Software-Upgrade-Verfahren für PIX 500 Security Appliance 6.x auf 7.x

Inhalt

Einführung

In diesem Dokument wird erläutert, wie Sie die PIX-Appliance von Version 6.2 oder 6.3 auf Version 7.x aktualisieren. Darüber hinaus wird die Installation von ASDM (Adaptive Security Device Manager) Version 5.0 behandelt.

Voraussetzungen

Anforderungen

Führen Sie diese Schritte aus, bevor Sie dieses Upgrade starten.

- Verwenden Sie den Befehl **show running-config** oder **write net**, um die aktuelle PIX-Konfiguration in einer Textdatei oder einem TFTP-Server zu speichern.

- Verwenden Sie den Befehl **show version**, um die Seriennummer und den Aktivierungsschlüssel anzuzeigen. Speichern Sie diese Ausgabe in einer Textdatei. Wenn Sie zu einer älteren Version des Codes zurückkehren müssen, benötigen Sie möglicherweise den ursprünglichen Aktivierungsschlüssel. Weitere Informationen zu Aktivierungsschlüsseln finden Sie unter Häufig gestellte Fragen zur PIX-Firewall.
- Vergewissern Sie sich, dass in der aktuellen Konfiguration keine **Kanäle** oder **ausgehenden** Befehle vorhanden sind. Diese Befehle werden in 7.x nicht mehr unterstützt, und sie werden beim Upgrade entfernt. Verwenden Sie das Output Interpreter-Tool (nur registrierte Kunden), um diese Befehle in Zugriffslisten umzuwandeln, bevor Sie das Upgrade durchführen.
- Stellen Sie sicher, dass PIX keine PPTP-Verbindungen (Point to Point Tunneling Protocol) terminiert. PIX 7.1 und höher unterstützt derzeit keine PPTP-Terminierung.
- Wenn Sie Failover verwenden, stellen Sie sicher, dass die LAN- oder Stateful-Schnittstelle nicht für Daten freigegeben wird, die Schnittstellen passieren. Wenn Sie z. B. Ihre Inside-Schnittstelle verwenden, um Datenverkehr sowie Ihre Stateful Failover-Schnittstelle (Failover-Verbindung innen) weiterzuleiten, müssen Sie die Stateful Failover-Schnittstelle vor dem Upgrade auf eine andere Schnittstelle verschieben. Andernfalls werden alle an die interne Schnittstelle gebundenen Konfigurationen entfernt. Außerdem durchläuft der Datenverkehr nach dem Upgrade nicht die Schnittstelle.
- Stellen Sie sicher, dass PIX die Version 6.2 oder 6.3 ausführt, bevor Sie fortfahren.
- Lesen Sie die Versionshinweise für die Version, auf die Sie ein Upgrade planen, sodass Sie alle neuen, geänderten und veralteten Befehle kennen.
- Weitere Befehlsänderungen zwischen den Versionen 6.x und 7.x finden Sie im Aktualisierungshandbuch.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- PIX Security Appliance 515, 515E, 525 und 535
- PIX Softwareversionen 6.3(4), 7.0(1)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Mindestsystemanforderungen

Bevor Sie das Upgrade auf Version 7.x starten, empfiehlt Cisco die Ausführung von PIX Version 6.2 oder höher. Dadurch wird sichergestellt, dass die aktuelle Konfiguration korrekt konvertiert wird. Darüber hinaus müssen diese Hardwareanforderungen für die minimalen RAM- und Flash-Anforderungen erfüllt werden:

PIX-Modell	RAM-Anforderungen		Flash-Anforderungen
	Eingeschränkt (R)	UnRestricted (UR)/Failover Only	

		(FO)	
PIX-515	64 MB*	128 MB*	16 MB
PIX-515 E	64 MB*	128 MB*	16 MB
PIX-525	128 MB	256 MB	16 MB
PIX-535	512 MB	1 GB	16 MB

* Für alle PIX-515- und PIX-515E-Appliances ist ein Speicher-Upgrade erforderlich.

Geben Sie den Befehl **show version** ein, um die derzeit auf dem PIX installierte RAM- und Flash-Kapazität zu ermitteln. Flash-Upgrades sind nicht erforderlich, da bei allen PIX-Appliances in dieser Tabelle standardmäßig 16 MB installiert sind.

Hinweis: Nur die in dieser Tabelle aufgeführten PIX Security Appliances werden in Version 7.x unterstützt. Ältere PIX Security Appliances wie PIX-520, 510, 1000 und Classic wurden eingestellt und führen keine Version 7.0 oder höher aus. Wenn Sie über eine dieser Appliances verfügen und 7.x oder höher ausführen möchten, wenden Sie sich an Ihr Cisco Account Team oder Ihren Reseller vor Ort, um eine neuere Security Appliance zu erwerben. Darüber hinaus können PIX-Firewalls mit weniger als 64 MB RAM (PIX-501, PIX-506 und PIX-506E) die erste Version von 7.0 nicht ausführen.

Informationen zum Speicher-Upgrade für PIX 515/515E-Appliances

Speicher-Upgrades sind nur für die PIX-515- und PIX-515E-Appliances erforderlich. In dieser Tabelle finden Sie die Teilenummern, die Sie zur Aktualisierung des Speichers dieser Appliances benötigen.

Hinweis: Die Teilenummer hängt von der auf dem PIX installierten Lizenz ab.

Aktuelle Appliance-Konfiguration		**Upgrade-Lösung**	
Plattformlizenz	**Gesamtspeicher (vor dem Upgrade)**	**Teilenummer**	**Gesamtspeicher (nach dem Upgrade)**
Eingeschränkt (R)	32 MB	PIX-515-MEM-32=	64 MB
Uneingeschränkt (UR)	32 MB	PIX-515-MEM-128=	128 MB
Failover Only (FO)	64 MB	PIX-515-MEM-128=	128 MB

Weitere Informationen finden Sie im Produktbulletin Cisco PIX 515/515E Security Appliance Memory Upgrade for PIX Software v7.0.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

PIX Security Appliance aktualisieren

Software-Downloads

Besuchen Sie das Cisco Software Center (nur registrierte Kunden), um die PIX 7.x-Software herunterzuladen. Die TFTP-Serversoftware ist nicht mehr über Cisco.com verfügbar. Sie können jedoch viele TFTP-Server finden, wenn Sie in Ihrer bevorzugten Internet-Suchmaschine nach "tftp server" suchen. Cisco empfiehlt keine spezielle TFTP-Implementierung. Weitere Informationen finden Sie auf der TFTP-Serverseite (nur registrierte Kunden).

Upgrade-Verfahren

Beachten Sie, dass das Upgrade Ihrer PIX Security Appliance auf Version 7.x eine wesentliche Änderung darstellt. Ein Großteil der CLI wird geändert, sodass Ihre Konfiguration nach dem Upgrade sehr unterschiedlich aussieht. Upgrades erfolgen nur während eines Wartungsfensters, da der Upgrade-Prozess einige Ausfallzeiten erfordert. Wenn Sie auf ein 6.x-Image zurücksetzen müssen, müssen Sie die Verfahren zum Downgrade befolgen. Andernfalls wird der PIX in eine kontinuierliche Neustartschleife geleitet. Um fortzufahren, suchen Sie Ihr PIX-Appliance-Modell in dieser Tabelle, und wählen Sie dann den Link aus, um Anweisungen zum Upgrade anzuzeigen.

PIX-Modell	Upgrade-Methode
PIX-515	Überwachung
PIX-515E	TFTP-Flash kopieren
PIX-525	TFTP-Flash kopieren
PIX-535 (kein PDM installiert)	TFTP-Flash kopieren
PIX-535 (PDM installiert)	Überwachung

PIX Security Appliance im Überwachungsmodus aktualisieren

Überwachungsmodus eingeben

Führen Sie diese Schritte aus, um in den Überwachungsmodus auf dem PIX zu wechseln.

1. Verbinden Sie ein Konsolenkabel mithilfe der folgenden Kommunikationseinstellungen mit dem Konsolenport auf dem PIX:9600 Bit pro Sekunde8 DatenbitsKeine Parität1 Stoppbitkeine Flusssteuerung
2. Schalten Sie den PIX aus oder laden Sie ihn neu. Während des Bootvorgangs werden Sie aufgefordert, BREAK oder ESC zu verwenden, um den Flash-Boot zu unterbrechen. Sie haben zehn Sekunden, um den normalen Startvorgang zu unterbrechen.
3. Drücken Sie die **ESC**-Taste, oder senden Sie ein **BREAK**-Zeichen, um in den Überwachungsmodus zu wechseln.Wenn Sie Windows Hyper Terminal verwenden, können Sie die **ESC**-Taste drücken oder **Strg+Break** drücken, um ein BREAK-Zeichen zu senden.Wenn Sie Telnet über einen Terminalserver auf den Konsolenport des PIX zugreifen möchten, drücken Sie **Strg+]** (Steuerung + rechte Halterung), um zur Telnet-Eingabeaufforderung zu gelangen. Geben Sie dann den Befehl **send break** ein.

4. Die Eingabeaufforderung `Monitor>` wird angezeigt.
5. Fahren Sie mit dem Abschnitt PIX-Upgrade vom Überwachungsmodus fort.

PIX aus Überwachungsmodus aktualisieren

Führen Sie diese Schritte aus, um Ihr PIX vom Überwachungsmodus zu aktualisieren.

Hinweis: Fast Ethernet-Karten in 64-Bit-Steckplätzen sind im Überwachungsmodus nicht sichtbar. Dieses Problem bedeutet, dass sich der TFTP-Server nicht auf einer dieser Schnittstellen befinden kann. Der Benutzer sollte den Befehl **copy tftp flash** verwenden, um die PIX Firewall-Image-Datei über TFTP herunterzuladen.

1. Kopieren Sie das Binär-Image der PIX-Appliance (z. B. pix701.bin) in das Stammverzeichnis des TFTP-Servers.
2. Wechseln Sie auf dem PIX in den Überwachungsmodus. Wenn Sie sich nicht sicher sind, wie dies geschieht, sehen Sie sich die Anweisungen zum Aufrufen des Überwachungsmodus in diesem Dokument an.**Hinweis:** Sobald Sie sich im Überwachungsmodus befinden, können Sie das "?" um eine Liste der verfügbaren Optionen anzuzeigen.
3. Geben Sie die Schnittstellennummer ein, mit der der TFTP-Server verbunden ist, oder die Schnittstelle, die dem TFTP-Server am nächsten ist. Der Standardwert ist "Interface 1 (Inside)".
   ```
   monitor>interface
   ```

   Hinweis: Im Überwachungsmodus handelt die Schnittstelle immer automatisch die Geschwindigkeit und den Duplex aus. Die Schnittstelleneinstellungen können nicht fest codiert werden. Wenn die PIX-Schnittstelle an einen fest codierten Switch für Geschwindigkeit/Duplex angeschlossen ist, konfigurieren Sie diese daher neu, um die automatische Aushandlung durchzuführen, während Sie sich im Überwachungsmodus befinden. Beachten Sie außerdem, dass die PIX-Appliance eine Gigabit Ethernet-Schnittstelle nicht über den Überwachungsmodus initialisieren kann. Sie müssen stattdessen eine Fast Ethernet-Schnittstelle verwenden.
4. Geben Sie die IP-Adresse der in Schritt 3 definierten Schnittstelle ein.
   ```
   monitor>address
   ```

5. Geben Sie die IP-Adresse des TFTP-Servers ein.
   ```
   monitor>server
   ```

6. (Optional) Geben Sie die IP-Adresse Ihres Kabelmodems ein. Eine Gateway-Adresse ist

erforderlich, wenn sich die Schnittstelle des PIX nicht im gleichen Netzwerk wie der TFTP-Server befindet.

```
monitor>gateway
```

7. Geben Sie den Namen der Datei auf dem TFTP-Server ein, den Sie laden möchten. Dies ist der Name der PIX-Binär-Image-Datei.

```
monitor>file
```

8. Pingen Sie vom PIX zum TFTP-Server, um die IP-Verbindung zu überprüfen.Wenn die Pings fehlschlagen, überprüfen Sie die Kabel, die IP-Adresse der PIX-Schnittstelle und des TFTP-Servers sowie ggf. die IP-Adresse des Gateways. Die Pings müssen erfolgreich sein, bevor Sie fortfahren.

```
monitor>ping
```

9. Geben Sie **tftp ein**, um den TFTP-Download zu starten.

```
monitor>tftp
```

10. Das PIX lädt das Bild in den RAM und bootet es automatisch.Während des Bootvorgangs wird das Dateisystem zusammen mit Ihrer aktuellen Konfiguration konvertiert. Sie sind jedoch noch nicht fertig. Beachten Sie diese Warnmeldung nach dem Starten, und fahren Sie mit Schritt 11 fort:

```
************************************************************
  **                                                      **
  **   *** 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. Sobald der Startvorgang gestartet wurde, aktivieren Sie den Aktivierungsmodus, und kopieren Sie das gleiche Bild erneut auf den PIX. Verwenden Sie dieses Mal den Befehl **copy tftp flash**.Dadurch wird das Bild im Flash-Dateisystem gespeichert. Wenn dieser Schritt nicht ausgeführt wird, wird beim nächsten Neustart des PIX eine Boot-Schleife erzeugt.

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

Hinweis: Detaillierte Anweisungen zum Kopieren des Images mit dem Befehl **copy tftp flash** finden Sie im Abschnitt Upgrade the PIX Security Appliance with the copy tftp flash Command.

12. Nachdem das Bild mit dem Befehl **copy tftp flash** kopiert wurde, ist der Aktualisierungsvorgang abgeschlossen.

Beispielkonfiguration - Aktualisieren der PIX Security Appliance vom Überwachungsmodus

```
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: 15998976 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)
  ------------------------------------------------------------------------
                                .           .
                                |           |
                               |||         |||
                             .|| ||.     .|| ||.
                           .:|||  | |||:..:|||  | |||:.
                            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/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#
```

Aktualisieren Sie die PIX Security Appliance mit dem Befehl copy tftp flash.

Führen Sie diese Schritte aus, um das PIX mithilfe des Befehls **copy tftp flash** zu aktualisieren.

1. Kopieren Sie das Binär-Image der PIX-Appliance (z. B. pix701.bin) in das Stammverzeichnis des TFTP-Servers.
2. Geben Sie an der Eingabeaufforderung enable den Befehl **copy tftp flash ein**.
   ```
   pixfirewall>enable
   Password:

   pixfirewall#copy tftp flash
   ```
3. Geben Sie die IP-Adresse des TFTP-Servers ein.
   ```
   Address or name of remote host [0.0.0.0]?
   ```
4. Geben Sie den Namen der Datei auf dem TFTP-Server ein, den Sie laden möchten. Dies ist der Name der PIX-Binär-Image-Datei.
   ```
   Source file name [cdisk]?
   ```
5. Wenn Sie aufgefordert werden, die TFTP-Kopie zu starten, geben Sie **yes ein**.
   ```
   copying tftp://172.18.173.123/pix701.bin to flash:image
   [yes|no|again]?yes
   ```
6. Das Image wird nun vom TFTP-Server in Flash kopiert.Diese Meldung wird angezeigt und weist darauf hin, dass die Übertragung erfolgreich ist, das alte Binär-Image in Flash gelöscht wird und das neue Image geschrieben und installiert wird.
   ```
   !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   Received 5124096 bytes
   Erasing current image
   Writing 5066808 bytes of image
   !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   Image installed
   pixfirewall#
   ```
7. Laden Sie die PIX-Appliance neu, um das neue Image zu starten.
   ```
   pixfirewall#reload
   Proceed with reload? [confirm]


   Rebooting....
   ```
8. Das PIX bootet jetzt das 7.0-Image und damit ist der Upgrade-Prozess abgeschlossen.

Beispielkonfiguration - Aktualisieren der PIX-Appliance mit dem Befehl copy tftp flash Command

```
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..ÿ

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 @ 0xfff00000

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/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>
```

Hinweis: Mit der uneingeschränkten Lizenz kann PIX 515 E bis zu acht VLANs und PIX 535 bis zu fünfundzwanzig VLANs umfassen.

Downgrade von PIX 7.x auf 6.x

PIX Security Appliances Version 7.0 und höher verwenden ein anderes Flash-Dateiformat als frühere PIX-Versionen. Aus diesem Grund können Sie mit dem Befehl **copy tftp flash** kein Downgrade von einem 7.0-Image auf ein 6.x-Image durchführen. Stattdessen müssen Sie den Befehl **Downgrade** verwenden. Andernfalls wird der PIX in eine Boot-Schleife gesteckt.

Bei der ursprünglichen PIX-Aktualisierung wurde die 6.x-Startkonfiguration in Flash als downgrade.cfg gespeichert. Wenn Sie dieses Downgrade durchführen, wird diese Konfiguration beim Herunterladen auf das Gerät wiederhergestellt. Diese Konfiguration kann überprüft werden, bevor Sie ein Downgrade durchführen, wenn Sie den Befehl **more flash:downgrade.cfg** von einer `enable>`-Eingabeaufforderung in 7.0 ausführen. Wenn das PIX per Monitor Mode aktualisiert wurde, wird das vorherige 6.x Binär-Image weiterhin als image_old.bin in Flash gespeichert. Sie können überprüfen, ob dieses Bild vorhanden ist, wenn Sie den **Blitz anzeigen:** aus. Wenn das Bild auf Flash vorhanden ist, können Sie dieses Bild in Schritt 1 dieses Verfahrens verwenden, anstatt es von einem TFTP-Server zu laden.

Führen Sie diese Schritte aus, um ein Downgrade der PIX Security Appliance durchzuführen.

1. Geben Sie den Befehl **Downgrade** ein, und geben Sie den Speicherort des Bilds an, auf das Sie ein Downgrade durchführen möchten.
   ```
   pixfirewall#downgrade tftp://
   ```

   Hinweis: Wenn Sie PIX vom Überwachungsmodus aus aktualisiert haben, wird das alte Binär-Image weiterhin in Flash gespeichert. Geben Sie diesen Befehl ein, um ein Downgrade auf das Bild durchzuführen:
   ```
   pixfirewall#downgrade flash:/image_old.bin
   ```

2. Es wird eine Warnmeldung angezeigt, die Sie darüber informiert, dass der Flash-Speicher gerade erstellt wird. Drücken Sie **die Eingabetaste**, um fortzufahren.
   ```
   This command will reformat the flash and automatically reboot the system.
   Do you wish to continue? [confirm]
   ```

3. Das Bild wird nun in den RAM kopiert, und die Startkonfiguration wird ebenfalls in den RAM kopiert.

```
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Buffering startup config

All items have been buffered successfully
```

4. Es wird eine zweite Warnmeldung angezeigt, die anzeigt, dass der Flash jetzt mit der Formatierung beginnt. Unterbrechen Sie diesen Vorgang NICHT, oder der Flash-Speicher kann beschädigt werden. Drücken Sie **die Eingabetaste**, um mit dem Format fortzufahren.

```
If the flash reformat is interrupted or fails,
data in flash will be lost
and the system might drop to monitor mode.
Do you wish to continue? [confirm]
```

5. Der Flash ist nun formatiert und das alte Image installiert, und der PIX wird neu gestartet.

```
Acquiring exclusive access to flash
Installing the correct file system for the image and
saving the buffered data
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Flash downgrade succeeded


Rebooting....
```

6. Der PIX startet jetzt bis zur normalen Eingabeaufforderung. Damit ist der Downgrade-Prozess abgeschlossen.

Beispielkonfiguration - Downgrade von PIX 7.x auf 6.x

```
pixfirewall#downgrade tftp://172.18.108.26/pix634.bin
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]

Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Buffering startup config

All items have been buffered successfully.
If the flash reformat is interrupted or fails, data in flash will be lost
and the system might drop to monitor mode.
Do you wish to continue? [confirm]
Acquiring exclusive access to flash
Installing the correct file system for the image and saving the buffered data
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Flash downgrade succeeded



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 @ 0xfff00000

Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Reading 1962496 bytes of image from flash.
################################################################################
################################
128MB RAM
mcwa i82559 Ethernet at irq 11 MAC: 0009.4360.ed44
mcwa i82559 Ethernet at irq 10 MAC: 0009.4360.ed43
System Flash=E28F128J3 @ 0xfff00000
BIOS Flash=am29f400b @ 0xd8000
IRE2141 with 2048KB

------------------------------------------------------------------------
|| ||
|| ||
|||| ||||
..:||||||:..:||||||:..
c i s c o S y s t e m s
Private Internet eXchange
------------------------------------------------------------------------
Cisco PIX Firewall

Cisco PIX Firewall Version 6.3(4)
Licensed Features:
Failover: Enabled
VPN-DES: Enabled
VPN-3DES-AES: Enabled
Maximum Physical Interfaces: 6
Maximum Interfaces: 10
Cut-through Proxy: Enabled
Guards: Enabled
URL-filtering: Enabled
Inside Hosts: Unlimited
Throughput: Unlimited
IKE peers: Unlimited

This PIX has an Unrestricted (UR) license.


****************************** Warning ******************************
Compliance with U.S. Export Laws and Regulations - Encryption.

This product performs encryption and is regulated for export
by the U.S. Government.
```

```
This product is not authorized for use by persons located
outside the United States and Canada that do not have prior
approval from Cisco Systems, Inc. or the U.S. Government.

This product may not be exported outside the U.S. and Canada
either by physical or electronic means without PRIOR approval
of Cisco Systems, Inc. or the U.S. Government.

Persons outside the U.S. and Canada may not re-export, resell
or transfer this product by either physical or electronic means
without prior approval of Cisco Systems, Inc. or the U.S.
Government.
****************************** Warning *******************************

Copyright (c) 1996-2003 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


Cryptochecksum(unchanged): 9fa48219 950977b6 dbf6bea9 4dc97255
Type help or '?' for a list of available commands.
pixfirewall>
```

Upgrade von PIX-Appliances in einem Failover-Set

Ein Upgrade von PIX Appliance 6.x auf 7.x ist ein wichtiges Upgrade. Dies ist nicht ohne Ausfallzeiten möglich, auch nicht für PIXes in einem Failover-Set. Viele der Failover-Befehle ändern sich mit der Aktualisierung. Als Upgrade-Pfad wird empfohlen, einen der PIX im Failover-Satz herunterzufahren. Befolgen Sie dann die Anweisungen in diesem Dokument, um ein Upgrade des eingeschalteten PIX durchzuführen. Nachdem die Aktualisierung abgeschlossen ist, überprüfen Sie, ob der Datenverkehr erfolgreich verläuft, und starten Sie den PIX auch einmal neu, um sicherzustellen, dass er problemlos wieder aufgenommen wird. Wenn Sie sich davon überzeugt haben, dass alles ordnungsgemäß funktioniert, schalten Sie das neu aktualisierte PIX aus, und schalten Sie das andere PIX ein. Folgen Sie dann den Anweisungen in diesem Dokument, um das PIX zu aktualisieren. Überprüfen Sie nach Abschluss der Aktualisierung, ob der Datenverkehr erfolgreich verläuft. Führen Sie auch einen einmal erneuten Neustart des PIX durch, um sicherzustellen, dass der PIX fehlerfrei wiederhergestellt wird. Wenn Sie sich davon überzeugt haben, dass alles ordnungsgemäß funktioniert, schalten Sie die andere PIX ein. Beide PIXs werden jetzt auf 7.x aktualisiert und eingeschaltet. Stellen Sie sicher, dass die Failover-Kommunikation mit dem Befehl **show failover** ordnungsgemäß eingerichtet wird.

Hinweis: PIX setzt jetzt die Einschränkung durch, dass eine Schnittstelle, die Datenverkehr übergibt, nicht auch als LAN-Failover-Schnittstelle oder Stateful Failover-Schnittstelle verwendet werden kann. Wenn Ihre aktuelle PIX-Konfiguration über eine gemeinsam genutzte Schnittstelle verfügt, über die der normale Datenverkehr sowie die LAN-Failover-Informationen oder Stateful-Informationen weitergeleitet werden. Wenn Sie ein Upgrade durchführen, wird der Datenverkehr nicht mehr über diese Schnittstelle geleitet. Alle Befehle, die dieser Schnittstelle zugeordnet sind,

schlagen ebenfalls fehl.

Installation des Adaptive Security Device Manager (ASDM)

Bevor Sie ASDM installieren, empfiehlt Cisco, die Versionshinweise für die Version zu lesen, die Sie installieren möchten. Die Versionshinweise enthalten die mindestens unterstützten Browser und Java-Versionen sowie eine Liste der unterstützten neuen Funktionen und offenen Hinweise.

Die Installation von ASDM erfolgt in Version 7.0 etwas anders als in der Vergangenheit. Nachdem das ASDM-Image in Flash kopiert wurde, müssen Sie es in der Konfiguration angeben, damit das PIX es verwenden kann. Führen Sie diese Schritte aus, um das ASDM-Image in Flash zu installieren.

1. Laden Sie das ASDM-Image (nur registrierte Kunden) von Cisco.com herunter, und legen Sie es im Stammverzeichnis Ihres TFTP-Servers ab.
2. Überprüfen Sie, ob Ihr PIX über eine IP-Verbindung zu Ihrem TFTP-Server verfügt. Dazu pingen Sie den TFTP-Server vom PIX.
3. Geben Sie an der Eingabeaufforderung enable den Befehl **copy tftp flash ein**.
   ```
   pixfirewall>enable
   Password:

   pixfirewall#copy tftp flash
   ```
4. Geben Sie die IP-Adresse des TFTP-Servers ein.
   ```
   Address or name of remote host [0.0.0.0]?
   ```
5. Geben Sie den Namen der ASDM-Datei auf dem TFTP-Server ein, den Sie laden möchten.
   ```
   Source file name [cdisk]?
   ```
6. Geben Sie den Namen der ASDM-Datei ein, die Sie in Flash speichern möchten. Drücken Sie **die Eingabetaste**, um den gleichen Dateinamen beizubehalten.
   ```
   Destination filename [asdm-501.bin]?
   ```
7. Das Image wird nun vom TFTP-Server in Flash kopiert. Diese Meldungen werden angezeigt und weisen darauf hin, dass die Übertragung erfolgreich war.
   ```
   Accessing tftp://172.18.173.123/asdm-501.bin...
   !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   !!!!!!!!!!!!!!!!
   Writing file flash:/asdm-501.bin...
   ```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!
5880016 bytes copied in 140.710 secs (42000 bytes/sec)
```

8. Nachdem das ASDM-Image kopiert wurde, geben Sie den **ASDM-Image-Flash** aus: , um das zu verwendende ASDM-Image anzugeben.
   ```
   pixfirewall(config)#asdm image flash:asdm-501.bin
   ```

9. Speichern Sie die Konfiguration mit dem Befehl **write memory** in Flash.
   ```
   pixfirewall(config)#write memory
   ```

10. Damit ist der ASDM-Installationsprozess abgeschlossen.

Fehlerbehebung

Symptom	Auflösung
Nachdem Sie die **copy tftp flash**-Methode verwendet haben, um das PIX zu aktualisieren und einen Neustart durchzuführen, bleibt es in dieser Reboot-Schleife stecken: **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.	PIX-Appliances mit BIOS-Versionen vor 4.2 können nicht mithilfe des Befehls **copy tftp flash** aktualisiert werden. Sie müssen diese mit der Monitor Mode-Methode aktualisieren.
Nachdem PIX 7.0 ausgeführt und neu gestartet wurde, bleibt es in dieser Reboot-Schleife stecken: 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...	Wenn das PIX vom Überwachungsmodus auf 7.0 aktualisiert wurde, das 7.0-Image jedoch nach dem ersten Start von 7.0 nicht erneut in Flash kopiert wurde, bleibt es beim erneuten Laden des PIX in einer Neustartschleife stecken. Die Auflösung besteht darin, das Bild erneut aus dem Überwachungsmodus zu laden. Nach dem Booten müssen Sie das Bild erneut mit der **copy tftp flash**-Methode kopieren.

<table>
<tr><td><code>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</code></td><td></td></tr>
<tr><td>Beim Upgrade mit der copy tftp flash method wird die folgende Fehlermeldung angezeigt:
<code>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#</code></td><td>Diese Meldung wird in der Regel angezeigt, wenn das PIX-535 oder PIX-515 (nicht E) über die copy tftp flash-Methode aktualisiert wird und PDM auch in Flash auf diesem PIX geladen wird. Die Auflösung besteht in der Aktualisierung mit der Monitor Mode-Methode.</td></tr>
<tr><td>Nachdem Sie das PIX von 6.x auf 7.0 aktualisiert haben, werden einige Konfigurationen nicht ordnungsgemäß migriert.</td><td>Die Ausgabe des Befehls show startup-config errors zeigt alle Fehler an, die während der Migration der Konfiguration aufgetreten sind. Die Fehler werden in dieser Ausgabe</td></tr>
</table>

	angezeigt, nachdem Sie das PIX zum ersten Mal gestartet haben. Untersuchen Sie diese Fehler, und versuchen Sie, sie zu beheben.
Auf dem PIX wird Version 7.x ausgeführt, und es wird eine neuere Version installiert. Beim Neustart des PIX wird die alte Version weiterhin geladen.	In PIX Version 7.x können Sie mehrere Bilder in Flash speichern. Das PIX sucht zunächst in der Konfiguration nach einem **Flash-Speicher** des **Startsystems:** Befehle. Diese Befehle geben an, welches Image das PIX booten muss. Wenn kein **Flash-Speicher des Startsystems angezeigt wird:** -Befehlen gefunden werden, startet PIX das erste bootfähige Image in Flash. Um eine andere Version zu starten, geben Sie die Datei mit dem Befehl **flash:/<filename>** an.
Ein ASDM-Image wird in Flash geladen, aber Benutzer können ASDM nicht in ihren Browser laden.	Stellen Sie zunächst sicher, dass die ASDM-Datei, die in Flash geladen wird, mit dem Befehl **asdm image flash://<asdm_file>** angegeben wird. Überprüfen Sie anschließend, ob sich der Befehl **http-server enable** in der Konfiguration befindet. Überprüfen Sie abschließend, ob der Host, der versucht, ASDM zu laden, über den Befehl **http <address> <mask> <interface>** zugelassen ist.
Nach einem Upgrade funktioniert FTP nicht.	Die FTP-Prüfung wurde nach dem Upgrade nicht aktiviert. Aktivieren Sie die FTP-Prüfung auf zwei Arten, wie im Abschnitt Enable FTP Inspection (FTP-Prüfung aktivieren) gezeigt.

FTP-Prüfung aktivieren

FTP-Prüfung kann mit einer der folgenden beiden Methoden aktiviert werden:

- **FTP zur Standard-/globalen Prüfrichtlinie hinzufügen.**Wenn sie nicht vorhanden ist, erstellen Sie die **Inspection_default** class-map.

```
PIX1#configure terminal
PIX1(config)#class-map inspection_default
PIX1(config-cmap)#match default-inspection-traffic
PIX1(config-cmap)#exit
```

Erstellen oder bearbeiten Sie die **global_policy-**Richtlinienzuordnung, und aktivieren Sie die FTP-Prüfung für die class **inspektion_default**.

```
PIX1(config)#policy-map global_policy
PIX1(config-pmap)#class inspection_default
PIX1(config-pmap-c)#inspect dns preset_dns_map
PIX1(config-pmap-c)#inspect ftp
PIX1(config-pmap-c)#inspect h323 h225
PIX1(config-pmap-c)#inspect h323 ras
PIX1(config-pmap-c)#inspect rsh
PIX1(config-pmap-c)#inspect rtsp
PIX1(config-pmap-c)#inspect esmtp
PIX1(config-pmap-c)#inspect sqlnet
PIX1(config-pmap-c)#inspect skinny
PIX1(config-pmap-c)#inspect sunrpc
PIX1(config-pmap-c)#inspect xdmcp
PIX1(config-pmap-c)#inspect sip
PIX1(config-pmap-c)#inspect netbios
PIX1(config-pmap-c)#inspect tftp
```

Aktivieren Sie die **global_policy** global.

```
PIX1(config)#service-policy global_policy global
```

- **Aktivieren Sie FTP, indem Sie eine separate Überprüfungsrichtlinie erstellen.**

```
PIX1#configure terminal
PIX1(config)#class-map ftp-traffic
!--- Matches the FTP data traffic. PIX1(config-cmap)#match port tcp eq ftp
PIX1(config-cmap)#exit

PIX1(config)#policy-map ftp-policy
```

```
PIX1(config-pmap)#class ftp-traffic

!--- Inspection for the FTP traffic is enabled. PIX1(config-pmap-c)#inspect ftp
PIX1(config-pmap)#exit
PIX1(config)#exit

!--- Applies the FTP inspection globally. PIX1(config)#service-policy ftp-policy global
```

Anfordern eines gültigen Servicevertrags

Sie benötigen einen gültigen Servicevertrag, um die PIX-Software herunterzuladen. Gehen Sie wie folgt vor, um einen Servicevertrag abzuschließen:

- Wenden Sie sich an Ihr Cisco Account Team, wenn Sie einen direkten Kaufvertrag abgeschlossen haben.
- Wenden Sie sich an einen Cisco Partner oder Reseller, um einen Servicevertrag zu erwerben.
- Verwenden Sie den Profile Manager, um Ihr Cisco.com-Profil zu aktualisieren und eine Zuordnung zu einem Servicevertrag anzufordern.

Zugehörige Informationen

- Support-Seite für PIX Security Appliance
- PIX-Befehlsreferenz
- Anforderungen für Kommentare (RFCs)
- PIX Firewall Häufig gestellte Fragen
- Technischer Support und Dokumentation für Cisco Systeme