MEM-128= 128 MB
僅故障轉移(FO)	64 MB PIX-515-MEM-128= 128 MB

注意：部件號取決於PIX上安裝的許可證。

軟體版本6.x到7.x的升級是無縫的，需要一些手動工作，但必須完成以下步驟才能開始：

1. 確保在當前配置中沒有**conduit**或**outbound/apply**命令。7.x不再支援這些命令，升級過程會刪除它們。嘗試升級之前，請使用[Conduit Converter](#)工具將這些命令轉換為訪問清單。
2. 確保PIX不會終止點對點隧道協定(PPTP)連線。軟體版本7.x當前不支援PPTP終止。
3. 開始升級過程之前，請為PIX上的VPN連線複製任何數位證書。
4. 請閱讀以下文檔，以確保您知道新的、已更改的和已棄用的命令：有關您計畫升級到的軟體版本的發行說明，請參閱「Cisco PIX安全裝置發行說明」。 [Cisco PIX 6.2和6.3使用者升級到Cisco PIX軟體7.0版指南](#)
5. 計畫在停機期間執行遷移。雖然遷移過程只需兩個步驟，但將PIX安全裝置升級到7.x是一項重大更改，需要一些停機時間。
6. 從[Cisco Downloads](#) (僅限註冊客戶) 下載7.x軟體。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA 5500系列安全裝置
- PIX安全裝置515、515E、525和535
- PIX軟體版本6.3、7.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱[思科技術提示慣例以瞭解更多有關文件慣例的資訊。](#)

手動配置轉換

通過手動轉換過程，您可以使用文本編輯器逐行完成配置，並將特定於PIX的命令轉換為ASA命令。

手動將PIX配置轉換為ASA配置可讓您最大程度地控制轉換過程。但是，該過程非常耗時，如果您必須進行多次轉換，則不能很好地擴展。

要從PIX遷移到ASA，必須完成以下三個步驟：

1. 將PIX軟體版本升級到7.x。
2. 將介面名稱從Cisco PIX軟體7.0轉換為Cisco ASA格式。
3. 將PIX軟體7.0配置複製到Cisco ASA 5500。

將PIX軟體版本升級到7.x

在開始實際的升級過程之前，請完成以下步驟：

1. 發出**show running-config**或**write net**命令，將PIX當前配置儲存到文本檔案或TFTP伺服器。
2. 發出**show version**命令以驗證要求，例如RAM。此外，將此命令的輸出儲存到文本檔案。如果需要恢復為舊版本的代碼，可能需要原始啟用金鑰。

如果PIX的基本輸入輸出系統(BIOS)版本低於4.2，或者您計畫升級已安裝PDM的PIX 515或PIX 535，則必須在「監控模式」下完成升級過程，而不是使用**copy tftp flash**方法。要檢視BIOS版本，請重新啟動PIX，並連線控制檯電纜，在啟動時閱讀消息。

BIOS版本在消息中列出，例如：

```
Rebooting....
```

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

注意：在升級過程中，6.x命令會自動轉換為7.x命令。命令的自動轉換會導致配置更改。您需要在7.x軟體啟動後檢查配置更改，以驗證自動更改是否令人滿意。然後，將配置儲存到快閃記憶體，以確保系統不會在下次安全裝置啟動時再次轉換配置。

註：系統升級為7.x後，請務必不要使用軟體版本6.x的磁碟實用程式（如密碼恢復），因為它會損壞7.x軟體映像並要求您從監控模式重新啟動系統。這還可能導致您丟失先前的配置、安全核心和金鑰資訊。

使用copy tftp flash命令升級PIX安全裝置

完成這些步驟，以便使用copy tftp flash命令升級PIX。

1. 將PIX裝置二進位制映像（例如pix701.bin）複製到TFTP伺服器的根目錄。
2. 在啟用提示符下，發出copy tftp flash命令。

```
pixfirewall>enable
Password:
```

```
pixfirewall#copy tftp flash
```

3. 輸入TFTP伺服器的IP地址。

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

4. 輸入要載入的TFTP伺服器上的檔名。這是PIX二進製影象檔名。

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

5. 系統提示啟動TFTP複製時，鍵入yes。

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

6. 現在，映像已從TFTP伺服器複製到快閃記憶體。系統將顯示此消息，指示傳輸成功，擦除快閃記憶體中的舊二進位制映像，並寫入和安裝新映像。

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

7. 重新載入PIX裝置以引導新映像。

```
pixfirewall#reload
Proceed with reload? [confirm]
```

```
Rebooting....
```

8. PIX現在啟動7.0映像，從而完成升級過程。

示例配置 — 使用copy tftp flash命令升級PIX裝置

```
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]? yes
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
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) -----
----- . . | | ||| ||| .|| ||. .|| ||. .:|||| | |||:..:|||| | |||:.
C i s c o S y s t e m s -----
--- 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/wvl/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>
```

註：發出show version命令，以驗證PIX現在是否運行7.x軟體版本。

注意：要檢查遷移配置期間發生的任何錯誤，請發出show startup-config errors命令。首次啟動PIX後，輸出中會顯示錯誤。

從監控模式升級PIX安全裝置

進入監控模式

完成以下步驟，進入PIX上的監控模式。

1. 使用以下通訊設定將控制檯電纜連線到PIX上的控制檯埠：9600位元/秒8個資料位無奇偶校驗1停止位無流量控制
2. 重新通電或重新載入PIX。啟動期間，系統將提示您使用BREAK或ESC以中斷快閃記憶體啟動。您有10秒的時間來中斷正常的引導過程。
3. 按ESC鍵或傳送BREAK字元以進入監控模式。如果使用Windows超級終端，可以按Esc鍵或按Ctrl+Break以傳送BREAK字元。如果通過終端伺服器Telnet以訪問PIX的控制檯埠，則需要按Ctrl+] (Control + 右括弧) 才能進入Telnet命令提示符。然後發出send break指令。
4. 將顯示monitor>提示。
5. 繼續前往[從監控模式升級PIX](#)部分。

從監控模式升級PIX

完成以下步驟，以便從監控模式升級PIX。

1. 將PIX裝置二進位制映像（例如pix701.bin）複製到TFTP伺服器的根目錄。
2. 進入PIX上的監控模式。如果您不確定如何執行此操作，請參閱[進入監控模式](#)。注意：一旦進入監控模式，您可以使用「？」鍵，檢視可用選項的清單。
3. 輸入TFTP伺服器所連線的介面編號，或最接近TFTP伺服器的介面。預設值為interface 1(Inside)。

```
monitor>interface
```

注意：在監控模式下，介面總是自動交涉速度和雙工。介面設定不能採用硬編碼。因此，如果PIX介面插入了硬編碼為速度/雙工的交換機，請在監控模式下將其重新配置為自動協商。此外，請注意，PIX裝置無法從監控模式初始化Gigabit乙太網介面。您必須改用快速乙太網路介面。

4. 輸入步驟3中定義的介面的IP地址。

```
monitor>address
```

5. 輸入TFTP伺服器的IP地址。

```
monitor>server
```

6. (可選) 輸入網關的IP地址。如果PIX的介面與TFTP伺服器不在同一網路上，則需要網關地址

o

```
monitor>gateway
```

7. 輸入要載入的TFTP伺服器上的檔名。這是PIX二進製影象檔名。

```
monitor>file
```

8. 從PIX ping TFTP伺服器以檢驗IP連通性。如果ping失敗，請仔細檢查電纜、PIX介面和TFTP伺服器的IP地址以及網關的IP地址 (如果需要)。ping必須成功才能繼續。

```
monitor>ping
```

9. 輸入**tftp**以開始TFTP下載。

```
monitor>tftp
```

10. PIX將映像下載到RAM中並自動啟動它。在引導過程中，檔案系統將隨當前配置一起轉換。但是，您尚未完成。在啟動後注意以下警告消息並繼續步驟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. 引導後，進入啟用模式並再次將同一映像複製到PIX。這一次，發出**copy tftp flash**命令。這

會將映像儲存到快閃記憶體檔案系統。如果未能完成此步驟，則下次重新載入PIX時會出現引導回圈。

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

註：有關如何使用copy tftp flash命令複製映像的詳細說明，請參閱[使用copy tftp flash命令升級PIX安全裝置](#)部分。

12. 使用copy tftp flash命令複製映像後，升級過程完成。示例配置 — 從監控模式升級PIX安全裝置

```
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 @ 0xffffd8000
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
```


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)
pixfirewall1#
```

將介面名稱從Cisco PIX軟體7.0轉換為Cisco ASA格式

該過程的下一步是離線編輯新轉換的基於Cisco PIX軟體7.0的配置。

由於Cisco ASA介面命名約定與Cisco PIX安全裝置不同，因此您需要先對Cisco PIX配置進行更改，然後再將其複製/上傳到Cisco ASA 5500系列安全裝置。

完成以下步驟，以便在PIX配置上更改介面名稱：

1. 離線複製新的基於Cisco PIX軟體7.0的配置。為此，請將組態上傳到TFTP/FTP伺服器，或將組態從主控台作業階段複製到文字編輯器中。若要將PIX配置上傳到TFTP/FTP伺服器，請從控制檯發出以下命令：

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

2. 基於Cisco PIX軟體7.0的配置檔案成功上傳到TFTP/FTP伺服器（或貼上或複製到文本編輯器）後，開啟記事本/寫字板或任何常用的文本編輯器，以更改PIX配置上的介面名稱。Cisco PIX安全裝置介面編號從0到n。Cisco ASA 5500系列安全裝置根據其位置/插槽對介面進行編號。嵌入式介面的編號範圍為0/0到0/3，管理介面為**Management 0/0**。4GE SSM模組上的介面編號範圍為1/0到1/3。運行7.0的基本許可證的Cisco ASA 5510具有三個快速乙太網埠（0/0到0/2）以及可用的管理0/0介面。具有Security Plus許可證的Cisco ASA 5510提供全部五個快速乙太網介面。Cisco ASA 5520和5540有四個千兆乙太網埠和一個快速乙太網管理埠。Cisco ASA 5550具有8個千兆乙太網埠和1個快速乙太網埠。將PIX配置上的介面名稱更改為ASA介面格式。**例如：**

```
Ethernet0 ==> Ethernet0/0
Ethernet1 ==> Ethernet0/1
GigabitEthernet0 ==> GigabitEthernet0/0
```

有關詳細資訊，請參閱[思科安全裝置命令列配置指南7.0版](#)中的「配置介面引數」一節。

將配置從PIX複製到ASA

此時，您擁有基於Cisco PIX軟體7.0的配置，其介面名稱已修改，準備複製或上傳到Cisco ASA 5500系列。將基於Cisco PIX軟體7.0的配置載入到Cisco ASA 5500系列裝置有兩種方法。

完成方法1中的步驟：[手動複製/貼上](#)或[方法2:從TFTP/FTP下載](#)。

方法1:手動複製/貼上

從PIX控制檯通過複製/貼上方法複製配置：

1. 在貼上修改的Cisco PIX軟體7.0配置之前，通過控制檯登入到Cisco ASA 5500系列並發出clear config all命令以清除配置。

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

2. 將配置複製並貼上到ASA控制檯，然後儲存配置。**注意：**在開始測試之前，請確保所有都處於no shutdown狀態。

方法2:從TFTP/FTP下載

第二種方法是從TFTP/FTP伺服器下載基於Cisco PIX軟體7.0的配置。對於此步驟，您需要在Cisco ASA 5500系列裝置上配置管理介面以進行TFTP/FTP下載：

1. 從ASA控制檯發出以下命令：

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

註：（可選）`route management <ip> <mask> <next-hop>`

2. 設定管理介面後，可以將PIX配置下載到ASA：

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

3. 儲存組態。

將PIX軟體版本6.x配置應用於ASA軟體版本7.x

將PIX 6.2或6.3配置轉換為新的ASA安全裝置是一個手動過程。ASA/PIX管理員需要轉換PIX 6.x語法以匹配ASA語法並將命令鍵入到ASA配置中。您可以剪下和貼上某些命令，例如**access-list**命令。請務必將PIX 6.2或6.3配置與新的ASA配置進行密切比較，以確保轉換過程中不會出錯。

注意： [Cisco CLI Analyzer](#)(**僅供已註冊**客戶使用)可用於將某些不支援的較舊命令(例如**apply**、**outbound**或**conduit**)轉換為相應的訪問清單。轉換後的報表需要徹底審查。必須驗證轉換是否匹配安全策略。

注意：升級到新ASA裝置的過程與升級到新PIX裝置的過程不同。嘗試使用PIX進程升級到ASA會在ASA上生成許多配置錯誤。

故障排除 — 手動配置轉換

裝置停滯在重新啟動環路中

- 使用**copy tftp flash**方法升級PIX並重新啟動後，它將停滯在此重新啟動環路中：

```
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.
```

使用copy tftp flash命令無法升級版本低於4.2的BIOS版本的PIX裝置。您必須使用監控模式方法對其進行升級。

- 在PIX運行7.x並重新啟動後，它將停滯在此重新啟動環路中：

```
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
```

如果PIX從監控模式升級到7.0，但7.0映像在大第一次引導7.0後沒有重新複製到快閃記憶體中，則當PIX重新載入時，它會停滯在重新啟動環路中。解析度是從監控模式重新載入影象。啟動後，您必須使用copy tftp flash方法再次複製映像。

錯誤消息

使用copy tftp flash方法進行升級時，您會看到以下錯誤消息：

```
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#
```

當使用copy tftp flash方法升級已安裝PDM的PIX 515或PIX 535時，通常會顯示此消息。

使用監控模式方法升級以解決此問題。

配置似乎不正確

將PIX從6.x升級到7.x後，某些配置不能正確遷移。

show startup-config errors命令的輸出顯示了遷移配置期間出現的任何錯誤。首次啟動PIX後，輸出中會顯示錯誤。檢查這些錯誤並嘗試解決它們。

某些服務 (例如FTP) 無法正常工作

有時，某些服務 (例如FTP) 在升級後無法正常工作。

升級後未啟用對這些服務的檢查。啟用相應服務的檢查。為此，請將它們新增到預設/全域性檢查策略或為所需服務建立單獨的檢查策略。

有關檢查策略的詳細資訊，請參閱[思科安全裝置命令列配置指南7.0版](#)中的「應用應用層協定檢查」一節。

將Cisco PIX安全裝置替換為Cisco Adaptive Security Appliance(ASA)時，無法訪問網際網路

如果在用思科自適應安全裝置(ASA)替換思科PIX安全裝置後無法訪問網際網路，請使用此部分。

當您將PIX從網路中拔出並將具有與PIX的外部介面IP地址相同的Outside interface IP地址的ASA連線到網路上時，上游路由器仍然具有與Outside interface IP Address對應的PIX的mac-address。因此，它無法將應答資料包傳送回ASA。為了使ASA正常工作，您必須清除上游路由器上的ARP條目，以便獲取新的/正確的mac地址條目。如果在計畫使用ASA替換PIX時清空ARP條目，它將解決Internet連線問題。ARP條目清除必須由ISP在其末端完成。

相關資訊

- [Cisco PIX 500系列安全裝置 — 簡介](#)
- [技術支援與文件 - Cisco Systems](#)