

Migration from PIX 500 Series Security Appliances to ASA 5500 Series Adaptive Security Appliances

Document ID: 91976

Introduction

Prerequisites

- Hardware and Software Requirements
- Components Used
- Conventions

Manual Configuration Conversion

- Upgrade the PIX Software Version to 7.x
- Convert Interface Names from Cisco PIX Software 7.0 to Cisco ASA Format
- Copy the Configuration from PIX to ASA
- Apply a PIX Software Version 6.x Configuration to ASA Software Version 7.x

Troubleshoot – Manual Configuration Conversion

- Device Stuck in Reboot Loop
- Error Message
- Configuration Does Not Seem Correct
- Some Services Such as FTP Do Not Work

Related Information

Introduction

This document explains how to migrate from PIX 500 Series Security Appliances to ASA 5500 Series Adaptive Security Appliances.

Note: The PIX 501, PIX 506 and PIX 506E do not support software version 7.

There are two ways to convert a PIX configuration to an ASA configuration

- Tool-Assisted Conversion
- Manual Conversion

Automatic Tool based / Tool-Assisted Conversion

Cisco recommends that you use the tool-assisted conversion in order to convert PIX configurations to ASA configurations.

The tool-assisted conversion method is faster and more scalable if you make multiple conversions. However, the output of the process in an intermediate configuration contains both old syntax and new syntax. This method relies on the installation of the intermediate configuration on the target adaptive security appliance to complete the conversion. Until it is installed on the target device, you cannot view the final configuration.

Note: Cisco has released the PIX to ASA Migration tool in order to help automate the process of migrating to the new ASA appliances. This tool can be downloaded from the PIX Software download site. Refer to Migrating the Configuration of PIX 500 Series Security Appliance to ASA 5500 Series Adaptive Security Appliances for more information.

Prerequisites

Hardware and Software Requirements

You can upgrade PIX 515, 515E, 525, 535 to version 7.0.

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 requirements:

PIX Model	RAM Requirements	
	Restricted (R)	UnRestricted (UR) / Failover Only (FO)
PIX-515	64 MB*	128 MB*
PIX-515 E	64 MB*	128 MB*
PIX-525	128 MB	256 MB
PIX-535	512 MB	1 GB

Issue the **show version** command in order to determine the amount of RAM currently installed on the PIX.

Note: PIX 515 and 515E software upgrades can require a memory upgrade as well:

- Those with restricted licenses and 32 MB of memory must be upgraded to 64 MB of memory.
- Those with unrestricted licenses and 64 MB of memory must be upgraded to 128 MB of memory.

See this table for the part numbers you need in order to upgrade the memory on these appliances.

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

Note: The part number depends upon the license installed on the PIX.

The upgrade of software version 6.x to 7.x is seamless and requires some manual work, but these steps must be completed before you begin:

1. Ensure you have no **conduit** or **outbound/apply** commands in your current configuration. These commands are no longer supported in 7.x and the upgrade process removes them. Use the Conduit Converter tool in order to convert these commands to access-lists before you attempt the upgrade.

2. Ensure that PIX does not terminate Point to Point Tunneling Protocol (PPTP) connections. Software version 7.x currently does not support PPTP termination.
3. Copy any digital certificates for VPN connections on the PIX before you start the upgrade process.
4. Read these documents in order to ensure that you are aware of new, changed and deprecated commands:
 - ◆ Release notes for the software version to which you plan to upgrade, which can be found at Cisco PIX Security Appliance Release Notes.
 - ◆ Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0
5. Plan to perform the migration during downtime. Although the migration is a simple two step process, the upgrade of the PIX Security Appliance to 7.x is a major change and requires some downtime.
6. Download the 7.x software from Cisco Downloads (registered customers only) .

Components Used

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

- ASA 5500 Series Security Appliances
- PIX Security Appliance 515, 515E, 525, and 535
- PIX Software versions 6.3, 7.0

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.

Conventions

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

Manual Configuration Conversion

With the manual conversion process, you use a text editor to go through your configuration line-by-line and convert PIX-specific commands to ASA commands.

Manual conversion of the PIX configuration to an ASA configuration gives you the most control over the conversion process. However, the process is time consuming and does not scale well if you must make more than one conversion.

These three steps must be completed in order to migrate from PIX to ASA:

1. Upgrade the PIX software version to 7.x.
2. Convert interface names from Cisco PIX software 7.0 to Cisco ASA Format.
3. Copy the PIX software 7.0 configuration to Cisco ASA 5500.

Upgrade the PIX Software Version to 7.x

Before you start the actual upgrade process, complete these steps:

1. Issue the **show running-config** or **write net** command in order to save the PIX current configuration to a text file or a TFTP server.
2. Issue the **show version** command in order to verify the requirements, such as RAM. Also, save the output of this command to a text file. If you need to revert back to an older version of the code, you can potentially need the original activation key.


```
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: Issue the **show version** command in order to verify that the PIX now runs the 7.x software version.

Note: In order to examine any errors that occurred during the migration of the configuration, issue the **show startup-config errors** command. The errors appear in this output after you boot the PIX for the first time.

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 the 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 in order 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, issue 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.

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 Enter Monitor Mode.

Note: Once in Monitor Mode, you can use the "?" key in order 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, 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 three.

```
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 want 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, the 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 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, issue the **copy tftp flash** command.

This saves the image to the Flash file system. Failure to complete 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 with 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.
```




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#

```

Convert Interface Names from Cisco PIX Software 7.0 to Cisco ASA Format

The next step in the process is to edit the newly converted Cisco PIX Software 7.0–based configuration offline.

Since the Cisco ASA interface naming convention is different from Cisco PIX Security Appliances, you need to make changes on the Cisco PIX configuration before you copy/upload it to your Cisco ASA 5500 Series Security Appliance.

Complete these steps in order to make the interface name changes on the PIX configuration:

1. Copy the new Cisco PIX Software 7.0–based configuration offline. In order to do this, upload the configuration to a TFTP/FTP server or copy the configuration from a console session to a text editor.

In order to upload the PIX configuration to a TFTP/FTP server, from the console, issue this command:

```
copy startup config tftp://n.n.n.n/PIX7cfg.txt
or
copy startup config ftp://n.n.n.n/PIX7cfg.txt
```

2. Once the Cisco PIX Software 7.0–based configuration file successfully uploads to the TFTP/FTP server (or is pasted/copied to a text editor), open Notepad/WordPad or any favorite text editor in order to change the interface names on the PIX configuration.

Cisco PIX Security Appliances number interfaces from 0 to n. Cisco ASA 5500 Series Security Appliances number interfaces based on their location/slot. Embedded interfaces are numbered from 0/0 to 0/3, and the management interface is **Management 0/0**. Interfaces on the 4GE SSM module are numbered from 1/0 to 1/3.

Cisco ASA 5510 with a base license that runs 7.0 has three Fast Ethernet ports (0/0 through 0/2) plus the Management 0/0 interface available. Cisco ASA 5510 with a Security Plus license has all five Fast Ethernet interfaces available. Cisco ASA 5520 and 5540 have four Gigabit Ethernet ports and one Fast Ethernet management port. Cisco ASA 5550 has eight Gigabit Ethernet ports and one Fast Ethernet port.

Change the interface names on the PIX configuration to ASA interface format.

For Example :

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

Refer to the Configuring Interface Parameters section of Cisco Security Appliance Command Line Configuration Guide, Version 7.0 for more information.

Copy the Configuration from PIX to ASA

At this point, you have a Cisco PIX Software 7.0–based configuration with the interface names modified ready to be copied or uploaded to your Cisco ASA 5500 Series. There are two ways to load the Cisco PIX Software 7.0–based configuration to the Cisco ASA 5500 Series appliance.

Complete the steps in Method 1: Manual Copy/Paste or Method 2: Download from TFTP/FTP.

Method 1: Manual Copy/Paste

Copy the configuration through the copy/paste method from the PIX console:

1. Log into the Cisco ASA 5500 series through the console and issue the **clear config all** command in order to clear the configuration before you paste the modified Cisco PIX Software 7.0 configuration.

```
ASA#config t
ASA(config)#clear config all
```

2. Copy and paste the configuration to the ASA console, and save the configuration.

Note: Make sure that all the interfaces are in the `no shutdown` state before you start to test.

Method 2: Download from TFTP/FTP

The second method is to download the Cisco PIX Software 7.0–based configuration from a TFTP/FTP server. For this step, you need to configure the management interface on the Cisco ASA 5500 series appliance for TFTP/FTP download:

1. From the ASA console, issue this:

```
ASA#config t
ASA(config)#interface management 0
ASA(config)#nameif management
ASA(config)#ip add <n.n.n.n> <netmask>
ASA(config)#no shut
```

Note: (Optional) `route management <ip> <mask> <next-hop>`

2. Once the management interface is set up, you can download the PIX configuration to the ASA:

```
ASA(Config)#copy tftp://<n.n.n.n>/PIX7cfg.txt running-config
```

3. Save the configuration.

Apply a PIX Software Version 6.x Configuration to ASA Software Version 7.x

The conversion of a PIX 6.2 or 6.3 configuration to a new ASA Security Appliance is a manual process. The ASA/PIX administrator is required to convert PIX 6.x syntax to match the ASA syntax and type the commands into the ASA configuration. You can cut and paste some commands such as the **access-list** command. Be sure to closely compare the PIX 6.2 or 6.3 configuration to the new ASA configuration in order to ensure no mistakes are made in the conversion.

Note: The Output Interpreter Tool (registered customers only) (OIT) can be used in order to convert some of the older, unsupported, commands such as **apply**, **outbound** or **conduit** to the appropriate access-list. The converted statements need to be reviewed thoroughly. It is necessary to verify that the conversion matches the security policies.

Note: The process for the upgrade to a new ASA appliance is different from an upgrade to a new PIX appliance. An attempt to upgrade to an ASA with the PIX process generates a number of configuration errors on the ASA.

Troubleshoot – Manual Configuration Conversion

Device Stuck in Reboot Loop

- After you use the **copy tftp flash** method in order to upgrade the PIX, and reboot, it gets stuck in this reboot loop:

```
Cisco Secure PIX Firewall BIOS (4.0) #0:
Thu Mar  2 22:59:20 PST 2000
Platform PIX-515
Flash=i28F640J5 @ 0x300

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

PIX appliances with BIOS versions earlier than 4.2 cannot be upgraded with the use of the **copy tftp flash** command. You must upgrade them with the Monitor Mode method.

- After the PIX runs 7.x, and reboots, it gets stuck in this reboot loop:

```
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
```

If the PIX is upgraded from Monitor Mode to 7.0, but the 7.0 image is 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.

The resolution is to load the image again from Monitor Mode. After it boots, you must copy the image one more time with the use of the **copy tftp flash** method.

Error Message

When you upgrade with the **copy tftp flash** method, you see this error message:

```
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#
```

This message typically appears when the PIX 515 or a PIX 535 with PDM already installed is upgraded with the **copy tftp flash** method.

Upgrade with the Monitor Mode method in order to resolve this.

Configuration Does Not Seem Correct

After you upgrade the PIX from 6.x to 7.x, some of the configuration does not properly migrate.

The output of the **show startup-config errors** command shows any errors that 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.

Some Services Such as FTP Do Not Work

Occasionally, some services such as FTP do not work after an upgrade.

The inspection for these services are not enabled after the upgrade. Enable the inspection for the appropriate services. In order to do this, add them to default/global inspection policy or create a separate inspection policy for the desired service.

Refer to the *Applying Application Layer Protocol Inspection* section of Cisco Security Appliance Command Line Configuration Guide, Version 7.0 for more information about inspection policies.

Related Information

- [Cisco PIX 500 Series Security Appliances – Introduction](#)
 - [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: Sep 26, 2008

Document ID: 91976
