

PIX 500 Security Appliance 6.x to 7.x Software Upgrade Procedure

Document ID: 63879

Note: This document covers how to upgrade the software on a PIX 500 Series Security Appliance. In order to download PIX software, refer to the **Software Center (registered customers only)**. You must log in and possess a valid service contract in order to access the PIX software.

Introduction

Prerequisites

Requirements

Components Used

Minimum System Requirements

Memory Upgrade Information for PIX 515/515E Appliances

Conventions

Upgrade the PIX Security Appliance

Software Downloads

Upgrade Procedure

Upgrade the PIX Security Appliance from Monitor Mode

Enter Monitor Mode

Upgrade the PIX from Monitor Mode

Upgrade the PIX Security Appliance with the copy tftp flash Command

Downgrade from PIX 7.x to 6.x

Upgrade PIX Appliances in a Failover Set

Install Adaptive Security Device Manager (ASDM)

Troubleshoot

Enable FTP Inspection

Obtain a Valid Service Contract

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document explains how to upgrade the PIX Appliance from version 6.2 or 6.3 to version 7.x. It also covers the installation of Adaptive Security Device Manager (ASDM) version 5.0.

Prerequisites

Requirements

Before you start this upgrade procedure, complete these tasks.

- Use the **show running-config** or **write net** command in order to save the current PIX configuration to a text file or a TFTP server.
- Use the **show version** command in order to display the serial number and activation key. Save this output to a text file. If you need to revert back to an older version of code, you might need the original activation key. For additional information on activation keys, refer to PIX Firewall Frequently Asked

Questions.

- Ensure you have no **conduit** or **outbound** commands in your current configuration. These commands are no longer supported in 7.x and the upgrade process removes them. Use the Output Interpreter (registered customers only) tool in order to convert these commands to access-lists before you attempt the upgrade.
- Ensure the PIX does not terminate Point to Point Tunneling Protocol (PPTP) connections. PIX 7.1 and later does not currently support PPTP termination.
- If you use Failover, ensure the LAN or Stateful interface is not shared with any data that passes interfaces. For example, if you use your Inside interface in order to pass data traffic as well as for your Stateful failover interface (failover link inside), you must move the Stateful failover interface to a different interface before you upgrade. Failure to do so causes all configurations tied to the Inside interface to be removed. Also, data traffic does not pass through the interface after the upgrade.
- Ensure that the PIX runs version 6.2 or 6.3 before you proceed.
- Read the Release Notes for the version you plan to upgrade to so that you are aware of all new, changed, and deprecated commands.
- Reference the Upgrade Guide for any additional command changes between versions 6.x and 7.x.

Components Used

The information in this document is based on these software and hardware versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Minimum System Requirements

Before you start the upgrade process to version 7.x, Cisco recommends that the PIX run version 6.2 or later. This ensures that the current configuration properly converts. In addition, these hardware requirements must be met for minimum RAM and Flash requirements:

PIX Model	RAM Requirements		Flash Requirements
	Restricted (R)	UnRestricted (UR) / Failover Only (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

* All PIX-515 and PIX-515E Appliances require a memory upgrade.

Issue the **show version** command in order to determine the amount of RAM and Flash currently installed on the PIX. No Flash upgrades are needed, as all PIX Appliances in this table have 16 MB installed by default.

Note: Only the PIX Security Appliances in this table are supported in version 7.x. Older PIX Security Appliances, such as the PIX-520, 510, 10000, and Classic have been discontinued and do not run version 7.0 or later. If you have one of these appliances and wish to run 7.x or later, contact your local Cisco Account Team or Reseller in order to purchase a newer Security Appliance. In addition, PIX Firewalls with less than 64 MB of RAM (PIX-501, PIX-506, and PIX-506E) are unable to run the initial 7.0 release.

Memory Upgrade Information for PIX 515/515E Appliances

Memory upgrades are only required for the PIX-515 and PIX-515E appliances. See this table for the part numbers you need in order to upgrade the memory on these appliances.

Note: The part number is dependent on the license installed on the PIX.

Current Appliance Configuration		Upgrade Solution	
Platform License	Total Memory (before upgrade)	Part Number	Total Memory (after upgrade)
Restricted (R)	32 MB	PIX-515-MEM-32-	64 MB
Unrestricted (UR)	32 MB	PIX-515-MEM-128-	128 MB
Failover-Only (FO)	64 MB	PIX-515-MEM-128-	128 MB

Refer to the Cisco PIX 515/515E Security Appliance Memory Upgrade for PIX Software v7.0 Product Bulletin for additional information.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Upgrade the PIX Security Appliance

Software Downloads

Visit the Cisco Software Center (registered customers only) in order to download PIX 7.x software. TFTP server software is no longer available from Cisco.com. However, you can find many TFTP servers when you search for "tftp server" on your favorite Internet search engine. Cisco does not specifically recommend any particular TFTP implementation. For more information, refer to the TFTP server page (registered customers only) .

Upgrade Procedure

Be aware that the upgrade of your PIX Security Appliance to version 7.x is a major change. Much of the CLI is modified and therefore your configuration after the upgrade will appear very different. Only upgrade during a Maintenance window as the upgrade process requires some downtime. If you need to revert back to a 6.x image, you must follow the Downgrade procedures. Failure to do so causes the PIX to go into a continuous reboot loop. In order to continue, locate your PIX Appliance model in this table and then select the link to see instructions for how to upgrade.

PIX Model	Upgrade Method
PIX-515	Monitor
PIX-515E	copy tftp flash
PIX-525	copy tftp flash
PIX-535 (No PDM installed)	copy tftp flash
PIX-535 (PDM installed)	Monitor

Upgrade the PIX Security Appliance from Monitor Mode

Enter Monitor Mode

Complete these steps in order to enter Monitor Mode on the PIX.

1. Connect a console cable to the console port on the PIX with the use of these communication settings:
 - ◆ 9600 bits per second
 - ◆ 8 data bits
 - ◆ no parity
 - ◆ 1 stop bit
 - ◆ no flow control
2. Power cycle or reload the PIX. During bootup you are prompted to use **BREAK** or **ESC** in order to interrupt Flash boot. You have ten seconds to interrupt the normal boot process.
3. Press the **ESC** key or send a **BREAK** character in order to enter Monitor Mode.
 - ◆ If you use Windows Hyper Terminal, you can press the **ESC** key or press **Ctrl+Break** in order to send a **BREAK** character.
 - ◆ If you Telnet through a terminal server to access the console port of the PIX, you need to press **Ctrl+] (Control + right bracket)** in order to get to the Telnet command prompt. Then enter the **send break** command.
4. The `monitor>` prompt displays.
5. Proceed to the Upgrade the PIX from Monitor Mode section.

Upgrade the PIX from Monitor Mode

Complete these steps in order to upgrade your PIX from Monitor Mode.

Note: Fast Ethernet cards in 64-bit slots are not visible in monitor mode. This problem means that the TFTP server cannot reside on one of these interfaces. The user should use the **copy tftp flash** command in order to download the PIX Firewall image file through TFTP.

1. Copy the PIX Appliance binary image (for example, `pix701.bin`) to the root directory of the TFTP server.
2. Enter Monitor Mode on the PIX. If you are unsure how to do this, see the instructions for how to enter Monitor Mode in this document.

Note: Once in Monitor Mode, you can use the "?" key to see a list of available options.

3. Enter the interface number that the TFTP server is connected to, or the interface that is closest to the TFTP server. The default is interface 1 (Inside).

```
monitor>interface <num>
```

Note: In Monitor Mode, the interface always auto negotiates the speed and duplex. The interface settings cannot be hard coded. Therefore, if the PIX interface is plugged into a switch that is hard coded for speed/duplex, then reconfigure it to auto negotiate while you are in Monitor Mode. Also be aware that the PIX Appliance cannot initialize a Gigabit Ethernet interface from Monitor Mode. You must use a Fast Ethernet interface instead.

4. Enter the IP address of the interface defined in step 3.

```
monitor>address <PIX_ip_address>
```

5. Enter the IP address of the TFTP server.

```
monitor>server <tftp_server_ip_address>
```

6. (Optional) Enter the IP address of your gateway. A gateway address is required if the interface of the PIX is not on the same network as the TFTP server.

```
monitor>gateway <gateway_ip_address>
```

7. Enter the name of the file on the TFTP server that you wish to load. This is the PIX binary image file name.

```
monitor>file <filename>
```

8. Ping from the PIX to the TFTP server in order to verify IP connectivity.

If the pings fail, double check the cables, IP address of the PIX interface and the TFTP server, and the IP address of the gateway (if needed). The pings must succeed before you continue.

```
monitor>ping <tftp_server_ip_address>
```

9. Type **tftp** in order to start the TFTP download.

```
monitor>tftp
```

10. The PIX downloads the image into RAM and automatically boots it.

During the boot process, the file system is converted along with your current configuration. However, you are not done yet. Note this Warning message after you boot and continue on to step 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. Once booted, enter enable mode and copy the same image over to the PIX again. This time use the **copy tftp flash** command.

This saves the image into the Flash file system. Failure to perform this step results in a boot loop the next time the PIX reloads.

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

Note: For detailed instructions on how to copy the image over with the use of the **copy tftp flash** command, see the Upgrade the PIX Security Appliance with the copy tftp flash Command section.

12. Once the image is copied over using the **copy tftp flash** command, the upgrade process is complete.

Example Configuration – Upgrade the PIX Security Appliance from Monitor Mode

```
monitor>interface 1
0: i8255X @ PCI(bus:0 dev:13 irq:10)
1: i8255X @ PCI(bus:0 dev:14 irq:7 )
2: i8255X @ PCI(bus:1 dev:0  irq:11)
3: i8255X @ PCI(bus:1 dev:1  irq:11)
4: i8255X @ PCI(bus:1 dev:2  irq:11)
5: i8255X @ PCI(bus:1 dev:3  irq:11)

Using 1: i82559 @ PCI(bus:0 dev:14 irq:7 ), MAC: 0050.54ff.4d81
monitor>address 10.1.1.2
address 10.1.1.2
monitor>server 172.18.173.123
server 172.18.173.123
monitor>gateway 10.1.1.1
gateway 10.1.1.1
monitor>file pix701.bin
file pix701.bin
monitor>ping 172.18.173.123
Sending 5, 100-byte 0xa014 ICMP Echoes to 172.18.173.123, timeout is 4 seconds:
!!!!
Success rate is 100 percent (5/5)
monitor>tftp
tftp pix701.bin@172.18.173.123.....
Received 5124096 bytes

Cisco PIX Security Appliance admin loader (3.0) #0: Mon Mar  7 17:39:03 PST 2005
#####
128MB RAM

Total NICs found: 6
mcwa i82559 Ethernet at irq 10  MAC: 0050.54ff.4d80
mcwa i82559 Ethernet at irq  7  MAC: 0050.54ff.4d81
mcwa i82558 Ethernet at irq 11  MAC: 00e0.b600.2014
mcwa i82558 Ethernet at irq 11  MAC: 00e0.b600.2015
mcwa i82558 Ethernet at irq 11  MAC: 00e0.b600.2016
mcwa i82558 Ethernet at irq 11  MAC: 00e0.b600.2017
BIOS Flash=AT29C257 @ 0xffffd8000
Old file system detected. Attempting to save data in flash

!--- This output indicates that the Flash file
!--- system is formatted. The messages are normal.

Initializing flashfs...
flashfs[7]: Checking block 0...block number was (-10627)
flashfs[7]: erasing block 0...done.
flashfs[7]: Checking block 1...block number was (-14252)
flashfs[7]: erasing block 1...done.
flashfs[7]: Checking block 2...block number was (-15586)
flashfs[7]: erasing block 2...done.
flashfs[7]: Checking block 3...block number was (5589)
flashfs[7]: erasing block 3...done.
flashfs[7]: Checking block 4...block number was (4680)
flashfs[7]: erasing block 4...done.
flashfs[7]: Checking block 5...block number was (-21657)
flashfs[7]: erasing block 5...done.
flashfs[7]: Checking block 6...block number was (-28397)
flashfs[7]: erasing block 6...done.
flashfs[7]: Checking block 7...block number was (2198)
flashfs[7]: erasing block 7...done.
flashfs[7]: Checking block 8...block number was (-26577)
flashfs[7]: erasing block 8...done.
flashfs[7]: Checking block 9...block number was (30139)
flashfs[7]: erasing block 9...done.
```

flashfs[7]: Checking block 10...block number 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]

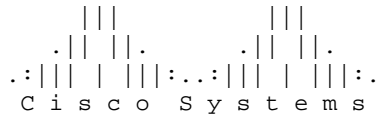
Licensed features for this platform:

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)

· ·
| |



Cisco PIX Security Appliance Software Version 7.0(1)

***** Warning *****

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

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

If you require further assistance please contact us by sending email to export@cisco.com.

***** Warning *****

Copyright (c) 1996-2005 by Cisco Systems, Inc.

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

!--- These messages are printed for any deprecated commands.

.ERROR: This command is no longer needed. The LOCAL user database is always enabled.
*** Output from config line 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:
<password>

pixfirewall#
pixfirewall#copy tftp flash

Address or name of remote host []? 172.18.173.123

Source filename []? pix701.bin

Destination filename [pix701.bin]?
<enter>

Accessing tftp://172.18.173.123/pix701.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file flash:/pix701.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
5124096 bytes copied in 139.790 secs (36864 bytes/sec)
pixfirewall#

```

Upgrade the PIX Security Appliance with the copy tftp flash Command

Complete these steps in order to upgrade the PIX with the use of the **copy tftp flash** command.

1. Copy the PIX Appliance binary image (for example, pix701.bin) to the root directory of the TFTP server.
2. From the enable prompt, issue the **copy tftp flash** command.

```

pixfirewall>enable
Password:
<password>

```

```

pixfirewall#copy tftp flash

```

3. Enter the IP address of the TFTP server.

```

Address or name of remote host [0.0.0.0]? <tftp_server_ip_address>

```

4. Enter the name of the file on the TFTP server that you wish to load. This is the PIX binary image file name.

```
Source file name [cdisk]?  
<filename>
```

5. When prompted to start the TFTP copy, type **yes**.

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

6. The image is now copied over from the TFTP server to Flash.

This message appears and indicates that the transfer is a success, the old binary image in Flash is erased, and the new image is written and installed.

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

7. Reload the PIX Appliance in order to boot the new image.

```
pixfirewall#reload  
Proceed with reload? [confirm]  
<enter>
```

Rebooting...

8. The PIX now boots the 7.0 image, and this completes the upgrade process.

Example Configuration – Upgrade the PIX Appliance with the 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]  
<enter>
```

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>
```

Note: With the unrestricted license, PIX 515 E can have up to eight VLANs and PIX 535 can have up to twenty-five VLANs.

Downgrade from PIX 7.x to 6.x

PIX Security Appliances versions 7.0 and later use a different Flash file format than earlier PIX versions. Therefore, you cannot downgrade from a 7.0 image to a 6.x image with the use of the **copy tftp flash** command. Instead, you must use the **downgrade** command. Failure to do so causes the PIX to get stuck in a boot loop.

When the PIX was originally upgraded, the 6.x startup-configuration was saved in Flash as `downgrade.cfg`. When you follow this downgrade procedure, this configuration is restored to the device when it is downgraded. This configuration can be reviewed before you downgrade when you issue the command **more flash:downgrade.cfg** from an `enable>` prompt in 7.0. Additionally, if the PIX was upgraded via Monitor Mode, then the previous 6.x binary image is still saved in Flash as `image_old.bin`. You can verify this image exists when you issue the **show flash:** command. If the image exists on Flash, you can use this image in step 1 of this procedure instead of loading the image from a TFTP server.

Complete these steps in order to downgrade your PIX Security Appliance.

1. Enter the **downgrade** command and specify the location of the image that you want to downgrade to.

```
pixfirewall#downgrade tftp://<tftp_server_ip_address>/<filename>
```

Note: If you upgraded your PIX from Monitor Mode, then the old binary image is still saved in Flash. Issue this command in order to downgrade back to that image:

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


Rebooting....

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

PCI Device Table.
Bus Dev Func VendID DevID Class Irq
00 00 00 8086 7192 Host Bridge
00 07 00 8086 7110 ISA Bridge
00 07 01 8086 7111 IDE Controller
00 07 02 8086 7112 Serial Bus 9
00 07 03 8086 7113 PCI Bridge
00 0D 00 8086 1209 Ethernet 11
00 0E 00 8086 1209 Ethernet 10
00 13 00 11D4 2F44 Unknown Device 5

Cisco Secure PIX Firewall BIOS (4.2) #0: Mon Dec 31 08:34:35 PST 2001
Platform PIX-515E
System Flash=E28F128J3 @ 0xffff00000

Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Reading 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 @ 0xffff00000
BIOS Flash=am29f400b @ 0xd8000
IRE2141 with 2048KB

..:|||||:..:|||||:..
c i s c o S y s t e m s
Private Internet eXchange

Cisco PIX Firewall

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

This PIX has an Unrestricted (UR) license.

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

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

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

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

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

***** Warning *****

Copyright (c) 1996-2003 by Cisco Systems, Inc.

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

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

Upgrade PIX Appliances in a Failover Set

An upgrade from PIX Appliance 6.x to 7.x is a major upgrade. It cannot be done without downtime, even for PIXes in a failover set. Many of the failover commands change with the upgrade. The recommend upgrade path is to power down one of the PIXes in the failover set. Then follow the instructions in this document in order to upgrade the powered on PIX. Once the upgrade is complete, verify that traffic passes, and also reboot the PIX once to verify it comes back up without issue. Once you are satisfied that everything properly works, power off the newly upgraded PIX and power on the other PIX. Then follow the instructions in this document in order to upgrade the PIX. Once the upgrade is complete, verify that traffic passes. Also reboot the PIX once in order to verify it comes back up without issue. Once you are satisfied that everything properly works, power on the other PIX. Both PIXes are now upgraded to 7.x and powered on. Verify they establish failover communications properly with the **show failover** command.

Note: The PIX now enforces the restriction that any interface that passes data traffic cannot also be used as the LAN failover interface, or the Stateful failover interface. If your current PIX configuration has a shared interface that is used to pass normal data traffic as well as the LAN failover information or the Stateful information, and if you upgrade, the data traffic no longer passes through this interface. All commands associated to that interface also fail.

Install Adaptive Security Device Manager (ASDM)

Before you install ASDM, Cisco recommends that you read the Release Notes for the version you plan to install. The Release Notes include the minimum supported browsers and Java versions as well as a list of new features supported and open caveats.

The process of installing ASDM is slightly different in version 7.0 than it has been in the past. Also, once the ASDM image is copied into the Flash, you must specify it in the configuration so the PIX knows to use it. Complete these steps in order to install the ASDM image into Flash.

1. Download the ASDM image (registered customers only) from Cisco.com and place it in the root directory of your TFTP server.
2. Verify your PIX has IP connectivity to your TFTP server. In order to do this, ping the TFTP server from the PIX.
3. From the enable prompt, issue the **copy tftp flash** command.

```
pixfirewall>enable
Password:
<password>
```

4. Enter the IP address of the TFTP server.

```
Address or name of remote host [0.0.0.0]? <tftp_server_ip_address>
```

5. Enter the name of the ASDM file on the TFTP server that you wish to load.

```
Source file name [cdisk]? <filename>
```

6. Enter the name for the ASDM file that you plan to save in Flash. Press **enter** to keep the same file name.

```
Destination filename [asdm-501.bin]? <enter>
```

7. The image is now copied over from the TFTP server to Flash. These messages appear and indicate that the transfer is a success.

```
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. After the ASDM image is copied over, issue the **asdm image flash:** command in order to specify the ASDM image to use.

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

9. Save the configuration to Flash with the **write memory** command.

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

10. This completes the ASDM installation process.

Troubleshoot

Symptom	Resolution
After you use the copy tftp flash method in order to upgrade the PIX, and reboot, it	PIX Appliances with

<p>gets stuck in this reboot loop:</p> <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>BIOS versions before 4.2 cannot be upgraded with the use of the copy tftp flash command. You must upgrade them with the Monitor Mode method.</p>
<p>After the PIX runs 7.0, and reboots, it gets stuck in this reboot loop:</p> <pre> 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>If the PIX was upgraded from Monitor Mode to 7.0, but the 7.0 image was not re-copied into Flash after the first boot of 7.0, then when the PIX is reloaded, it becomes stuck in a reboot loop.</p>
<p>When you upgrade with the copy tftp flash method, you see this error message:</p> <pre> 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# </pre>	<p>The resolution is to load the image again from Monitor Mode. After it boots up, you must copy the image one more time typically seen when with the use of the PIX-535 or PIX-515 (non E) is upgraded via the copy tftp flash method, and PDM is also loaded in Flash on that PIX.</p>
<p>After you upgrade the PIX from 6.x to 7.0, some of the configuration does not properly migrate.</p>	<p>The output of the show resolution is to upgrade with startup-config errors on the show command shows any errors that</p>

	<p>occurred during the migration of the configuration. The errors appear in this output after you boot the PIX for the first time. Examine these errors and attempt to resolve them.</p>
<p>The PIX runs version 7.x, and a newer version is installed. When the PIX reboots, the old version continues to load.</p>	<p>In PIX version 7.x, you can save multiple images in Flash. The PIX first looks in the configuration for any boot system flash: commands. These commands specify what image the PIX needs to boot. If no boot system flash: commands are found, the PIX boot the first bootable image in Flash. In order to boot a different version, specify the file with the use of the boot system flash:/<filename> command.</p>
<p>An ASDM image is loaded into Flash, but users are unable to load ASDM in their browser.</p>	<p>First, ensure the ASDM file loaded in Flash is specified by the asdm image flash://<asdm_file> command. Second, verify the http server enable command is in the configuration. Finally, verify the host that attempts to load ASDM is permitted via the http <address> <mask> <interface> command.</p>

FTP does not work after an upgrade.

FTP inspection was not enabled after the upgrade. Enable the FTP inspection in one of two ways as shown in the Enable FTP Inspection section.

Enable FTP Inspection

FTP inspection can be enabled with either of these two methods:

- **Add FTP to the default/global inspection policy.**

1. If it does not exist, create the **inspection_default** class-map.

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

2. Create or edit the **global_policy** policy map and enable FTP inspection for the class **inspection_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
```

3. Enable the **global_policy** globally.

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

- **Enable FTP by creating a separate inspection policy.**

```
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
```

Obtain a Valid Service Contract

You must have a valid service contract in order to download the PIX software. In order to obtain a service contract, perform these steps:

- Contact your Cisco Account team if you have a Direct Purchase Agreement.
- Contact a Cisco Partner or Reseller in order to purchase a service agreement.
- Use the Profile Manager in order to update your Cisco.com profile and request association to a service agreement.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [PIX Security Appliance Support Page](#)
- [Documentation for PIX Firewall](#)
- [PIX Command Reference](#)
- [Requests for Comments \(RFCs\)](#)
- [PIX Firewall Frequently Asked Questions](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 16, 2008

Document ID: 63879
