Migration von Security Appliances der Serie PIX 500 zu Adaptive Security Appliances der Serie ASA 5500

Inhalt

Einführung

In diesem Dokument wird erläutert, wie Sie von den Sicherheitslösungen der Serie PIX 500 auf Adaptive Security Appliances der Serie ASA 5500 migrieren.

Hinweis: PIX 501, PIX 506 und PIX 506E unterstützen die Softwareversion 7 nicht.

Es gibt zwei Möglichkeiten, eine PIX-Konfiguration in eine ASA-Konfiguration zu konvertieren:

- Tool-unterstützte Konvertierung
- Manuelle Konvertierung

Automatische Tool-/Tool-gestützte Konvertierung

Cisco empfiehlt die Verwendung der Tool-unterstützten Konvertierung, um PIX-Konfigurationen in ASA-Konfigurationen zu konvertieren.

Die Konvertierungsmethode mit Tool-Unterstützung ist schneller und skalierbarer, wenn Sie mehrere Konvertierungen vornehmen. Die Ausgabe des Prozesses in einer Zwischenkonfiguration enthält jedoch sowohl die alte Syntax als auch die neue Syntax. Diese Methode erfordert die Installation der Zwischenkonfiguration auf der Adaptive Security Appliance, um die Konvertierung abzuschließen. Bis es auf dem Zielgerät installiert ist, können Sie die endgültige Konfiguration nicht anzeigen.

Hinweis: Cisco hat das Migrationstool PIX to ASA veröffentlicht, um die Migration auf die neuen ASA-Appliances zu automatisieren. Dieses Tool kann von der Download-Website der PIX-Software heruntergeladen werden. Weitere Informationen finden Sie unter Migration der Konfiguration der Sicherheitslösungen der Serie PIX 500 auf Adaptive Security Appliances der Serie ASA 5500.

Voraussetzungen

Hardware- und Softwareanforderungen

Sie können PIX 515, 515E, 525, 535 auf Version 7.0 aktualisieren.

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-Anforderungen erfüllt werden:

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

Geben Sie den Befehl **show version** ein, um die derzeit auf dem PIX installierte RAM-Kapazität zu ermitteln.

Hinweis: Software-Upgrades für PIX 515 und 515E erfordern u. U. auch ein Speicher-Upgrade:

- Diejenigen mit eingeschränkten Lizenzen und 32 MB Arbeitsspeicher müssen auf 64 MB Arbeitsspeicher aktualisiert werden.
- Diejenigen mit uneingeschränkten Lizenzen und 64 MB Arbeitsspeicher müssen auf 128 MB Arbeitsspeicher aktualisiert werden.

In dieser Tabelle finden Sie die Teilenummern, die Sie zur Aktualisierung des Speichers dieser Appliances benötigen.

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

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

Das Upgrade der Software-Version 6.x auf 7.x ist nahtlos und erfordert einige manuelle Schritte. Diese Schritte müssen jedoch vor dem Start abgeschlossen sein:

1. Vergewissern Sie sich, dass in Ihrer aktuellen Konfiguration keine **Kabelkanäle** oder **ausgehende/angewendete** Befehle vorhanden sind. Diese Befehle werden in 7.x nicht mehr unterstützt, und sie werden beim Upgrade entfernt. Verwenden Sie das Tool Conduit Converter, um diese Befehle in Zugriffslisten zu konvertieren, bevor Sie das Upgrade durchführen.
2. Stellen Sie sicher, dass PIX keine PPTP-Verbindungen (Point to Point Tunneling Protocol) terminiert. Die Softwareversion 7.x unterstützt derzeit keine PPTP-Terminierung.
3. Kopieren Sie alle digitalen Zertifikate für VPN-Verbindungen auf dem PIX, bevor Sie mit dem Upgrade-Prozess beginnen.
4. Lesen Sie diese Dokumente, um sicherzustellen, dass Sie über neue, geänderte und veraltete Befehle informiert sind:Versionshinweise für die Softwareversion, auf die Sie ein Upgrade planen, finden Sie unter "Versionshinweise zur Cisco PIX Security Appliance".Leitfaden für Benutzer von Cisco PIX 6.2 und 6.3: Upgrade auf Cisco PIX Software Version 7.0
5. Planen Sie die Migration während Ausfallzeiten. Die Migration ist zwar ein einfacher zweistufiger Prozess, aber das Upgrade der PIX Security Appliance auf 7.x ist eine große Änderung, die einige Ausfallzeiten erfordert.
6. Laden Sie die Software 7.x von Cisco Downloads herunter (nur registrierte Kunden).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Security Appliances der Serie ASA 5500
- PIX Security Appliance 515, 515E, 525 und 535
- PIX Softwareversionen 6.3, 7.0

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

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

Manuelle Konfigurationsumwandlung

Bei der manuellen Konvertierung verwenden Sie einen Texteditor, um die Konfiguration Zeile für Zeile durchzuführen und PIX-spezifische Befehle in ASA-Befehle zu konvertieren.

Die manuelle Konvertierung der PIX-Konfiguration in eine ASA-Konfiguration bietet Ihnen die

größte Kontrolle über den Konvertierungsprozess. Der Vorgang ist jedoch zeitaufwendig und nicht gut skalierbar, wenn Sie mehrere Konvertierungen vornehmen müssen.

Diese drei Schritte müssen ausgeführt werden, um von PIX auf ASA zu migrieren:

1. Aktualisieren Sie die PIX-Softwareversion auf 7.x.
2. Konvertieren von Schnittstellennamen der Cisco PIX-Software 7.0 in das Cisco ASA-Format
3. Kopieren Sie die PIX Software 7.0-Konfiguration auf die Cisco ASA 5500.

Upgrade der PIX-Softwareversion auf 7.x

Führen Sie die folgenden Schritte aus, bevor Sie das eigentliche Upgrade starten:

1. Geben Sie den Befehl **show running-config** oder **write net** ein, um die aktuelle PIX-Konfiguration in einer Textdatei oder einem TFTP-Server zu speichern.
2. Geben Sie den Befehl **show version** ein, um die Anforderungen (z. B. RAM) zu überprüfen. Speichern Sie außerdem die Ausgabe dieses Befehls in einer Textdatei. Wenn Sie zu einer älteren Version des Codes zurückkehren müssen, benötigen Sie möglicherweise den ursprünglichen Aktivierungsschlüssel.

Wenn das PIX über eine BIOS-Version (Basic Input Output System) vor 4.2 verfügt oder ein PIX 515 oder PIX 535 mit bereits installiertem PDM aktualisiert werden soll, müssen Sie das Upgrade im Überwachungsmodus durchführen, anstatt mit der **copy tftp flash-**Methode. Um die BIOS-Version anzuzeigen, starten Sie das PIX neu, und lesen Sie die Meldungen beim Start, wenn ein Konsolenkabel angeschlossen ist.

Die BIOS-Version wird in einer Meldung aufgeführt, z. B.:

```
Rebooting....


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

Hinweis: Die 6.x-Befehle werden während des Upgrades automatisch in 7.x-Befehle konvertiert. Die automatische Konvertierung von Befehlen führt zu einer Änderung der Konfiguration. Sie müssen die Konfigurationsänderungen nach dem Booten der 7.x-Software überprüfen, um sicherzustellen, dass die automatischen Änderungen zufriedenstellend sind. Speichern Sie dann die Konfiguration im Flash-Speicher, um sicherzustellen, dass die Konfiguration beim nächsten Booten der Sicherheitslösung nicht erneut konvertiert wird.

Hinweis: Nachdem das System auf 7.x aktualisiert wurde, ist es wichtig, dass Sie das Festplattendienstprogramm der Softwareversion 6.x (z. B. Kennwortwiederherstellung) nicht verwenden, da es das 7.x-Software-Image beschädigt und Sie dazu verpflichtet, Ihr System vom Überwachungsmodus aus neu zu starten. Es kann auch dazu führen, dass Sie Ihre vorherige Konfiguration, Ihren Sicherheitskernel und Ihre Schlüsselinformationen verlieren.

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...

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: Geben Sie den Befehl **show version** ein, um zu überprüfen, ob das PIX jetzt die 7.x-Softwareversion ausführt.

Hinweis: Führen Sie den Befehl **show startup-config errors aus**, um alle Fehler zu überprüfen, die während der Migration der Konfiguration aufgetreten sind. Die Fehler werden in dieser Ausgabe angezeigt, nachdem Sie das PIX zum ersten Mal gestartet haben.

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 verwenden, um auf den Konsolenport des PIX zuzugreifen, müssen Sie **Strg++** drücken (Steuerung + rechte Halterung), um zur Telnet-Eingabeaufforderung zu gelangen. Geben Sie dann den Befehl **send break** aus.
4. Die Eingabeaufforderung `Monitor>` wird angezeigt.
5. Fahren Sie mit dem *Abschnitt PIX vom Überwachungsmodus-Upgrade fort*.

PIX aus Überwachungsmodus aktualisieren

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

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, lesen Sie Enter Monitor Mode.**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-Einheit 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 den TFTP-Server 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. Notieren 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. Führen Sie dieses Mal den Befehl **copy tftp flash aus**.Dadurch wird das Bild im Flash-Dateisystem gespeichert. Wenn dieser Schritt nicht abgeschlossen wird, wird beim nächsten Neustart des PIX eine Bootschleife 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#
```

Konvertieren von Schnittstellennamen der Cisco PIX Software 7.0 in das Cisco ASA-Format

Im nächsten Schritt wird die neu konvertierte Cisco PIX Software 7.0-basierte Konfiguration offline bearbeitet.

Da sich die Namenskonvention für die Cisco ASA-Schnittstelle von der der Cisco PIX Security Appliances unterscheidet, müssen Sie Änderungen an der Cisco PIX-Konfiguration vornehmen, bevor Sie diese auf die Cisco Security Appliance der Serie ASA 5500 kopieren bzw. hochladen.

Führen Sie die folgenden Schritte aus, um Änderungen an den Schnittstellennamen in der PIX-Konfiguration vorzunehmen:

1. Kopieren Sie die neue Cisco PIX Software 7.0-basierte Konfiguration offline. Laden Sie dazu die Konfiguration auf einen TFTP/FTP-Server hoch, oder kopieren Sie die Konfiguration aus einer Konsolensitzung in einen Text-Editor.Führen Sie folgenden Befehl aus, um die PIX-Konfiguration von der Konsole auf einen TFTP/FTP-Server hochzuladen:
   ```
   copy startupâˆ’config tftp://n.n.n.n/PIX7cfg.txt
       or
   copy startupâˆ’config ftp://n.n.n.n/PIX7cfg.txt
   ```

2. Wenn die auf Cisco PIX Software 7.0 basierende Konfigurationsdatei erfolgreich auf den TFTP/FTP-Server hochgeladen wurde (oder in einen Text-Editor eingefügt/kopiert wurde), öffnen Sie den Editor/WordPad oder einen beliebigen bevorzugten Text-Editor, um die Schnittstellennamen in der PIX-Konfiguration zu ändern.Die Nummernschnittstellen der

Cisco PIX Security Appliances von 0 bis n. Die Cisco Security Appliances der Serie ASA 5500 verfügen über Nummernschnittstellen je nach Standort/Steckplatz. Eingebettete Schnittstellen sind von 0/0 bis 0/3 nummeriert, und die Management-Schnittstelle ist **Management 0/0**. Die Schnittstellen des 4GE SSM-Moduls sind zwischen 1/0 und 1/3 nummeriert.Die Cisco ASA 5510 mit einer Basislizenz für 7.0 verfügt über drei Fast Ethernet-Ports (0/0 bis 0/2) sowie über eine verfügbare Management 0/0-Schnittstelle. Die Cisco ASA 5510 mit Security Plus-Lizenz verfügt über alle fünf Fast Ethernet-Schnittstellen. Die Cisco ASA 5520 und 5540 verfügen über vier Gigabit Ethernet-Ports und einen Fast Ethernet-Management-Port. Die Cisco ASA 5550 verfügt über acht Gigabit Ethernet-Ports und einen Fast Ethernet-Port.Ändern Sie die Schnittstellennamen in der PIX-Konfiguration in das ASA-Schnittstellenformat.**Beispiel:**

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

Weitere Informationen finden Sie im Abschnitt "Konfigurieren von Schnittstellenparametern" im Cisco Security Appliance Command Line Configuration Guide, Version 7.0.

Kopieren der Konfiguration von PIX auf ASA

Zu diesem Zeitpunkt verfügen Sie über eine Konfiguration auf Basis der Cisco PIX Software 7.0, bei der die geänderten Schnittstellennamen kopiert oder in die Cisco Serie ASA 5500 hochgeladen werden können. Es gibt zwei Möglichkeiten, die auf Cisco PIX Software 7.0 basierende Konfiguration auf die Appliance der Cisco Serie ASA 5500 zu laden.

Führen Sie die Schritte in Methode 1 aus: Manuelles Kopieren/Einfügen oder Methode 2: Download über TFTP/FTP.

Methode 1: Manuelles Kopieren/Einfügen

Kopieren Sie die Konfiguration über die Copy/Paste-Methode der PIX-Konsole:

1. Melden Sie sich über die Konsole bei der Cisco Serie ASA 5500 an, und geben Sie den Befehl **clear config all** aus, um die Konfiguration zu löschen, bevor Sie die geänderte Konfiguration der Cisco PIX Software 7.0 einfügen.
   ```
   ASA#config t
   ASA(config)#clear config all
   ```

2. Kopieren Sie die Konfiguration, fügen Sie sie in die ASA-Konsole ein, und speichern Sie die Konfiguration.**Hinweis:** Vergewissern Sie sich, dass alle Schnittstellen vor dem Testen im `Zustand "Kein Herunterfahren"` sind.

Methode 2: Von TFTP/FTP herunterladen

Die zweite Methode besteht darin, die Cisco PIX Software 7.0-basierte Konfiguration von einem TFTP/FTP-Server herunterzuladen. Für diesen Schritt müssen Sie die Verwaltungsschnittstelle auf der Appliance der Cisco Serie ASA 5500 für den TFTP/FTP-Download konfigurieren:

1. Führen Sie folgende Schritte in der ASA-Konsole aus:

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

Hinweis: (Optional) `Routenmanagement <ip> <mask> <next-hop>`

2. Sobald die Management-Schnittstelle eingerichtet ist, können Sie die PIX-Konfiguration auf die ASA herunterladen:
```
ASA(Config)#copy tftp://
```

3. Speichern Sie die Konfiguration.

Wenden Sie die Konfiguration der PIX Software Version 6.x auf die ASA Software Version 7.x an.

Die Umwandlung einer PIX 6.2- oder 6.3-Konfiguration in eine neue ASA Security Appliance ist ein manueller Prozess. Der ASA/PIX-Administrator muss die PIX 6.x-Syntax entsprechend der ASA-Syntax konvertieren und die Befehle in die ASA-Konfiguration eingeben. Sie können einige Befehle ausschneiden und einfügen, z. B. den Befehl **access-list**. Vergleichen Sie unbedingt die PIX 6.2- oder 6.3-Konfiguration genau mit der neuen ASA-Konfiguration, um sicherzustellen, dass bei der Konvertierung keine Fehler auftreten.

Hinweis: Der Cisco CLI Analyzer (nur registrierte Kunden) kann verwendet werden, um einige der älteren, nicht unterstützten Befehle, wie **Anwendung**, **ausgehender** oder Kanal, in die entsprechende Zugriffsliste **umzuwandeln**. Die umgewandelten Aussagen müssen gründlich überprüft werden. Es muss überprüft werden, ob die Konvertierung mit den Sicherheitsrichtlinien übereinstimmt.

Hinweis: Der Prozess für das Upgrade auf eine neue ASA-Appliance unterscheidet sich von einem Upgrade auf eine neue PIX-Appliance. Beim Versuch, ein Upgrade auf eine ASA mit dem PIX-Prozess durchzuführen, werden eine Reihe von Konfigurationsfehlern auf der ASA ausgelöst.

Fehlerbehebung - Manuelle Konfigurationsumwandlung

Gerät in Reboot-Schleife stecken

- 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.

- Wenn das PIX 7.x ausgeführt und neu gestartet wird, 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...
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
```

Wenn das PIX vom Überwachungsmodus auf 7.0 aktualisiert wird, das 7.0-Image jedoch nach dem ersten Start von 7.0 nicht erneut in Flash kopiert wird, 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.

Fehlermeldung

Beim Upgrade mit der **copy tftp flash** method wird die folgende Fehlermeldung angezeigt:

```
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#
```

Diese Meldung wird normalerweise angezeigt, wenn das PIX 515 oder ein PIX 535 mit bereits installiertem PDM mit der **copy tftp flash-**Methode aktualisiert wird.

Führen Sie ein Upgrade mit der Monitor Mode-Methode durch, um dieses Problem zu beheben.

Konfiguration scheint nicht korrekt zu sein.

Nachdem Sie das PIX von 6.x auf 7.x aktualisiert haben, werden einige Konfigurationen nicht ordnungsgemäß migriert.

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 angezeigt, nachdem Sie das PIX zum ersten Mal gestartet haben. Untersuchen Sie diese Fehler, und versuchen Sie, sie zu beheben.

Einige Dienste wie FTP funktionieren nicht.

Gelegentlich funktionieren einige Dienste wie FTP nach einem Upgrade nicht.

Die Überprüfung für diese Services ist nach dem Upgrade nicht aktiviert. Aktivieren Sie die Prüfung für die entsprechenden Services. Fügen Sie sie dazu der Standard-/globalen Prüfrichtlinie hinzu, oder erstellen Sie eine separate Prüfrichtlinie für den gewünschten Dienst.

Weitere Informationen zu den Prüfungsrichtlinien finden Sie im Abschnitt "Anwenden der Anwendungs-Layer-Protokollüberprüfung" im Cisco Security Appliance Command Line Configuration Guide, Version 7.0.

Kein Internetzugriff, wenn die Cisco PIX Security Appliance durch die Cisco Adaptive Security Appliance (ASA) ersetzt wurde

Wenn Sie nach dem Austausch der Cisco PIX Security Appliance durch die Cisco Adaptive Security Appliance (ASA) nicht mehr auf das Internet zugreifen können, verwenden Sie diesen Abschnitt.

Wenn Sie den PIX aus dem Netzwerk entfernen und die ASA mit einer externen Schnittstellen-IP-Adresse, die mit der **externen Schnittstelle des PIX** identisch ist, an das Netzwerk anschließen, verfügt der Upstream-Router weiterhin über die **MAC-Adresse** für das PIX, die der **IP-Adresse** der **externen Schnittstelle entspricht**. Daher kann es die Antwortpakete nicht an die ASA zurücksenden. Damit die ASA funktioniert, müssen Sie den **ARP-**Eintrag auf dem Upstream-Router löschen, damit er den neuen/korrekten MAC-Adresseintrag erhält. Wenn Sie die ARP-Einträge leeren, wenn Sie planen, den PIX durch ASA zu ersetzen, wird das Problem der Internetverbindung behoben. Der ARP-Eintrag muss vom ISP am Ende gelöscht werden.

Zugehörige Informationen

- Cisco PIX Security Appliances der Serie 500 - Einführung
- Technischer Support und Dokumentation - Cisco Systems