

# Aggiornamento software per PIX 500 Security Appliance da 6.x a 7.x

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Requisiti minimi di sistema](#)

[Informazioni sull'aggiornamento della memoria per gli accessori PIX 515/515E](#)

[Convenzioni](#)

[Aggiornamento di PIX Security Appliance](#)

[Download di software](#)

[Procedura di aggiornamento](#)

[Aggiornamento di PIX Security Appliance dalla modalità Monitor](#)

[Accedere alla modalità Monitor](#)

[Aggiornamento del PIX dalla modalità Monitor](#)

[Aggiornare PIX Security Appliance con il comando `copy tftp flash`](#)

[Downgrade da PIX 7.x a 6.x](#)

[Aggiornare gli accessori PIX in un set di failover](#)

[Installare Adaptive Security Device Manager \(ASDM\)](#)

[Risoluzione dei problemi](#)

[Abilita ispezione FTP](#)

[Ottieni un contratto di assistenza valido](#)

[Informazioni correlate](#)

## Introduzione

Questo documento spiega come aggiornare l'accessorio PIX dalla versione 6.2 o 6.3 alla versione 7.x. e l'installazione di Adaptive Security Device Manager (ASDM) versione 5.0.

## Prerequisiti

### Requisiti

Prima di avviare la procedura di aggiornamento, completare le seguenti attività.

- Usare il comando **show running-config** o **write net** per salvare la configurazione PIX corrente in un file di testo o in un server TFTP.
- Per visualizzare il numero di serie e la chiave di attivazione, usare il comando **show version**.

Salva questo output in un file di testo. Se è necessario ripristinare una versione precedente del codice, potrebbe essere necessaria la chiave di attivazione originale. Per ulteriori informazioni sui tasti di attivazione, consultare il documento sulle [domande frequenti relative a PIX Firewall](#).

- Accertarsi di non avere comandi **conduit** o **outbound** nella configurazione corrente. Questi comandi non sono più supportati in 7.x e vengono rimossi dal processo di aggiornamento. Usare lo strumento [Output Interpreter](#) (solo utenti [registrati](#)) per convertire questi comandi in elenchi degli accessi prima di tentare l'aggiornamento.
- Verificare che il PIX non termini le connessioni PPTP (Point to Point Tunneling Protocol). PIX 7.1 e versioni successive non supportano la terminazione PPTP.
- Se si utilizza il failover, verificare che l'interfaccia LAN o stateful non sia condivisa con i dati che passano le interfacce. Ad esempio, se si utilizza l'interfaccia interna per passare il traffico di dati e per l'interfaccia di failover stateful (collegamento di failover interno), è necessario spostare l'interfaccia di failover stateful su un'altra interfaccia prima di eseguire l'aggiornamento. In caso contrario, tutte le configurazioni legate all'interfaccia interna verranno rimosse. Inoltre, il traffico di dati non passa attraverso l'interfaccia dopo l'aggiornamento.
- Prima di procedere, accertarsi che la versione del PIX sia 6.2 o 6.3.
- Leggere le note sulla versione per la quale si intende eseguire l'aggiornamento, in modo da conoscere tutti i comandi nuovi, modificati e deprecati.
- Per ulteriori modifiche ai comandi tra la versione 6.x e la versione 7.x, consultare la [guida all'aggiornamento](#).

## [Componenti usati](#)

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

- PIX Security Appliance 515, 515E, 525 e 535
- PIX Software versioni 6.3(4), 7.0(1)

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.

## [Requisiti minimi di sistema](#)

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, questi requisiti hardware devono essere soddisfatti per i requisiti minimi di RAM e Flash:

Modello PIX	Requisiti RAM		Requisiti Flash
	Con restrizioni (R)	Senza restrizioni (URL) / Solo failover (FO)	
PIX-515	64 MB*	128 MB*	16 MB
PIX-515E	64 MB*	128 MB*	16 MB

PIX-525	128 MB	256 MB	16 MB
PIX-535	512 MB	1 GB	16 MB

\* Tutti gli accessori PIX-515 e PIX-515E richiedono un aggiornamento della memoria.

Usare il comando **show version** per determinare la quantità di RAM e di flash attualmente installata sul PIX. Non sono necessari aggiornamenti Flash, in quanto per impostazione predefinita in tutti gli accessori PIX della tabella sono installati 16 MB.

**Nota:** nella versione 7.x sono supportati solo gli accessori di sicurezza PIX riportati in questa tabella. Le versioni precedenti delle appliance di sicurezza PIX, ad esempio PIX-520, 510, 10000 e Classic, non sono più disponibili e non possono essere eseguite dalla versione 7.0 o successive. Se si dispone di uno di questi accessori e si desidera eseguire la versione 7.x o successive, contattare il team amministrativo o il rivenditore Cisco locale per acquistare una nuova appliance di sicurezza. Inoltre, i firewall PIX con meno di 64 MB di RAM (PIX-501, PIX-506 e PIX-506E) non sono in grado di eseguire la versione 7.0 iniziale.

### [Informazioni sull'aggiornamento della memoria per gli accessori PIX 515/515E](#)

Gli aggiornamenti della memoria sono richiesti solo per gli accessori PIX-515 e PIX-515E. Per aggiornare la memoria di questi accessori, vedere la tabella dei numeri di parte necessari.

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

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

Per ulteriori informazioni, consultare il [documento sull'aggiornamento della memoria di Cisco PIX 515/515E Security Appliance per il software PIX v7.0](#).

### [Convenzioni](#)

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

## [Aggiornamento di PIX Security Appliance](#)

## [Download di software](#)

Visitare il [Cisco Software Center](#) (solo utenti [registrati](#)) per scaricare il software PIX 7.x. Il software server TFTP non è più disponibile all'indirizzo Cisco.com. Tuttavia, è possibile trovare molti server TFTP quando si cerca "server tftp" sul motore di ricerca Internet preferito. Cisco non consiglia specificamente una particolare implementazione TFTP. Per ulteriori informazioni, consultare la [pagina sul server TFTP](#) (solo utenti [registrati](#)).

## [Procedura di aggiornamento](#)

Tenere presente che l'aggiornamento di PIX Security Appliance alla versione 7.x rappresenta una modifica importante. Gran parte della CLI viene modificata e quindi la configurazione dopo l'aggiornamento apparirà molto diversa. Aggiornare solo durante una finestra di manutenzione in quanto il processo di aggiornamento richiede tempi di inattività. Se è necessario ripristinare un'immagine 6.x, seguire le procedure di [downgrade](#). In caso contrario, il PIX entra in un ciclo continuo di riavvio. Per continuare, individuare nella tabella il modello di accessorio PIX e quindi selezionare il collegamento per visualizzare le istruzioni per l'aggiornamento.

Modello PIX	Metodo di aggiornamento
PIX-515	<a href="#">Monitor (Monitora)</a>
PIX-515E	<a href="#">copy tftp flash</a>
PIX-525	<a href="#">copy tftp flash</a>
PIX-535 (senza PDM installato)	<a href="#">copy tftp flash</a>
PIX-535 (PDM installato)	<a href="#">Monitor (Monitora)</a>

## [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 secondo, 8 bit di dati, nessuna parità, 1 bit di stop, nessun controllo del flusso.
2. Spegner 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. Immettere 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.

**Nota:** le schede Fast Ethernet in slot a 64 bit non sono visibili in modalità monitor. Questo problema significa che il server TFTP non può risiedere su una di queste interfacce. L'utente deve usare il comando **copy tftp flash** per scaricare il file di immagine del firewall PIX tramite TFTP.

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. In caso di dubbi, vedere le istruzioni per [accedere alla modalità Monitor](#) in questo documento.**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 presente che l'accessorio PIX non è in grado di inizializzare un'interfaccia Gigabit Ethernet dalla modalità di monitoraggio. In alternativa, è necessario utilizzare un'interfaccia Fast Ethernet.

4. Immettere l'indirizzo IP dell'interfaccia definita al passaggio 3.

```
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 *** 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 usate il comando **copy tftp flash**. L'immagine viene salvata nel file system Flash. Se questa operazione non viene eseguita, 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 completo.

## 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)
```



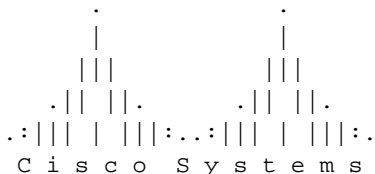
Need to burn loader....  
Erasing sector 0...[OK]  
Burning sector 0...[OK]  
Erasing sector 64...[OK]  
Burning sector 64...[OK]

Licensed features for this platform:

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

This platform has an Unrestricted (UR) license.

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



Cisco PIX Security Appliance Software Version 7.0(1)

\*\*\*\*\* Warning \*\*\*\*\*

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

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

If you require further assistance please contact us by sending email to [export@cisco.com](mailto: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#
```

## [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..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 @ 0xffff00000

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

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

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

*!--- This output indicates that the Flash file !--- system is formatted. The messages are normal.* Initializing flashfs... flashfs[7]: Checking block 0...block number was (-27642)  
flashfs[7]: erasing block 0...done. flashfs[7]: Checking block 1...block number was (-30053)  
flashfs[7]: erasing block 1...done. flashfs[7]: Checking block 2...block number was (-1220)  
flashfs[7]: erasing block 2...done. flashfs[7]: Checking block 3...block number was (-22934)  
flashfs[7]: erasing block 3...done. flashfs[7]: Checking block 4...block number was (2502)  
flashfs[7]: erasing block 4...done. flashfs[7]: Checking block 5...block number was (29877)  
flashfs[7]: erasing block 5...done. flashfs[7]: Checking block 6...block number was (-13768)  
flashfs[7]: erasing block 6...done. flashfs[7]: Checking block 7...block number was (9350)  
flashfs[7]: erasing block 7...done. flashfs[7]: Checking block 8...block number was (-18268)  
flashfs[7]: erasing block 8...done. flashfs[7]: Checking block 9...block number was (7921)  
flashfs[7]: erasing block 9...done. flashfs[7]: Checking block 10...block number was (22821)  
flashfs[7]: erasing block 10...done. flashfs[7]: Checking block 11...block number was (7787)  
flashfs[7]: erasing block 11...done. flashfs[7]: Checking block 12...block number was (15515)  
flashfs[7]: erasing block 12...done. flashfs[7]: Checking block 13...block number was (20019)  
flashfs[7]: erasing block 13...done. flashfs[7]: Checking block 14...block number was (-25094)  
flashfs[7]: erasing block 14...done. flashfs[7]: Checking block 15...block number was (-7515)  
flashfs[7]: erasing block 15...done. flashfs[7]: Checking block 16...block number was (-10699)  
flashfs[7]: erasing block 16...done. flashfs[7]: Checking block 17...block number was (6652)  
flashfs[7]: erasing block 17...done. flashfs[7]: Checking block 18...block number was (-23640)  
flashfs[7]: erasing block 18...done. flashfs[7]: Checking block 19...block number was (23698)  
flashfs[7]: erasing block 19...done. flashfs[7]: Checking block 20...block number was (-28882)  
flashfs[7]: erasing block 20...done. flashfs[7]: Checking block 21...block number was (2533)  
flashfs[7]: erasing block 21...done. flashfs[7]: Checking block 22...block number was (-966)  
flashfs[7]: erasing block 22...done. flashfs[7]: Checking block 23...block number was (-22888)  
flashfs[7]: erasing block 23...done. flashfs[7]: Checking block 24...block number was (-9762)  
flashfs[7]: erasing block 24...done. flashfs[7]: Checking block 25...block number was (9747)  
flashfs[7]: erasing block 25...done. flashfs[7]: Checking block 26...block number was (-22855)  
flashfs[7]: erasing block 26...done. flashfs[7]: Checking block 27...block number was (-32551)

```

flashfs[7]: erasing block 27...done. flashfs[7]: Checking block 28...block number was (-13355)
flashfs[7]: erasing block 28...done. flashfs[7]: Checking block 29...block number was (-29894)
flashfs[7]: erasing block 29...done. flashfs[7]: Checking block 30...block number was (-18595)
flashfs[7]: erasing block 30...done. flashfs[7]: Checking block 31...block number was (22095)
flashfs[7]: erasing block 31...done. flashfs[7]: Checking block 32...block number was (1486)
flashfs[7]: erasing block 32...done. flashfs[7]: Checking block 33...block number was (13559)
flashfs[7]: erasing block 33...done. flashfs[7]: Checking block 34...block number was (24215)
flashfs[7]: erasing block 34...done. flashfs[7]: Checking block 35...block number was (21670)
flashfs[7]: erasing block 35...done. flashfs[7]: Checking block 36...block number was (-24316)
flashfs[7]: erasing block 36...done. flashfs[7]: Checking block 37...block number was (29271)
flashfs[7]: erasing block 37...done. flashfs[7]: Checking block 125...block number was (0)
flashfs[7]: erasing block 125...done. flashfs[7]: inconsistent sector list, fileid 7,
parent_fileid 0 flashfs[7]: inconsistent sector list, fileid 12, parent_fileid 0 flashfs[7]: 5
files, 3 directories flashfs[7]: 0 orphaned files, 0 orphaned directories flashfs[7]: Total
bytes: 16128000 flashfs[7]: Bytes used: 5128192 flashfs[7]: Bytes available: 10999808
flashfs[7]: flashfs fsck took 59 seconds. flashfs[7]: Initialization complete. Saving the
configuration ! Saving a copy of old configuration as downgrade.cfg ! Saved the activation key
from the flash image Saved the default firewall mode (single) to flash Saving image file as
image.bin !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! Upgrade process complete Need
to burn loader.... Erasing sector 0...[OK] Burning sector 0...[OK] Licensed features for this
platform: Maximum Physical Interfaces : 6 Maximum VLANs : 25 Inside Hosts : Unlimited
Failover : Active/Active VPN-DES : Enabled VPN-3DES-AES : Enabled Cut-through Proxy : Enabled
Guards : Enabled URL Filtering : Enabled Security Contexts : 2 GTP/GPRS : Disabled VPN
Peers : Unlimited This platform has an Unrestricted (UR) license. Encryption hardware device :
VAC (IRE2141 with 2048KB, HW:1.0, CGXROM:1.9, FW:6.5) -----
----- . . | | ||| ||| .|| ||. .|| ||. .:|||| | |||:..:|||| | |||:.
C i s c o S y s t e m s -----
--- Cisco PIX Security Appliance Software Version 7.0(1) ***** Warning
***** This product contains cryptographic features and is subject to
United States and local country laws governing, import, export, transfer, and use. Delivery of
Cisco cryptographic products does not imply third-party authority to import, export, distribute,
or use encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with applicable laws
and regulations. If you are unable to comply with U.S. and local laws, return the enclosed items
immediately. A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/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:** con la licenza senza restrizioni, PIX 515 E può avere fino a otto VLAN e PIX 535 fino a venticinque VLAN.

## Downgrade da PIX 7.x a 6.x

PIX Security Appliance versione 7.0 e successive utilizzano un formato di file Flash diverso rispetto alle versioni PIX precedenti. Pertanto, non è possibile effettuare il downgrade da un'immagine 7.0 a un'immagine 6.x con il comando **copy tftp flash**. Usare al suo posto il comando **downgrade**. In caso contrario, il PIX si blocca in un loop di avvio.

Quando il PIX è stato originariamente aggiornato, la configurazione di avvio 6.x è stata salvata in Flash come `downgrade.cfg`. Se si esegue questa procedura di downgrade, la configurazione viene ripristinata sul dispositivo al momento del downgrade. È possibile rivedere questa configurazione prima di effettuare il downgrade quando si immette il comando **more flash:downgrade.cfg** da un prompt `enable>` in 7.0. Inoltre, se il PIX è stato aggiornato in modalità Monitor, l'immagine binaria 6.x precedente viene ancora salvata in Flash come `image_old.bin`. Per verificare l'esistenza di questa immagine, usare il comando **show flash**: Se l'immagine è presente in Flash, è possibile utilizzarla nel passaggio 1 di questa procedura anziché caricarla da un server TFTP.

Completare questi passaggi per effettuare il downgrade di PIX Security Appliance.

1. Immettere il comando **downgrade** e specificare la posizione dell'immagine in cui eseguire il downgrade.

```
pixfirewall#downgrade tftp://
```

**Nota:** se il PIX è stato aggiornato dalla modalità Monitor, la vecchia immagine binaria viene ancora salvata in Flash. Per effettuare il downgrade all'immagine, usare questo comando:

```
pixfirewall#downgrade flash:/image_old.bin
```

2. Viene visualizzato un messaggio di avvertenza che avvisa l'utente che la formattazione di Flash sta per essere eseguita. Premere **Invio** per continuare.

```
This command will reformat the flash and automatically reboot the system.  
Do you wish to continue? [confirm]
```

3. L'immagine viene copiata nella RAM e la configurazione di avvio viene copiata anche nella RAM.

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

```
Buffering startup config
```

```
All items have been buffered successfully
```

4. Viene visualizzato un secondo messaggio di avvertenza che indica che Flash inizia ora a formattare. **NON** interrompere questo processo, altrimenti Flash potrebbe danneggiarsi. Premere **Invio** per continuare con il formato.

```
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]
```



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>
```

## [Aggiornare gli accessori PIX in un set di failover](#)

L'aggiornamento da PIX Appliance 6.x a 7.x è un aggiornamento importante. Non è possibile farlo senza downtime, anche per i PIX in un set di failover. Molti comandi di failover cambiano con l'aggiornamento. Il percorso di aggiornamento consigliato consiste nello spegnere uno dei PIX nel set di failover. Quindi, seguire le istruzioni in questo documento per aggiornare il PIX acceso. Una volta completato l'aggiornamento, verificare che il traffico passi, e anche riavviare il PIX una volta per verificare che ritorni senza problemi. Una volta verificato che tutto funzioni correttamente, spegnere il PIX appena aggiornato e accendere l'altro PIX. Quindi seguire le istruzioni in questo documento per aggiornare il PIX. Al termine dell'aggiornamento, verificare che il traffico passi. Riavviare inoltre il PIX una volta per verificare che torni attivo senza problemi. Una volta verificato che tutto funzioni correttamente, accendere l'altro PIX. Entrambi i PIX sono stati aggiornati alla versione 7.x e sono accesi. Verificare che le comunicazioni di failover vengano stabilite correttamente con il comando **show failover**.

**Nota:** il PIX applica ora la restrizione secondo cui qualsiasi interfaccia che passa il traffico di dati non può essere utilizzata come interfaccia di failover LAN o interfaccia di failover stateful. Se la configurazione PIX corrente dispone di un'interfaccia condivisa utilizzata per passare il normale traffico di dati, nonché le informazioni di failover LAN o le informazioni stateful e se si esegue l'aggiornamento, il traffico di dati non passa più attraverso questa interfaccia. Anche tutti i comandi associati all'interfaccia hanno esito negativo.

## [Installare Adaptive Security Device Manager \(ASDM\)](#)

Prima di installare ASDM, Cisco consiglia di leggere le note sulla versione per la quale si intende installare ASDM. Le Note di rilascio includono i browser e le versioni Java minimi supportati, nonché un elenco di nuove funzionalità supportate e avvertenze aperte.

Il processo di installazione di ASDM è leggermente diverso nella versione 7.0 rispetto al passato. Inoltre, una volta copiata l'immagine ASDM nella memoria flash, è necessario specificarla nella configurazione in modo che il PIX sappia di utilizzarla. Per installare l'immagine ASDM in Flash, effettuare i seguenti passaggi.

1. Scaricare l'[immagine ASDM](#) (solo utenti [registrati](#)) da Cisco.com e inserirla nella directory principale del server TFTP.
2. Verificare che il PIX disponga di connettività IP al server TFTP. A tal fine, eseguire il ping tra il server TFTP e il PIX.
3. Dal prompt di abilitazione, usare il comando **copy tftp flash**.

```
pixfirewall>enable  
Password:
```



```
pixfirewall#copy tftp flash
```

4. Immettere l'indirizzo IP del server TFTP.

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

5. Immettere il nome del file ASDM sul server TFTP che si desidera caricare.

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

6. Immettere il nome del file ASDM che si intende salvare in Flash. Premere **Invio** per mantenere lo stesso nome di file.

```
Destination filename [asdm-501.bin]?
```

7. L'immagine viene ora copiata dal server TFTP a Flash. Vengono visualizzati messaggi che indicano che il trasferimento è stato completato.

```
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. Dopo aver copiato l'immagine ASDM, usare il comando **asdm image flash:** per specificare l'immagine ASDM da utilizzare.

```
pixfirewall(config)#asdm image flash:asdm-501.bin
```

9. Salvare la configurazione in Flash con il comando **write memory**.

```
pixfirewall(config)#write memory
```

10. Il processo di installazione di ASDM è stato completato.

## Risoluzione dei problemi

Sintomo	Risoluzione
Dopo aver usato il metodo <b>copy tftp flash</b> per aggiornare il PIX e il riavvio, si blocca in questo ciclo di riavvio:	Gli accessori PIX con versioni del BIOS precedenti alla 4.2 non possono essere aggiornati con il comando

<pre> 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. </pre>	<p>copy tftp flash. È necessario aggiornarli con il metodo <a href="#">Modalità monitor</a>.</p>
<pre> Una volta eseguita la versione 7.0 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 </pre>	<p>Se il PIX è stato aggiornato dalla modalità Monitor alla versione 7.0, ma l'immagine 7.0 non è stata 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 <a href="#">modalità Monitor</a>. Una volta avviato, è necessario copiare di nuovo l'immagine utilizzando il metodo <b>copy tftp flash</b>.</p>
<p>Quando si esegue l'aggiornamento con il</p>	<p>Questo messaggio viene in genere visualizzato</p>

<pre> metodo <b>copy tftp flash</b>, viene visualizzato questo messaggio di errore: pixfirewall#<b>copy tftp flash</b> 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 <b>Insufficient flash space available for this request:</b> Size info: request:5066808 current:1966136 delta:3100672 free:2752512 Image not installed pixfirewall# </pre>	<p>quando il PIX-535 o PIX-515 (non E) viene aggiornato tramite il metodo <b>copy tftp flash</b> e anche il PDM viene caricato nella memoria flash su tale PIX. La risoluzione consiste nell'eseguire l'aggiornamento con il metodo <a href="#">Modalità monitor</a>.</p>
<p>Dopo l'aggiornamento di PIX dalla versione 6.x alla 7.0, alcune configurazioni non vengono migrate correttamente.</p>	<p>L'output del comando <b>show startup-config errors</b> 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.</p>
<p>PIX esegue la versione 7.x ed è installata una versione più recente. Quando il PIX viene riavviato, la versione precedente continua a essere caricata.</p>	<p>In PIX versione 7.x, potete salvare più immagini in Flash. Il PIX cerca prima nella configurazione la <b>memoria flash del sistema di avvio</b>: comandi. Questi comandi specificano l'immagine che il PIX deve avviare. Se il <b>sistema di avvio non lampeggia</b>: PIX avviano la prima immagine avviabile in Flash. Per avviare una versione diversa, specificare il file usando il comando <b>boot system flash: /&lt;nomefile&gt;</b>.</p>

<p>Un'immagine ASDM viene caricata in Flash, ma gli utenti non possono caricare ASDM nel browser.</p>	<p>Innanzitutto, accertatevi che il file ASDM caricato in Flash sia specificato dal comando <b>asdm image flash://&lt;asdm_file&gt;</b>. Verificare quindi che il comando <b>http server enable</b> sia presente nella configurazione. Infine, verificare che l'host che tenta di caricare ASDM sia autorizzato tramite il comando <b>http &lt;address&gt; &lt;mask&gt; &lt;interface&gt;</b>.</p>
<p>L'FTP non funziona dopo un aggiornamento.</p>	<p>Ispezione FTP non abilitata dopo l'aggiornamento. Abilitare l'ispezione FTP in uno dei due modi descritti nella sezione <a href="#">Abilita ispezione FTP</a>.</p>

## [Abilita ispezione FTP](#)

L'ispezione FTP può essere abilitata con uno dei due metodi seguenti:

- **Aggiungere FTP al criterio di ispezione predefinito/globale.** Se non esiste, creare la mappa di classe `inspection_default`.

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

Creare o modificare la mappa dei criteri `global_policy` e abilitare l'ispezione FTP per la classe `selection_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
```

Abilitare `global_policy` globalmente.

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

- **Abilitare FTP creando un criterio di ispezione separato.**

```
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
```

## [Ottieni un contratto di assistenza valido](#)

Per scaricare il software PIX, è necessario disporre di un contratto di assistenza valido. Per ottenere un contratto di assistenza, eseguire i seguenti passaggi:

- Se disponi di un contratto di acquisto diretto, contatta il team Cisco che gestisce gli account.
- [Per](#) acquistare un contratto di assistenza, [contattare](#) un partner o un rivenditore Cisco.
- Utilizzare [Profile Manager](#) per aggiornare il profilo Cisco.com e richiedere l'associazione a un contratto di assistenza.

## [Informazioni correlate](#)

- [Pagina di supporto per PIX Security Appliance](#)
- [Informazioni di riferimento sui comandi PIX](#)
- [RFC \(Requests for Comments\)](#)
- [Domande frequenti su PIX Firewall](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)