Migrazione dalle appliance di sicurezza PIX serie 500 alle appliance di sicurezza adattive ASA serie 5500

Sommario

Introduzione

Questo documento spiega come eseguire la migrazione da PIX serie 500 Security Appliance ad ASA serie 5500 Adaptive Security Appliance.

Nota: i PIX 501, PIX 506 e PIX 506E non supportano la versione 7 del software.

Per convertire una configurazione PIX in una configurazione ASA, è possibile procedere in due modi:

- Conversione assistita da strumenti
- Conversione manuale

Conversione automatica basata su strumenti/assistita da strumenti

Cisco consiglia di usare la conversione assistita da strumento per convertire le configurazioni PIX

in configurazioni ASA.

Il metodo di conversione basato su strumenti è più rapido e scalabile se si eseguono conversioni multiple. Tuttavia, l'output del processo in una configurazione intermedia contiene sia la sintassi precedente che quella nuova. Per completare la conversione, è necessario installare la configurazione intermedia sull'accessorio di protezione adattiva di destinazione. Finché non viene installato sul dispositivo di destinazione, non è possibile visualizzare la configurazione finale.

Nota: Cisco ha rilasciato lo strumento di migrazione da PIX ad ASA per automatizzare il processo di migrazione alle nuove appliance ASA. Questo strumento può essere scaricato dal sito di download del software PIX. Per ulteriori informazioni, fare riferimento a Migrazione della configurazione di un'appliance di sicurezza PIX serie 500 ad ASA serie 5500 Adaptive Security Appliance.

Prerequisiti

Requisiti hardware e software

Èpossibile aggiornare PIX 515, 515E, 525, 535 alla versione 7.0.

Prima di avviare il processo di aggiornamento alla versione 7.x, Cisco consiglia di eseguire PIX versione 6.2 o successive. Ciò garantisce che la configurazione corrente venga convertita correttamente. Inoltre, per i requisiti RAM minimi è necessario soddisfare i seguenti requisiti hardware:

Modello PIX	Requisiti RAM	
	Con restrizioni (R)	Senza restrizioni (URL) / Solo failover (FO)
PIX-515	64 MB*	128 MB*
PIX-515E	64 MB*	128 MB*
PIX-525	128 MB	256 MB
PIX-535	512 MB	1 GB

Usare il comando **show version** per determinare la quantità di RAM attualmente installata sul PIX.

Nota: anche gli aggiornamenti dei software PIX 515 e 515E possono richiedere un aggiornamento della memoria:

- I dispositivi con licenze limitate e 32 MB di memoria devono essere aggiornati a 64 MB.
- I dispositivi con licenze senza restrizioni e 64 MB di memoria devono essere aggiornati a 128 MB.

Per aggiornare la memoria di questi accessori, vedere la tabella dei numeri di parte necessari.

Configurazione accessorio corrente		Aggiorna soluzione	
Licenza per piattaforma	Memoria totale (prima dell'aggiornamento)	Codice prodotto	Memoria totale (dopo l'aggiornamento)
Con restrizioni (R)	32 MB	PIX-515-MEM-32	64 MB
Senza restrizioni (UR)	32 MB	PIX-515-MEM-128	128 MB
Solo failover (FO)	64 MB	PIX-515-MEM-128	128 MB

Nota: il numero di parte dipende dalla licenza installata sul PIX.

L'aggiornamento del software dalla versione 6.x alla versione 7.x è semplice e richiede alcune operazioni manuali, ma prima di iniziare è necessario completare i seguenti passaggi:

1. Accertarsi di non avere comandi **conduit** o **outbound/apply** nella configurazione corrente. Questi comandi non sono più supportati in 7.x e vengono rimossi dal processo di aggiornamento. Usare lo strumento Conduci Converter per convertire questi comandi in elenchi degli accessi prima di tentare l'aggiornamento.
2. Verificare che PIX non interrompa le connessioni PPTP (Point to Point Tunneling Protocol). Il software versione 7.x non supporta la terminazione PPTP.
3. Copiare tutti i certificati digitali per le connessioni VPN sul PIX prima di avviare il processo di aggiornamento.
4. Leggere questi documenti per essere certi di conoscere i comandi nuovi, modificati e deprecati:Note sulla versione del software a cui si intende aggiornare il software, disponibili in "Cisco PIX Security Appliance Release Notes".Guida per gli utenti di Cisco PIX 6.2 e 6.3 Aggiornamento al software Cisco PIX versione 7.0
5. Pianificare l'esecuzione della migrazione durante i tempi di inattività. Sebbene la migrazione sia un semplice processo in due fasi, l'aggiornamento di PIX Security Appliance alla versione 7.x è una modifica importante e richiede tempi di inattività.
6. Scaricare il software 7.x da Cisco Downloads (solo utenti registrati).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA serie 5500 Security Appliance
- PIX Security Appliance 515, 515E, 525 e 535
- Software PIX versioni 6.3, 7.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Conversione manuale della configurazione

Con il processo di conversione manuale, è possibile usare un editor di testo per esaminare la configurazione riga per riga e convertire i comandi specifici del PIX in comandi ASA.

La conversione manuale della configurazione PIX in una configurazione ASA offre il massimo controllo sul processo di conversione. Tuttavia, il processo richiede tempo e non è scalabile correttamente se è necessario eseguire più di una conversione.

Per migrare da PIX ad ASA, è necessario completare i seguenti tre passaggi:

1. Aggiornare la versione del software PIX a 7.x.
2. Convertire i nomi delle interfacce dal software Cisco PIX 7.0 al formato Cisco ASA.
3. Copiare la configurazione del software PIX 7.0 su Cisco ASA 5500.

Aggiornamento della versione del software PIX alla 7.x

Prima di avviare il processo di aggiornamento effettivo, effettuare le seguenti operazioni:

1. Usare il comando **show running-config** o **write net** per salvare la configurazione corrente del PIX in un file di testo o in un server TFTP.
2. Usare il comando **show version** per verificare i requisiti, ad esempio la RAM. Salvare inoltre l'output di questo comando in un file di testo. Se è necessario ripristinare una versione precedente del codice, è possibile che sia necessaria la chiave di attivazione originale.

Se il PIX ha una versione del BIOS (Basic Input Output System) precedente alla 4.2 o se si intende aggiornare un PIX 515 o un PIX 535 con un PDM già installato, è necessario completare la procedura di aggiornamento in modalità Monitor invece che con il metodo **copy tftp flash**. Per visualizzare la versione del BIOS, riavviare il PIX e, con un cavo console collegato, leggere i messaggi all'avvio.

La versione del BIOS è elencata in un messaggio, ad esempio:

```
Rebooting....


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

Nota: i comandi 6.x vengono convertiti automaticamente in comandi 7.x durante l'aggiornamento. La conversione automatica dei comandi determina una modifica della configurazione. Dopo l'avvio del software 7.x è necessario rivedere le modifiche alla configurazione per verificare che le modifiche automatiche siano soddisfacenti. Quindi, salvare la configurazione nella memoria flash in modo che non venga convertita nuovamente al successivo avvio dell'appliance di sicurezza.

Nota: dopo l'aggiornamento del sistema alla versione 7.x, è importante non utilizzare l'utilità disco np versione 6.x, ad esempio il recupero della password, poiché danneggia l'immagine del software 7.x e richiede il riavvio del sistema dalla modalità Monitor. Ciò può inoltre causare la perdita della configurazione precedente, del kernel di sicurezza e delle informazioni principali.

Aggiornare PIX Security Appliance con il comando copy tftp flash

Completare questa procedura per aggiornare il PIX con il comando **copy tftp flash**.

1. Copiare l'immagine binaria dell'accessorio PIX, ad esempio pix701.bin, nella directory principale del server TFTP.
2. Dal prompt di abilitazione, usare il comando **copy tftp flash**.

```
pixfirewall>enable
Password:

pixfirewall#copy tftp flash
```

3. Immettere l'indirizzo IP del server TFTP.
   ```
   Address or name of remote host [0.0.0.0]?
   ```
4. Immettere il nome del file sul server TFTP che si desidera caricare. Nome del file di immagine binario PIX.
   ```
   Source file name [cdisk]?
   ```
5. Quando viene richiesto di avviare la copia TFTP, digitare **yes**.
   ```
   copying tftp://172.18.173.123/pix701.bin to flash:image
   [yes|no|again]?yes
   ```
6. L'immagine viene ora copiata dal server TFTP a Flash.Questo messaggio viene visualizzato e indica che il trasferimento è riuscito, che la vecchia immagine binaria in Flash viene cancellata e che la nuova immagine viene scritta e installata.
   ```
   !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   Received 5124096 bytes
   Erasing current image
   Writing 5066808 bytes of image
   !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   Image installed
   pixfirewall#
   ```
7. Ricaricare l'accessorio PIX per avviare la nuova immagine.
   ```
   pixfirewall#reload
   Proceed with reload? [confirm]



   Rebooting....
   ```
8. Il PIX ora avvia l'immagine 7.0 e questo completa il processo di aggiornamento.

Configurazione di esempio - Aggiornare l'accessorio PIX con il comando copy tftp flash

```
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>
```

Nota: utilizzare il comando **show version** per verificare che sul PIX sia in esecuzione la versione software 7.x.

Nota: per esaminare gli eventuali errori verificatisi durante la migrazione della configurazione,

usare il comando **show startup-config errors**. Gli errori vengono visualizzati in questo output dopo il primo avvio di PIX.

Aggiornamento di PIX Security Appliance dalla modalità Monitor

Accedere alla modalità Monitor

Completare questa procedura per accedere alla modalità Monitor sul PIX.

1. Collegare un cavo console alla porta console sul PIX utilizzando queste impostazioni di comunicazione:9600 bit al secondo8 bit di datinessuna parità1 bit di stopnessun controllo del flusso
2. Spegnere e riaccendere il PIX. Durante l'avvio viene richiesto di utilizzare BREAK o ESC per interrompere l'avvio di Flash. Sono necessari dieci secondi per interrompere il normale processo di avvio.
3. Per accedere alla modalità Monitor, premere **ESC** o inviare un carattere **BREAK**.Se si utilizza Windows Hyper Terminal, è possibile premere **Esc** o **Ctrl+Break** per inviare un carattere di interruzione.Se si utilizza Telnet tramite un Terminal Server per accedere alla porta console del PIX, è necessario premere **Ctrl+]** (Ctrl + parentesi destra) per accedere al prompt dei comandi Telnet. Eseguire quindi il comando **send break**.
4. Viene visualizzato il prompt `monitor>`.
5. Procedere alla sezione *Aggiornamento del PIX dalla modalità monitor*.

Aggiornamento del PIX dalla modalità Monitor

Completare questi passaggi per aggiornare PIX dalla modalità Monitor.

1. Copiare l'immagine binaria dell'accessorio PIX, ad esempio pix701.bin, nella directory principale del server TFTP.
2. Accedere alla modalità Monitor sul PIX. Se non si è certi della procedura da seguire, vedere Accedere alla modalità Monitor.**Nota:** in modalità Monitor è possibile utilizzare il punto interrogativo "?" per visualizzare un elenco delle opzioni disponibili.
3. Immettere il numero di interfaccia a cui è connesso il server TFTP o l'interfaccia più vicina al server TFTP. Il valore predefinito è interface 1 (Inside).
   ```
   monitor>interface
   ```

   Nota: in modalità monitor, l'interfaccia esegue sempre la negoziazione automatica della velocità e del duplex. Le impostazioni dell'interfaccia non possono essere hardcoded. Pertanto, se l'interfaccia PIX è collegata a uno switch hardcoded per velocità/duplex, riconfigurarla per la negoziazione automatica mentre è in modalità monitor. Tenere inoltre presente che l'accessorio PIX non è in grado di inizializzare un'interfaccia Gigabit Ethernet dalla modalità Monitor. In alternativa, è necessario utilizzare un'interfaccia Fast Ethernet.
4. Immettere l'indirizzo IP dell'interfaccia definita nel passaggio tre.
   ```
   monitor>address
   ```

5. Immettere l'indirizzo IP del server TFTP.
   ```
   monitor>server
   ```

6. (Facoltativo) Immettere l'indirizzo IP del gateway. È necessario un indirizzo gateway se l'interfaccia del PIX non si trova sulla stessa rete del server TFTP.
   ```
   monitor>gateway
   ```

7. Immettere il nome del file sul server TFTP che si desidera caricare. Nome del file di immagine binario PIX.
   ```
   monitor>file
   ```

8. Eseguire il ping tra il PIX e il server TFTP per verificare la connettività IP.Se i ping hanno esito negativo, controllare i cavi, l'indirizzo IP dell'interfaccia PIX e del server TFTP e l'indirizzo IP del gateway (se necessario). I ping devono avere esito positivo prima di continuare.
   ```
   monitor>ping
   ```

9. Digitare **tftp** per avviare il download del TFTP.
   ```
   monitor>tftp
   ```

10. Il PIX scarica l'immagine nella RAM e la avvia automaticamente.Durante il processo di avvio, il file system viene convertito insieme alla configurazione corrente. Tuttavia, non hai ancora finito. Notare questo messaggio di avviso dopo l'avvio e continuare con il passaggio 11:
    ```
    ************************************************************
      **                                                        **
      **   *** 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. Una volta avviato, accedere alla modalità di abilitazione e copiare nuovamente la stessa immagine sul PIX. Questa volta, usare il comando **copy tftp flash**.L'immagine viene salvata nel file system Flash. Se questa operazione non viene completata, al successivo caricamento del PIX verrà eseguito un ciclo di avvio.

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

Nota: per istruzioni dettagliate su come copiare l'immagine con il comando **copy tftp flash**, consultare la sezione Aggiornamento dell'appliance di sicurezza PIX con il comando copy tftp flash.

12. Una volta copiata l'immagine con il comando **copy tftp flash**, il processo di aggiornamento è completato.**Configurazione di esempio - Aggiornamento di PIX Security Appliance dalla modalità di monitoraggio**

```
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#
```

Conversione dei nomi di interfaccia dal software Cisco PIX 7.0 al formato Cisco ASA

Il passaggio successivo del processo è la modifica offline della configurazione basata su Cisco PIX Software 7.0 appena convertita.

Poiché la convenzione di denominazione dell'interfaccia Cisco ASA è diversa da quella delle appliance di sicurezza Cisco PIX, è necessario modificare la configurazione di Cisco PIX prima di copiarla/caricarla sull'appliance di sicurezza Cisco ASA serie 5500.

Completare questa procedura per apportare le modifiche al nome dell'interfaccia sulla configurazione PIX:

1. Copiare la nuova configurazione basata su Cisco PIX Software 7.0 offline. A tal fine, caricare la configurazione su un server TFTP/FTP o copiare la configurazione da una sessione della console a un editor di testo.Per caricare la configurazione PIX su un server TFTP/FTP, dalla console, usare questo comando:
```
copy startupâ^'config tftp://n.n.n.n/PIX7cfg.txt
    or
copy startupâ^'config ftp://n.n.n.n/PIX7cfg.txt
```

2. Una volta che il file di configurazione basato su Cisco PIX Software 7.0 è stato caricato correttamente sul server TFTP/FTP (o è stato incollato/copiato su un editor di testo), aprire Blocco note/WordPad o un editor di testo preferito per modificare i nomi delle interfacce nella configurazione PIX.Cisco PIX Security Appliance numera le interfacce da 0 a n. Le appliance di sicurezza Cisco ASA serie 5500 numerano le interfacce in base alla posizione/slot. Le interfacce incorporate sono numerate da 0/0 a 0/3 e l'interfaccia di gestione è **Management 0/0**. Le interfacce sul modulo SSM 4GE sono numerate da 1/0 a 1/3.Cisco ASA 5510 con una licenza base con versione 7.0 ha tre porte Fast Ethernet (da 0/0 a 0/2) più l'interfaccia di gestione 0/0 disponibile. Cisco ASA 5510 con licenza Security Plus ha tutte e cinque le interfacce Fast Ethernet disponibili. Cisco ASA 5520 e 5540 hanno quattro porte Gigabit Ethernet e una porta di gestione Fast Ethernet. Cisco ASA 5550 ha otto porte Gigabit Ethernet e una porta Fast Ethernet.Modificare i nomi delle interfacce nella configurazione PIX nel formato di interfaccia ASA.**Ad esempio:**

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

Per ulteriori informazioni, consultare la sezione "Configuring Interface Parameters" della guida alla configurazione della riga di comando di Cisco Security Appliance, versione 7.0.

Copia della configurazione da PIX ad ASA

A questo punto, la configurazione basata su Cisco PIX Software 7.0 è stata modificata e i nomi delle interfacce sono pronti per essere copiati o caricati su Cisco ASA serie 5500. Esistono due modi per caricare la configurazione basata su Cisco PIX Software 7.0 sull'appliance Cisco ASA serie 5500.

Completare la procedura descritta in Metodo 1: Copia/Incolla manuale o Metodo 2: Scarica da TFTP/FTP.

Metodo 1: Copia/Incolla manuale

Copiare la configurazione dalla console PIX con il metodo copy/paste:

1. Accedere alla Cisco ASA serie 5500 dalla console e usare il comando **clear config all** per cancellare la configurazione prima di incollare la configurazione modificata del software Cisco PIX 7.0.
```
ASA#config t
ASA(config)#clear config all
```

2. Copiare e incollare la configurazione sulla console ASA e salvare la configurazione.**Nota:** verificare che tutte le interfacce siano nello stato `no shutdown` prima di iniziare il test.

Metodo 2: Scarica da TFTP/FTP

Il secondo metodo consiste nel scaricare la configurazione basata su Cisco PIX Software 7.0 da un server TFTP/FTP. Per eseguire questo passaggio, è necessario configurare l'interfaccia di gestione sull'accessorio Cisco ASA serie 5500 per il download di TFTP/FTP:

1. Dalla console ASA, usare il comando seguente:
```
ASA#config t
ASA(config)#interface management 0
ASA(config)#nameif management
ASA(config)#ip add
```

Nota: (facoltativo) `gestione route <ip> <mask> <hop successivo>`

2. Dopo aver configurato l'interfaccia di gestione, è possibile scaricare la configurazione PIX sull'appliance ASA:
```
ASA(Config)#copy tftp://
```

3. Salvare la configurazione.

Applicazione di una configurazione software PIX versione 6.x al software ASA versione 7.x

La conversione di una configurazione PIX 6.2 o 6.3 in una nuova appliance ASA Security è un processo manuale. L'amministratore ASA/PIX deve convertire la sintassi PIX 6.x in modo che corrisponda alla sintassi ASA e digitare i comandi nella configurazione ASA. È possibile tagliare e incollare alcuni comandi, ad esempio **access-list**. Accertarsi di confrontare attentamente la configurazione PIX 6.2 o 6.3 con la nuova configurazione ASA in modo da evitare errori durante la conversione.

Nota: Cisco CLI Analyzer (solo utenti registrati) può essere usato per convertire alcuni dei comandi meno recenti non supportati, come **apply**, **outbound** o **conduit** nell'elenco degli accessi appropriato. Le dichiarazioni convertite devono essere riviste in modo approfondito. È necessario verificare che la conversione corrisponda ai criteri di protezione.

Nota: il processo di aggiornamento a un nuovo accessorio ASA è diverso da quello di un aggiornamento a un nuovo accessorio PIX. Il tentativo di eseguire l'aggiornamento a un'ASA con il processo PIX genera una serie di errori di configurazione sull'ASA.

Risoluzione dei problemi - Conversione manuale della configurazione

Periferica bloccata nel ciclo di riavvio

- Dopo aver usato il metodo **copy tftp flash** per aggiornare il PIX e il riavvio, si blocca in questo ciclo di riavvio:

```
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.
```

  Gli accessori PIX con versioni BIOS precedenti alla 4.2 non possono essere aggiornati con il comando **copy tftp flash**. È necessario aggiornarli con il metodo Modalità monitor.
- Una volta eseguita la versione 7.x del PIX e riavviato, il PIX rimane bloccato nel seguente ciclo di riavvio:

```
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
```

Se il PIX viene aggiornato dalla modalità Monitor alla versione 7.0, ma l'immagine 7.0 non viene copiata nuovamente nella memoria flash dopo il primo avvio di 7.0, quando il PIX viene ricaricato, si blocca in un ciclo di riavvio.La risoluzione consiste nel caricare nuovamente l'immagine dalla modalità Monitor. Una volta avviato, è necessario copiare di nuovo l'immagine utilizzando il metodo **copy tftp flash**.

Messaggio di errore

Quando si esegue l'aggiornamento con il metodo **copy tftp flash**, viene visualizzato questo messaggio di errore:

```
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#
```

Questo messaggio viene in genere visualizzato quando un PIX 515 o un PIX 535 con PDM già installato viene aggiornato con il metodo **flash copy tftp**.

Per risolvere il problema, eseguire l'aggiornamento con il metodo Modalità monitor.

Configurazione non corretta

Dopo l'aggiornamento di PIX da 6.x a 7.x, alcune configurazioni non vengono migrate correttamente.

L'output del comando **show startup-config errors** visualizza gli eventuali errori verificatisi durante la migrazione della configurazione. Gli errori vengono visualizzati in questo output dopo il primo avvio di PIX. Esaminare gli errori e tentare di risolverli.

Alcuni servizi, ad esempio FTP, non funzionano

Talvolta, alcuni servizi, ad esempio FTP, non funzionano dopo un aggiornamento.

L'ispezione per questi servizi non è abilitata dopo l'aggiornamento. Abilitare l'ispezione per i servizi appropriati. A tale scopo, aggiungerli ai criteri di ispezione predefiniti/globali o creare un criterio di ispezione separato per il servizio desiderato.

Per ulteriori informazioni sui criteri di ispezione, consultare la sezione "Application Layer Protocol Inspection" della guida alla configurazione della riga di comando di Cisco Security Appliance, versione 7.0.

Impossibile accedere a Internet quando Cisco PIX Security Appliance viene sostituito con Cisco Adaptive Security Appliance (ASA)

Utilizzare questa sezione se non è possibile accedere a Internet dopo aver sostituito Cisco PIX Security Appliance con Cisco Adaptive Security Appliance (ASA).

Quando si scollega il PIX dalla rete e si collega l'ASA alla rete con un indirizzo IP dell'interfaccia esterna che è lo stesso **dell'interfaccia esterna del PIX**, il router a monte ha ancora l'**indirizzo MAC** per il PIX corrispondente all'**indirizzo IP** dell'**interfaccia esterna**. Di conseguenza, non è in grado di inviare i pacchetti di risposta all'appliance ASA. Affinché l'ASA funzioni, è necessario cancellare la voce **ARP** sul router a monte in modo che apprenda la voce mac-address nuova o corretta. Se si eliminano le voci ARP quando si intende sostituire il PIX con un'ASA, il problema di connettività Internet viene risolto. Lo scaricamento della voce ARP deve essere eseguito dall'ISP alla fine di tale voce.

Informazioni correlate

- Cisco PIX serie 500 Security Appliance - Introduzione
- Documentazione e supporto tecnico – Cisco Systems