CHAPTER 4

Upgrading

Prerequisites to Upgrading

Note Before beginning this section, read Chapter 1, "Before You Begin."

If you are upgrading from a PIX 515 or a PIX 535 with PDM already installed, you *must* upgrade from monitor mode. See the instructions in the "Upgrading in Monitor Mode" section on page 4-9.

If you attempt to upgrade using the instructions in the "Basic Upgrade from PIX Version 6.3 to Security Appliance Version 7.0" section on page 4-12, you will receive the following output:

```
Insufficient flash space available for this request:
Size info:request:5025848 current:1966136 delta:3059712 free:1310720
Image not installed
```

Several prerequisites are required before upgrading to PIX Security appliance Version 7.0, covered in the following sections:

- Minimum Hardware Requirements, page 4-1
- Minimum Software Requirements, page 4-2
- Minimum Memory Requirements, page 4-2
- Client PC Operating System and Browser Requirements, page 4-3
- Minimum Connectivity Requirements, page 4-4

Minimum Hardware Requirements

The PIX Security appliance Version 7.0 software runs on the PIX 515/515E, PIX 525, and PIX 535 platforms. PIX Security appliance Version 7.0 is not currently supported on PIX 501 or PIX 506/506E hardware.

Minimum Software Requirements

The minimum software version required before performing an upgrade to PIX Security appliance Version 7.0 is PIX Version 6.2. If you are running a PIX release before PIX Version 6.2, you must first upgrade to PIX Version 6.2 or PIX Version 6.3 before you can begin the upgrade to PIX Security appliance Version 7.0.

Note We recommend backing up your images, and configurations before performing the upgrade.

To upgrade your PIX software image, go to the following website:

http://www.cisco.com/cisco/software/navigator.html

Minimum Memory Requirements

If you are a PIX 515 or PIX 515E user with a PIX Version 6.3, you will need to upgrade your memory before performing an upgrade to PIX Security appliance Version 7.0. PIX Security appliance Version 7.0 requires at least 64 MB of RAM for Restricted (R) licenses and 128 MB of RAM for Unrestricted (UR) and Failover (FO) licenses (see Table 1).

Table 2 lists the minimum memory requirements for PIX 525 and PIX 535.

Table 1 Minimum Memory Requirements for PIX 515/515E

PIX Version 6.3 Platform License	Current Memory (MB)	Desired Upgrade Platform License	Part Number	Required Memory (MB)
R	32	—	PIX-515-MEM-32= Download software from cisco.com or purchase PIX-SW-UPGRADE=	64
R	64	—	Download software from cisco.com or purchase PIX-SW-UPGRADE=	64
R	32	UR	PIX-515-SW-R-UR= Remove your existing 32 MB memory module (DIMM) and replace it with two new 64 MB modules to achieve a total of 128 MB	128
R	64	UR	PIX-515-SW-R-UR= Remove your two existing 32 MB memory modules and replace with two new 64 MB modules to achieve a total of 128 MB	128
UR	64	—	PIX-515-MEM-128= Download software from cisco.com or purchase PIX-SW-UPGRADE=	128
UR	128	—	Download software from cisco.com or purchase PIX-SW-UPGRADE=	128
FO	64	—	PIX-515-MEM-128= Download software from cisco.com or purchase PIX-SW-UPGRADE=	128

Table 1 Minimum Memory Requirements for PIX 515/515E (continued)

PIX Version 6.3 Platform License	Current Memory (MB)	Desired Upgrade Platform License	Part Number	Required Memory (MB)
FO	128	—	Download software from cisco.com or purchase PIX-SW-UPGRADE=	128
FO	64	UR	PIX-515-SW-FO-UR=	128
FO	128	UR	PIX-515-SW-FO-UR=	128
R	64	UR	PIX-515-SW-R-UR=	128
FO	128	UR	PIX-515-SW-FO-UR=	128
FO	128	U	PIX-515-SW-FO-R=	64

The PIX 515 and PIX 515E memory upgrades do not require a BIOS update.

Note The minimum Flash memory requirement is 16 MB.

Table 2 lists the minimum memory requirements for PIX 525 and PIX 535.

Table 2 PIX 525 and PIX 535 Minimum Memory Requirements

Model	Minimum RAM
Cisco PIX 525 security appliance	128 MB on Restricted models
	256 MB on Unrestricted, Failover, and Failover Active/Active models
Cisco PIX 535 security appliance	512 MB on Restricted models
	1024 MB on Unrestricted, Failover, and Failover Active/Active models

Client PC Operating System and Browser Requirements

Table 3 lists the supported and recommended platforms for ASDM Version 5.0.

Table 3 Operating System and Browser Requirements

	Operating System	Browser	Other Requirements
Windows[1]	Windows 2000 (Service Pack 4) or Windows XP operating systems	Internet Explorer 6.0 with Java Plug-in 1.4.2 or 1.5.0 **Note** **HTTP 1.1**—Settings for Internet Options > Advanced > HTTP 1.1 should use HTTP 1.1 for both proxy and non-proxy connections. Netscape 7.1/7.2 with Java Plug-in 1.4.2 or 1.5.0	**SSL Encryption Settings**—All available encryption options are enabled for SSL in the browser preferences.
Sun Solaris	Sun Solaris 8 or 9 running CDE window manager	Mozilla 1.7.3 with Java Plug-in 1.4.2 or 1.5.0	
Linux	Red Hat Linux 9.0 or Red Hat Linux WS, Version 3 running GNOME or KDE	Mozilla 1.7.3 with Java Plug-in 1.4.2 or 1.5.0	

[1] ASDM is not supported on Windows 3.1, 95, 98, ME or Windows NT4.

Minimum Connectivity Requirements

The minimum connectivity requirements to perform an upgrade to PIX Security appliance Version 7.0 are as follows:

- A PC or server connected to any network port of the PIX and running TFTP software. (Your PC or server can be connected to the PIX using a switch or a crossover cable.)
- A DB-9 connector, and rollover cable, and a console connectivity program, such as HyperTerminal or another Terminal Emulation, to talk to the PIX.

Upgrade Procedure

This section includes the following topics:

- Basic Upgrade Procedure, page 4-5
- Upgrading in Monitor Mode, page 4-9
- Upgrade Examples, page 4-12

Important Notes

- If you are upgrading from a PIX 515 or a PIX 535 with PDM already installed, you *must* upgrade from monitor mode. See the instructions in the "Upgrading in Monitor Mode" section on page 4-9.

- The PIX Version 6.3 image on a PIX 515 or PIX 535 only accesses the first 8 MB of Flash memory, instead of the entire 16 MB of Flash. If the PIX Security appliance Version 7.0 image in combination with the Flash memory contents exceeds the 8 MB limit, following error message may result: **Insufficient flash space available for this request.** The solution is to load the image from monitor mode. See the "Upgrading in Monitor Mode" section on page 4-9.
- The PDM image in Flash memory is not automatically copied to the new filesystem. For information about installing ASDM (which replaces PDM on Version 7.0), see the ASDM Release Notes.
- To avoid installation failures, make sure that you have read the "Prerequisites to Upgrading" section on page 4-1 before proceeding.
- See the "Upgrade Examples" section on page 4-12 for configuration examples. These will be useful to review before you start your upgrade procedure.

⚠ **Caution** **If you share the Stateful Failover update link with a link for regular traffic such as your inside interface, you must change your configuration before upgrading. Please do not upgrade until you have corrected your configuration, as this is not a supported configuration and PIX Security appliance Version 7.0 treats the LAN failover and Stateful Failover update interfaces as special interfaces.**

If you upgrade to PIX Security appliance Version 7.0 with a configuration that shares an interface for both regular traffic and the Stateful Failover updates, configuration related to the regular traffic interface will be lost after the upgrade. The lost configuration may prevent you from connecting to the security appliance over the network.

Basic Upgrade Procedure

Note The automatic conversion of commands results in a change in your configuration. You should save your configuration after you upgrade, and review the changed configuration lines. Until you do so, the software will convert the old configuration automatically every time you read the configuration.

To upgrade using the commands available in PIX Version 6.3, perform the following steps:

Step 1 Enter the **login** command to log in to the PIX console.

Example:

```
pix> login
```

Step 2 Enter your username and password at the prompts.

```
Username:
Password:
```

Step 3 Enter the **enable** command to enter privileged mode and begin the upgrade procedure.

Example:

```
pix> enable
```

Step 4 Enter your password at the prompt.

```
Password:
```

You are now in privileged mode.

Step 5 Enter the **ping** <*ip address*> command to confirm access to the selected TFTP server.

Example:

```
pix> ping 192.168.2.200
```

Note Replace 192.168.2.200 with your TFTP server IP address.

Step 6 Enter the **write net** <*ip address*> <*filename*> command to save the current working configuration to the TFTP server.

Example:

```
pix> write net 192.168.2.200:63config.txt
```

Note Replace 63config.txt with a filename of your choice.

Step 7 Enter the **configure terminal** (**config t**) command to change from privilege mode to configuration mode.

```
pix# configure terminal
```

Step 8 Enter the **copy tftp flash:image** command to copy the PIX Security appliance Version 7.0 image from the TFTP server to the PIX Flash filesystem in configuration mode.

```
pix(config)# copy tftp flash:image
```

Note There is no: (colon) after tftp.

Step 9 Enter the name or IP address of the TFTP server.

```
Address or name of remote host [0.0.0.0]? 192.168.2.200
```

Note Replace 192.168.2.200 with your TFTP server IP address.

Step 10 Enter the PIX Security appliance Version 7.0 image name.

```
Source file name [cdisk]? pix704.bin
```

Step 11 Enter **yes** to copy the PIX Security appliance Version 7.0 image from the TFTP server to the security appliance running configuration.

```
copying tftp://192.168.2.200/pix704.bin to flash:image
[yes|no|again]? yes

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
…
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Received 5087232 bytes

Erasing current image

Writing 4833336 bytes of image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
…
```

```
!!!!!!!!!!!!!!
Image installed
```

Step 12 Enter the **reload** command to reboot the system. At the ‘Proceed with reload?’ prompt, press **Enter** to confirm the command.

```
pix# reload
Proceed with reload? [confirm]

Rebooting..

CISCO SYSTEMS PIX FIREWALL
Embedded BIOS Version 4.3.207 01/02/02 16:12:22.73
Compiled by xxxxxx
…
```

Note The PIX Security appliance Version 7.0 includes the same operational characteristics as PIX Version 6.3, such as licensing (as described by the PIX Version 6.3 activation key), IP addresses, access lists, access groups, VPN configurations, passwords, and preshared keys.

Step 13 and Step 14 are necessary only if you have configured authentication. If authentication is not enabled, skip to Step 15.

Step 13 Enter the **login** command to log in to the security appliance console.

```
pix> login
```

Step 14 Enter your username and password at the prompts.

```
Username:
Password:
```

Step 15 Enter the **enable** command to enter privileged mode and begin the upgrade procedure.

```
pix> enable
```

Step 16 Enter your password at the prompt.

```
Password:
```

You are now in privileged mode.

Step 17 Enter the **show running | grep boot** command to display configuration information.

```
pix# show running | grep boot
boot system flash:/<filename>
```

Note The correct <*filename*> is the name of the image on Flash.

- If the command line is correct, enter the **write memory** command to retain this configuration.

  ```
  pix# write memory
  …
  ```

- If the command line is incorrect:
  - **a.** Enter the **configure terminal** command to enter configuration mode.
  - **b.** Enter the **no boot system flash**:<*image*>**.bin** command.
  - **c.** Enter the correct command line.

d. Enter the **exit** command.

e. Enter **write memory** command to retain this configuration.

f. To load the PIX Security appliance Version 7.0 image from monitor mode, perform the following steps:

– Reload the PIX Security appliance Version 7.0 image.

– At the “Use BREAK or ESC to interrupt Flash boot” prompt, click ESC to enter monitor mode.

```
Proceed with reload? [confirm] [Press the enter key]
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.
Flash boot interrupted.
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.efc7
Use ? for help.
monitor>
```

– Enter the **interface #** command at the prompt, where # is the interface number.

Note Specify the correct interface number in place of # to indicate which interface to use to connect to the TFTP server.

```
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 0:i82559 @ PCI(bus:0 dev:13 irq:10), MAC:0050.54ff.efc6
```

Step 18 Enter the **reload** command to complete the upgrade process. Click Enter to confirm correct booting of the security appliance and the new image at the prompt.

```
pix# reload
Proceed with reload? [confirm]

Rebooting..

CISCO SYSTEMS PIX FIREWALL
Embedded BIOS Version 4.3.207 01/02/02 16:12:22.73
Compiled by xxxxxx
…
```

This completes the procedure to upgrade from PIX Version 6.3 to PIX Security appliance Version 7.0.

Upgrading in Monitor Mode

This section includes instructions for upgrading to PIX Security appliance Version 7.0 in monitor mode.

Examples of existing PIX Version 6.3 configurations can be found at the "Upgrade Examples" section on page 4-12. Review these before you start your upgrade procedure.

Important Notes

- **Use of the PIX Version 6.3 npdisk utility, such as password recovery, will corrupt the PIX Security appliance Version 7.0 image and will require that you restart your system from monitor mode, and could cause you to lose your previous configuration, security kernel, and key information.**
- If you are upgrading from an existing PIX 515 or a PIX 535 with PDM installed, you *must* upgrade from monitor mode.
- You can only upgrade the PIX 535 in monitor mode from an FE card in a slot connected to a 32-bit bus, otherwise an error message results. Effectively, you can only upgrade the PIX 535 from bus 2 using interfaces from slots 4 though 8.
- To avoid installation failures, make sure that you have read the "Prerequisites to Upgrading" section on page 4-1 before proceeding.

Procedure

Perform the following steps to upgrade procedure in monitor mode:

Step 1 To load the PIX Security appliance Version 7.0 image from monitor mode, perform the following steps:

a. Reload the image.

b. At the "Use BREAK or ESC to interrupt Flash boot" prompt, click **ESC** to enter monitor mode.

```
Proceed with reload? [confirm] [Press the enter key]
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.
Flash boot interrupted.
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.efc7
Use ? for help.
monitor>
```

c. Enter the **interface #** command at the prompt, where # is the interface number.

Note Specify the correct interface number in place of # to indicate which interface to use to connect to the TFTP server.

```
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 0:i82559 @ PCI(bus:0 dev:13 irq:10), MAC:0050.54ff.efc6
```

d. Enter the **address** <*ip addres*s> command using the e0 interface IP address.

```
monitor> address 20.0.0.10
address 20.0.0.10
```

e. Enter the **server** <*ip address*> command, using the TFTP server IP address.

```
monitor> server 20.0.0.101
server 20.0.0.101
```

f. Enter the **ping** <*ip address*> command using the TFTP server IP address to verify that it can be reached.

```
monitor> ping 20.0.0.101
Sending 5, 100-byte 0xc56 ICMP Echoes to 20.0.0.101, timeout is 4 sec
!!!!!
Success rate is 100 percent (5/5)
```

g. Enter the optional **gateway** <ip> command to specify the default gateway address if the TFTP server is not on the directly connected network segment.

h. Enter the **file** <*filename for the 7.0 image*> command, using the PIX Security appliance Version 7.0 filename.

```
monitor> file pix704.bin
file pix704.bin
monitor> tftp
pix704.bin@20.0.0.101.....................................
............................................................
```

i. After the image has been copied, wait for the normal prompt to return. (This may take 3 minutes on a PIX 525 to as much as 10 minutes on a PIX 515E.)

The preceding step loads the security appliance image into RAM, starts its execution, saves the old configuration in the Flash filesystem, and converts the running configuration to the new CLI structure, but does not save the converted configuration to Flash.

j. Check your converted configuration for errors, addresses, and access control lists.

Step 2 To save the PIX Security appliance Version 7.0 image to Flash from global configuration mode, perform the following steps:

a. Copy the PIX Security appliance Version 7.0 image from the TFTP server using the following commands. (This requires you to configure an IP address on the security appliance interface that connects to the TFTP server.)

```
PIX(config)#interface ethernet 0
PIX(config-if)# ip address 20.0.0.10 255.255.255.0
copy tftp [:[[//location] [/tftp_pathname]]] flash[:[image | pdm]]
PIX(config)# copy tftp://20.0.0.101/pix704.bin flash:
```

The following set of TFTP prompts results from the preceding command:

```
Address or name of remote host [20.0.0.101]?
Source filename [pix704.bin]?
Destination filename [pix704.bin]?
```

Note Multiple lines referring to invalid Flash blocks will be printed while the Flash is reformatted, which is normal.

Your PIX Version 6.3 configuration will be saved as downgrade.cfg in PIX Security appliance Version 7.0.

b. Enter the **show flash** command to confirm that the image was copied to the Flash.

```
PIX(config)#show flash
Directory of flash:/
-rw- 2024 05:31:23 Apr 23 2004 downgrade.cfg
-rw- 4644864 06:13:53 Apr 22 2004 pix704.bin
```

c. Enter the new **boot system flash:/** command to boot from the new image.

```
PIX(config)#boot system flash:/
```

For example:

```
boot system flash:pix704.bin
```

d. Enter the **write memory** command to update the Flash configuration file.

```
PIX(config)#write memory
```

e. Enter the **show version** command to confirm that the image has been upgraded.

```
PIX(config)#show version
```

Note Use the **show startup-config errors** command to see the errors that occurred while reading the configuration from Flash memory.

To display output from the upgrade, see "Upgrade Examples" section on page 4-12.

Upgrade Examples

To upgrade your PIX Version 6.3 software to PIX Security appliance Version 7.0, perform the steps in the "Upgrade Procedure" section on page 4-4. Seven output configuration scenarios are included in this section. Each scenario includes the assumptions used, a before upgrade configuration example, an upgrade configuration example, and an after upgrade configuration example.

- Basic Upgrade from PIX Version 6.3 to Security Appliance Version 7.0, page 4-12
- Upgrading to a VPN Client with Remote Access, page 4-22
- Upgrading to Security Appliance Version 7.0 Using VLAN, page 4-32
- Upgrading to Security Appliance Version 7.0 with Voice Over IP, page 4-43
- Upgrading to Security Appliance Version 7.0 with Authentication, page 4-53
- Upgrading to Security Appliance Version 7.0 with Active/Standby Failover, page 4-62
- Upgrading to Security Appliance Version 7.0 with Conduits, page 4-84

Note Occasionally the upgrade from PIX Version 6.3 to PIX Security appliance Version 7.0 will produce warning and system messages related to the change in command syntax. These messages are normal.

The **show run** command is interchangeable with the **write terminal** command in the following examples.

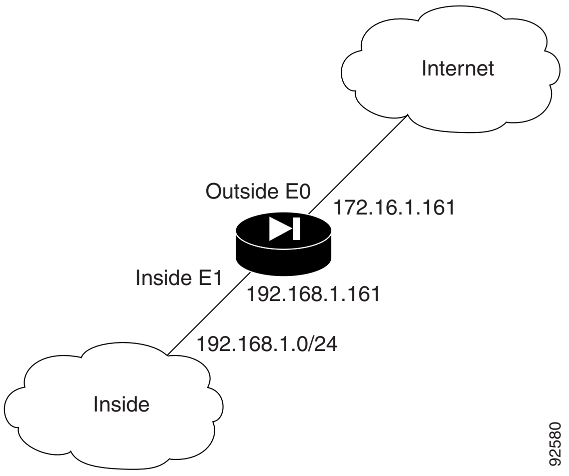
Basic Upgrade from PIX Version 6.3 to Security Appliance Version 7.0

Assumptions

When performing a basic upgrade from PIX Version 6.3 to PIX Security appliance Version 7.0, this configuration example assumes the following (see Figure 1):

- All inside hosts have outside access via a global pool
- DHCP provides address information to a small number of inside hosts
- The HTTP server is accessible from the inside and outside interfaces for management
- ICMP is permitted across the security appliance to enable network connectivity testing
- Telnet is permitted from outside sources to a specific inside host

Figure 1 ***Sample Basic Upgrade Configuration***



Before Upgrade

The following is sample output from the **show run** command from your current PIX Version 6.3 configuration before upgrading to PIX Security appliance Version 7.0:

```
Migration1(config)# show run
: Saved
:
PIX Version 6.3(4)

interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
nameif ethernet3 intf3 security6
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Migration1
domain-name ciscopix.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
name 172.16.1.75 Linux
```

```
access-list 101 permit icmp any any
access-list 101 permit tcp any host 172.16.1.160 eq telnet
pager lines 24
logging on
logging trap informational
logging host inside 192.168.1.99
icmp permit any outside
icmp permit any inside
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
ip address outside 172.16.1.161 255.255.255.0
ip address inside 192.168.1.161 255.255.255.0
no ip address dmz
no ip address intf3
no ip address intf4
no ip address intf5
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address dmz
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
pdm location 192.168.1.99 255.255.255.255 inside
pdm history enable
arp timeout 14400
global (outside) 1 172.16.1.210-172.16.1.212
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 172.16.1.160 192.168.1.100 netmask 255.255.255.255 0 0
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
http server enable
http 0.0.0.0 0.0.0.0 outside
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.100-192.168.1.102 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable inside
terminal width 80
Cryptochecksum:513c9e266857650270411a7f884e68f7
: end
```

Upgrade

Enter the **copy tftp://<***ip address***>/pix704.bin.<***image***>flash:image** command to upgrade to the new image.

The following output reflects the upgrade procedure from your current PIX Version 6.3 configuration to PIX Security appliance Version 7.0:

```
Migration1# copy tftp://192.168.1.161/cdisk.7.0(4) flash:image
copying tftp://192.168.1.100/cdisk.7.0(4) to flash:image

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!

Received 5124096 bytes

Erasing current image

Writing 5062712 bytes of image

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Image installed

Migration1# reload
Proceed with reload? [confirm]

Rebooting..

CISCO SYSTEMS PIX FIREWALL

Embedded BIOS Version 4.3.207 01/02/02 16:12:22.73
Compiled by xxxxxx
64 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  11  00   14E4   5823  Co-Processor       11
 00  13  00   8086   B154  PCI-to-PCI Bridge
 01  04  00   8086   1229  Ethernet           11
 01  05  00   8086   1229  Ethernet           10
 01  06  00   8086   1229  Ethernet           9
 01  07  00   8086   1229  Ethernet           5

Cisco Secure PIX Firewall BIOS (4.2) #0: Mon Dec 31 08:34:35 PST 2001
Platform PIX-515E
System Flash=E28F128J3 @ 0xfff00000

Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.

Reading 5059072 bytes of image from flash.

###########################################################################################
###########################################################################################
###########################################################################################
###########################################################################################
###########################################################################################
######
64MB RAM

Total NICs found: 6
mcwa i82559 Ethernet at irq 11  MAC: 0011.937e.0650
mcwa i82559 Ethernet at irq 10  MAC: 0011.937e.064f
mcwa i82559 Ethernet at irq 11  MAC: 000d.88ee.dfa0
mcwa i82559 Ethernet at irq 10  MAC: 000d.88ee.dfa1
mcwa i82559 Ethernet at irq  9  MAC: 000d.88ee.dfa2
mcwa i82559 Ethernet at irq  5  MAC: 000d.88ee.dfa3
BIOS Flash=am29f400b @ 0xd8000
Old file system detected. Attempting to save data in flash


Initializing flashfs...
flashfs[7]: Checking block 0...block number was (-14264)
flashfs[7]: erasing block 0...done.
flashfs[7]: Checking block 1...block number was (12668)
flashfs[7]: erasing block 1...done.
flashfs[7]: Checking block 2...block number was (15104)
flashfs[7]: erasing block 2...done.
flashfs[7]: Checking block 3...block number was (-18577)
flashfs[7]: erasing block 3...done.
flashfs[7]: Checking block 4...block number was (11973)
flashfs[7]: erasing block 4...done.
flashfs[7]: Checking block 5...block number was (-4656)
flashfs[7]: erasing block 5...done.
flashfs[7]: Checking block 6...block number was (-24944)
flashfs[7]: erasing block 6...done.
flashfs[7]: Checking block 7...block number was (23499)
flashfs[7]: erasing block 7...done.
flashfs[7]: Checking block 8...block number was (7137)
flashfs[7]: erasing block 8...done.
flashfs[7]: Checking block 9...block number was (20831)
flashfs[7]: erasing block 9...done.
flashfs[7]: Checking block 10...block number was (6185)
flashfs[7]: erasing block 10...done.
```

```
flashfs[7]: Checking block 11...block number was (25501)
flashfs[7]: erasing block 11...done.
flashfs[7]: Checking block 12...block number was (-5607)
flashfs[7]: erasing block 12...done.
flashfs[7]: Checking block 13...block number was (27450)
flashfs[7]: erasing block 13...done.
flashfs[7]: Checking block 14...block number was (-6772)
flashfs[7]: erasing block 14...done.
flashfs[7]: Checking block 15...block number was (-10286)
flashfs[7]: erasing block 15...done.
flashfs[7]: Checking block 16...block number was (2597)
flashfs[7]: erasing block 16...done.
flashfs[7]: Checking block 17...block number was (30610)
flashfs[7]: erasing block 17...done.
flashfs[7]: Checking block 18...block number was (20305)
flashfs[7]: erasing block 18...done.
flashfs[7]: Checking block 19...block number was (-29480)
flashfs[7]: erasing block 19...done.
flashfs[7]: Checking block 20...block number was (3742)
flashfs[7]: erasing block 20...done.
flashfs[7]: Checking block 21...block number was (10580)
flashfs[7]: erasing block 21...done.
flashfs[7]: Checking block 22...block number was (-2896)
flashfs[7]: erasing block 22...done.
flashfs[7]: Checking block 23...block number was (-812)
flashfs[7]: erasing block 23...done.
flashfs[7]: Checking block 24...block number was (23019)
flashfs[7]: erasing block 24...done.
flashfs[7]: Checking block 25...block number was (-32643)
flashfs[7]: erasing block 25...done.
flashfs[7]: Checking block 26...block number was (25350)
flashfs[7]: erasing block 26...done.
flashfs[7]: Checking block 27...block number was (-4434)
flashfs[7]: erasing block 27...done.
flashfs[7]: Checking block 28...block number was (-25787)
flashfs[7]: erasing block 28...done.
flashfs[7]: Checking block 29...block number was (8591)
flashfs[7]: erasing block 29...done.
flashfs[7]: Checking block 30...block number was (-25606)
flashfs[7]: erasing block 30...done.
flashfs[7]: Checking block 31...block number was (-26665)
flashfs[7]: erasing block 31...done.
flashfs[7]: Checking block 32...block number was (12429)
flashfs[7]: erasing block 32...done.
flashfs[7]: Checking block 33...block number was (18421)
flashfs[7]: erasing block 33...done.
flashfs[7]: Checking block 34...block number was (29655)
flashfs[7]: erasing block 34...done.
flashfs[7]: Checking block 35...block number was (-5147)
flashfs[7]: erasing block 35...done.
flashfs[7]: Checking block 36...block number was (21867)
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]: relinked orphaned file into the fs as "/lost+found/00011".
flashfs[7]: relinked orphaned directory into the fs as "/lost+found/00008".
flashfs[7]: relinked orphaned directory into the fs as "/lost+found/00002".
flashfs[7]: 220 files, 8 directories
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 16128000
flashfs[7]: Bytes used: 7895040
flashfs[7]: Bytes available: 8232960
```

```
flashfs[7]: flashfs fsck took 53 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+ (Crypto5823 revision 0x1)
  --------------------------------------------------------------------------
                                 .            .
                                 |            |
                                |||          |||
                              .|| ||.      .|| ||.
                           .:||| | |||:..:||| | |||:.
                            C i s c o  S y s t e m s
  --------------------------------------------------------------------------

Cisco PIX Security Appliance Software Version 7.0(4)

  ****************************** 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

Cryptochecksum(unchanged): 513c9e26 68576502 70411a7f 884e68f7
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.
```

After Upgrade

After performing the PIX Security appliance Version 7.0 upgrade, enter the **enable** command to enter configuration mode, then enter your password, and finally enter the **show run** command. The output is as follows:

```
Migration1> enable
Password:

Migration1(config)# show run
: Saved

PIX Version 7.0(4)
```

```
names
name 172.16.1.75 Linux
!
interface Ethernet0
 speed 100
 duplex full
 nameif outside
 security-level 0
 ip address 172.16.1.161 255.255.255.0
!
interface Ethernet1
 speed 100
 duplex full
 nameif inside
 security-level 100
 ip address 192.168.1.161 255.255.255.0
!
interface Ethernet2
 shutdown
 nameif dmz
 security-level 50
 no ip address
!
interface Ethernet3
 shutdown
 nameif intf3
 security-level 6
 no ip address
!
interface Ethernet4
 shutdown
 nameif intf4
 security-level 8
 no ip address
!
interface Ethernet5
 shutdown
 nameif intf5
 security-level 10
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Migration1
domain-name ciscopix.com
boot system flash:/image.bin
ftp mode passive
access-list 101 extended permit icmp any any
access-list 101 extended permit tcp any host 172.16.1.160 eq telnet
pager lines 24
logging enable
logging trap informational
logging host inside 192.168.1.99
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
no failover
monitor-interface outside
monitor-interface inside
monitor-interface dmz
monitor-interface intf3
```

```
monitor-interface intf4
monitor-interface intf5
icmp permit any outside
icmp permit any inside
asdm history enable
arp timeout 14400
nat-control
global (outside) 1 172.16.1.210-172.16.1.212
nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 172.16.1.160 192.168.1.100 netmask 255.255.255.255
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 sunrpc 0:10:00 h323
0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
http server enable
http 0.0.0.0 0.0.0.0 outside
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp
no sysopt connection permit-ipsec
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 5
ssh timeout 5
ssh version 1
console timeout 0
dhcpd address 192.168.1.100-192.168.1.102 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable inside
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:513c9e266857650270411a7f884e68f7
: end

Migration1#
```

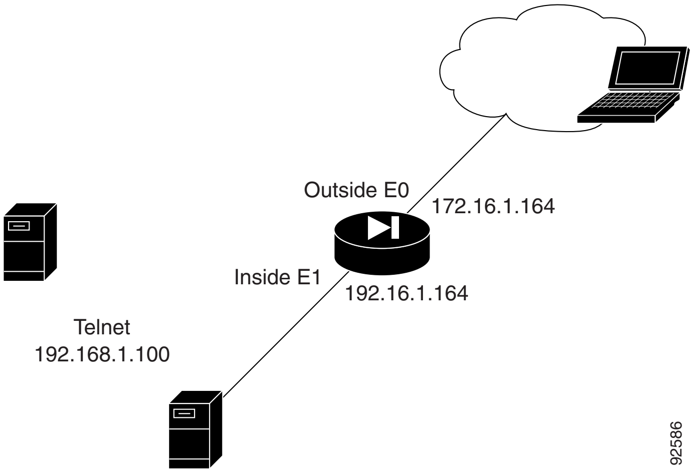
Upgrading to a VPN Client with Remote Access

Assumptions

When performing an upgrade to a VPN client with remote access, this configuration example assumes the following (see Figure 2):

- The PIX 515E functions as a headend device; incoming remote VPN clients terminate at the PIX 515E
- Authentication of the VPN client (not the user) connection is performed through preshared keys
- User authentication is performed using a Windows username and password
- Client addresses are between 3.3.3.0 and 3.3.3.254; use the **ip pool** command to find the correct IP address
- PDM is enabled from the inside network

Figure 2 Sample VPN Client Configuration



Before Upgrade

The following is sample output from the **show run** command from your current PIX Version 6.3 configuration before upgrading to PIX Security appliance Version 7.0:

```
vpnra# show run
: Saved
:
PIX Version 6.3(4)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 100full
interface ethernet3 100full
interface ethernet4 100full
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
nameif ethernet3 intf3 security6
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname vpnra
domain-name migration.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list nat0 permit ip any 3.3.3.0 255.255.255.0
pager lines 24
logging on
logging buffered debugging
icmp permit any outside
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
ip address outside 172.16.1.164 255.255.255.0
ip address inside 192.168.1.164 255.255.255.0
no ip address intf2
no ip address intf3
no ip address intf4
no ip address intf5
ip audit info action alarm
ip audit attack action alarm
ip local pool migratepool 3.3.3.1-3.3.3.254
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
pdm location 192.168.3.0 255.255.255.0 outside
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nat0
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 172.16.1.100 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
```

```
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto dynamic-map outside_dyn_map 20 set transform-set ESP-3DES-MD5
crypto map ForRA 20 ipsec-isakmp dynamic outside_dyn_map
crypto map ForRA interface outside
isakmp enable outside
isakmp policy 30 authentication pre-share
isakmp policy 30 encryption 3des
isakmp policy 30 hash md5
isakmp policy 30 group 2
isakmp policy 30 lifetime 86400
vpngroup migration address-pool migratepool
vpngroup migration idle-time 1800
vpngroup migration password ********
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:4a5e923ecb2353471603a82ee2f4df47
: end
```

Upgrade

Enter the **copy tftp://<*ip address*>/pix704.bin.<*image*>flash:image** command to upgrade to the new image. The following output reflects the upgrade procedure from your current PIX Version 6.3 configuration to PIX Security appliance Version 7.0:

```
vpnra# copy tftp://192.168.1.100/cdisk.7.0(4) flash:image
copying tftp://192.168.1.100/cdisk.7.0(4) to flash:image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Received 5124096 bytes
Erasing current image
Writing 5062712 bytes of image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image installed
```

Enter the **reload** command to begin using the new PIX Security appliance Version 7.0 image, then press **Enter** at the next prompt to confirm the **reload** command.

```
vpnra# reload
Proceed with reload? [confirm]


Rebooting...

CISCO SYSTEMS PIX FIREWALL
Embedded BIOS Version 4.3.207 01/02/02 16:12:22.73
Compiled by xxxxxx
64 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  11  00   14E4   5823  Co-Processor       11
 00  13  00   8086   B154  PCI-to-PCI Bridge
 01  04  00   8086   1229  Ethernet           11
 01  05  00   8086   1229  Ethernet           10
 01  06  00   8086   1229  Ethernet           9
 01  07  00   8086   1229  Ethernet           5

Cisco Secure PIX Firewall BIOS (4.2) #0: Mon Dec 31 08:34:35 PST 2001
Platform PIX-515E
System Flash=E28F128J3 @ 0xfff00000

Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Reading 5059072 bytes of image from flash.
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
########################################################
64MB RAM

Total NICs found: 6
mcwa i82559 Ethernet at irq 11  MAC: 0011.937e.0650
mcwa i82559 Ethernet at irq 10  MAC: 0011.937e.064f
mcwa i82559 Ethernet at irq 11  MAC: 000d.88ee.dfa0
mcwa i82559 Ethernet at irq 10  MAC: 000d.88ee.dfa1
mcwa i82559 Ethernet at irq  9  MAC: 000d.88ee.dfa2
mcwa i82559 Ethernet at irq  5  MAC: 000d.88ee.dfa3
BIOS Flash=am29f400b @ 0xd8000
Old file system detected. Attempting to save data in flash
```

```
Initializing flashfs...
flashfs[7]: Checking block 0...block number was (-14264)
flashfs[7]: erasing block 0...done.
flashfs[7]: Checking block 1...block number was (12668)
flashfs[7]: erasing block 1...done.
flashfs[7]: Checking block 2...block number was (15104)
flashfs[7]: erasing block 2...done.
flashfs[7]: Checking block 3...block number was (-18577)
flashfs[7]: erasing block 3...done.
flashfs[7]: Checking block 4...block number was (11973)
flashfs[7]: erasing block 4...done.
flashfs[7]: Checking block 5...block number was (-4656)
flashfs[7]: erasing block 5...done.
flashfs[7]: Checking block 6...block number was (-24944)
flashfs[7]: erasing block 6...done.
flashfs[7]: Checking block 7...block number was (23499)
flashfs[7]: erasing block 7...done.
flashfs[7]: Checking block 8...block number was (7137)
flashfs[7]: erasing block 8...done.
flashfs[7]: Checking block 9...block number was (20831)
flashfs[7]: erasing block 9...done.
flashfs[7]: Checking block 10...block number was (6185)
flashfs[7]: erasing block 10...done.
flashfs[7]: Checking block 11...block number was (25501)
flashfs[7]: erasing block 11...done.
flashfs[7]: Checking block 12...block number was (-5607)
flashfs[7]: erasing block 12...done.
flashfs[7]: Checking block 13...block number was (27450)
flashfs[7]: erasing block 13...done.
flashfs[7]: Checking block 14...block number was (-6772)
flashfs[7]: erasing block 14...done.
flashfs[7]: Checking block 15...block number was (-10286)
flashfs[7]: erasing block 15...done.
flashfs[7]: Checking block 16...block number was (2597)
flashfs[7]: erasing block 16...done.
flashfs[7]: Checking block 17...block number was (30610)
flashfs[7]: erasing block 17...done.
flashfs[7]: Checking block 18...block number was (20305)
flashfs[7]: erasing block 18...done.
flashfs[7]: Checking block 19...block number was (-29480)
flashfs[7]: erasing block 19...done.
flashfs[7]: Checking block 20...block number was (3742)
flashfs[7]: erasing block 20...done.
flashfs[7]: Checking block 21...block number was (10580)
flashfs[7]: erasing block 21...done.
flashfs[7]: Checking block 22...block number was (-2896)
flashfs[7]: erasing block 22...done.
flashfs[7]: Checking block 23...block number was (-812)
flashfs[7]: erasing block 23...done.
flashfs[7]: Checking block 24...block number was (23019)
flashfs[7]: erasing block 24...done.
flashfs[7]: Checking block 25...block number was (-32643)
flashfs[7]: erasing block 25...done.
flashfs[7]: Checking block 26...block number was (25350)
flashfs[7]: erasing block 26...done.
flashfs[7]: Checking block 27...block number was (-4434)
flashfs[7]: erasing block 27...done.
flashfs[7]: Checking block 28...block number was (-25787)
flashfs[7]: erasing block 28...done.
flashfs[7]: Checking block 29...block number was (8591)
flashfs[7]: erasing block 29...done.
flashfs[7]: Checking block 30...block number was (-25606)
```

```
flashfs[7]: erasing block 30...done.
flashfs[7]: Checking block 31...block number was (-26665)
flashfs[7]: erasing block 31...done.
flashfs[7]: Checking block 32...block number was (12429)
flashfs[7]: erasing block 32...done.
flashfs[7]: Checking block 33...block number was (18421)
flashfs[7]: erasing block 33...done.
flashfs[7]: Checking block 34...block number was (29655)
flashfs[7]: erasing block 34...done.
flashfs[7]: Checking block 35...block number was (-5147)
flashfs[7]: erasing block 35...done.
flashfs[7]: Checking block 36...block number was (21867)
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]: relinked orphaned file into the fs as "/lost+found/00238".
flashfs[7]: 229 files, 11 directories
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 16128000
flashfs[7]: Bytes used: 8273920
flashfs[7]: Bytes available: 7854080
flashfs[7]: flashfs fsck took 53 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+ (Crypto5823 revision 0x1)
  --------------------------------------------------------------------------
                                 .            .
                                 |            |
                                |||          |||
                              .|| ||.      .|| ||.
                          .:||| | |||:..:||| | |||:.
                            C i s c o   S y s t e m s
  --------------------------------------------------------------------------

Cisco PIX Security Appliance Software Version 7.0(4)

  ****************************** 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

Cryptochecksum(unchanged): 4a5e923e cb235347 1603a82e e2f4df47
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
Type help or '?' for a list of available commands.

San Jose, California 95134-1706
```

After Upgrade

Output from the PIX Security appliance Version 7.0 image upgrade includes the assumptions in “Before Upgrade” section on page 4-22, with the following changes:

- Interface information is now grouped
- The **vpngroup** command has been replaced by the **group-policy** and **tunnel-group** commands
- The default ISAKMP policy is now listed as policy number 65535, as shown in the following example:

PIX Version 6.3 syntax:

```
#
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit

#
```

The PIX Security appliance Version 7.0 syntax:

```
#
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400
```

After performing the PIX Security appliance Version 7.0 upgrade, enter the **enable** command to enter configuration mode, then enter your password, and finally enter the **show run** command. The output is as follows:

```
vpnra> enable
Password:
vpnra# show run
: Saved
:
PIX Version 7.0(4)
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.16.1.164 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 192.168.1.164 255.255.255.0
!
interface Ethernet2
 speed 100
 duplex full
 nameif intf2
 security-level 4
 no ip address
!
interface Ethernet3
 speed 100
 duplex full
 nameif intf3
 security-level 6
 no ip address
!
interface Ethernet4
 speed 100
 duplex full
 nameif intf4
 security-level 8
 no ip address
!
interface Ethernet5
 shutdown
 nameif intf5
 security-level 10
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname vpnra
domain-name migration.com
boot system flash:/image.bin
ftp mode passive
access-list nat0 extended permit ip any 3.3.3.0 255.255.255.0
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
ip local pool migratepool 3.3.3.1-3.3.3.254
no failover
monitor-interface outside
monitor-interface inside
monitor-interface intf2
monitor-interface intf3
monitor-interface intf4
monitor-interface intf5
icmp permit any outside
asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 0 access-list nat0
nat (inside) 1 0.0.0.0 0.0.0.0
route outside 0.0.0.0 0.0.0.0 172.16.1.100 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 sunrpc 0:10:00
```

```
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
group-policy migration internal
group-policy migration attributes
 vpn-idle-timeout 30
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto dynamic-map outside_dyn_map 20 set transform-set ESP-3DES-MD5
crypto map ForRA 20 ipsec-isakmp dynamic outside_dyn_map
crypto map ForRA interface outside
isakmp enable outside
isakmp policy 30 authentication pre-share
isakmp policy 30 encryption 3des
isakmp policy 30 hash md5
isakmp policy 30 group 2
isakmp policy 30 lifetime 86400
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400
telnet timeout 5
ssh timeout 5
ssh version 1
console timeout 0
tunnel-group migration type ipsec-ra
tunnel-group migration general-attributes
 address-pool migratepool
 default-group-policy migration
tunnel-group migration ipsec-attributes
 pre-shared-key *
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect ils
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:4a5e923ecb2353471603a82ee2f4df47
```

```
: end
vpnra#
```

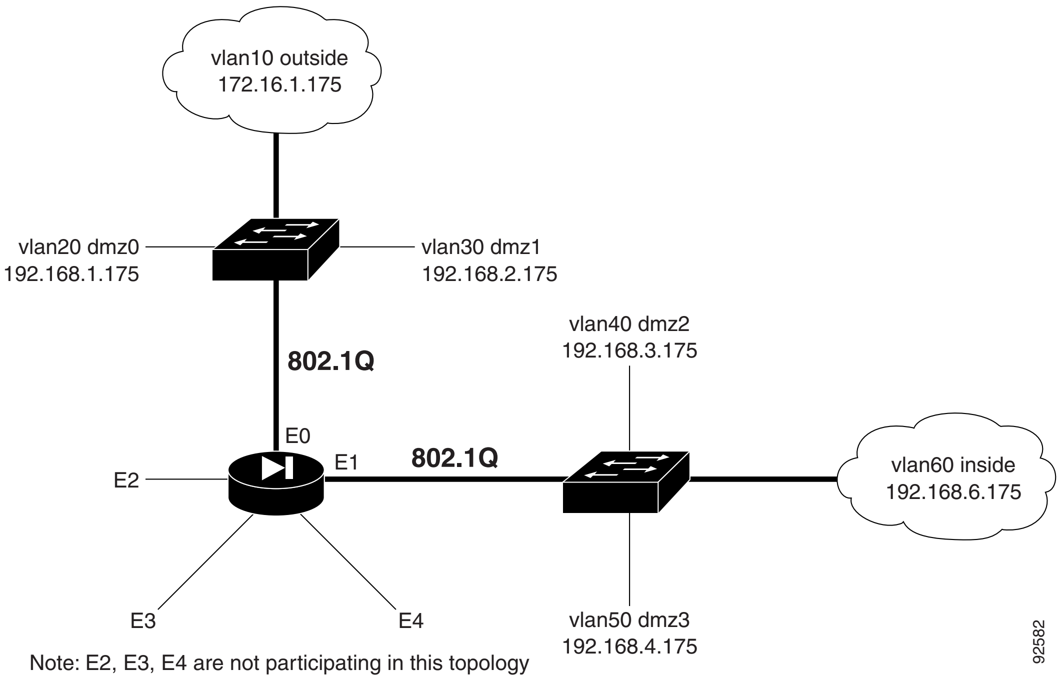
Upgrading to Security Appliance Version 7.0 Using VLAN

Assumptions

When performing an upgrade to PIX Security appliance Version 7.0 using VLAN, this configuration example assumes the following (see Figure 3):

- VLANs are enabled; 6 interfaces in total, 3 each on two trunk interfaces are outside; dmz0, dmz1, dmz2, dmz3 are inside
- Fixup protocols for **rsh** and **sqlnet** are turned off
- Logging at the debugging level is buffered
- Hosts on interface inside can originate connections through interface outside
- A server on interface dmz2 is available on interface outside
- Ethernet0 is an 802.1q trunk to a switch
- Ethernet1 is an 802.1a trunk to a switch
- Ethernet2 is non-trunk connection to a server farm

Figure 3 Sample VLAN Configuration



Before Upgrade

The following is sample output from the **show run** command from your current PIX Version 6.3 configuration before upgrading to PIX Security appliance Version 7.0:

```
PixVlan# show run
: Saved
:
PIX Version 6.3(4)
interface ethernet0 100full
interface ethernet0 vlan10 physical
interface ethernet0 vlan20 logical
interface ethernet0 vlan30 logical
interface ethernet1 100full
interface ethernet1 vlan40 physical
interface ethernet1 vlan50 logical
interface ethernet1 vlan60 logical
interface ethernet2 100full
interface ethernet3 100full
interface ethernet4 100full
interface ethernet5 auto shutdown
interface ethernet6 auto shutdown
interface ethernet7 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 dmz2 security40
nameif ethernet2 intf2 security4
nameif ethernet3 intf3 security6
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
nameif ethernet6 intf6 security12
nameif ethernet7 intf7 security14
nameif vlan20 dmz0 security20
nameif vlan30 dmz1 security30
nameif vlan50 dmz3 security50
nameif vlan60 inside security100
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PixVlan
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
no fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
no fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list 1 permit ip any host 172.16.1.144
pager lines 24
logging on
logging buffered debugging
mtu outside 1500
mtu dmz2 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
mtu intf6 1500
mtu intf7 1500
ip address outside 172.16.1.175 255.255.255.0
ip address dmz2 192.168.3.175 255.255.255.0
ip address intf2 10.1.1.1 255.255.255.0
no ip address intf3
no ip address intf4
no ip address intf5
no ip address intf6
no ip address intf7
ip address dmz0 192.168.1.175 255.255.255.0
ip address dmz1 192.168.2.175 255.255.255.0
ip address dmz3 192.168.4.175 255.255.255.0
ip address inside 192.168.6.175 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address dmz2
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
no failover ip address intf6
no failover ip address intf7
no failover ip address dmz0
no failover ip address dmz1
no failover ip address dmz3
no failover ip address inside
pdm history enable
arp timeout 14400
global (outside) 1 172.16.1.101-172.16.1.110
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (dmz2,outside) 172.16.1.144 192.168.3.144 netmask 255.255.255.255 0 0
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
http server enable
http 192.168.4.0 255.255.255.0 dmz3
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:8931adafa47b3649c5954e72212043a1
: end
```

Upgrade

Enter the **copy tftp://<*ip address*>/pix704.bin.<*image*>flash:image** command to upgrade to the new image. The following output reflects the upgrade procedure from your current PIX Version 6.3 configuration to PIX Security appliance Version 7.0:

```
PixVlan# copy tftp://10.1.1.100/cdisk.7.0(4) flash:image
copying tftp://10.1.1.100/cdisk.7.0(4) to flash:image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Received 5124096 bytes
Erasing current image
Writing 5062712 bytes of image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image installed
```

Enter the **reload** command to begin using the new PIX Security appliance Version 7.0 image, then press **Enter** at the next prompt to confirm the **reload** command.

```
PixVlan# reload
Proceed with reload? [confirm]
Rebooting..

Wait.....

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  0B  00   1011   0026  PCI-to-PCI Bridge
 00  0D  00   8086   1209  Ethernet           11
 00  0E  00   8086   1209  Ethernet           10
 00  11  00   8086   1229  Ethernet           11
 00  13  00   8086   1229  Ethernet           5
 01  00  00   8086   1229  Ethernet           11
 01  01  00   8086   1229  Ethernet           104.3
 01  02  00   8086   1229  Ethernet           9
 01  03  00   8086   1229  Ethernet           5
Initializing Intel Boot Agent Version 2.2
Initializing Intel Boot Agent Version 2.2ram..
Press Ctrl+S to enter into the Setup Program..
+---------------------------------------+--------------------------------------+
|          System BIOS Configuration, (C) 2000 General Software, Inc.          |
+---------------------------------------+--------------------------------------+
| System CPU           : Pentium III    | Low Memory           : 638KB         |
| Coprocessor          : Enabled        | Extended Memory      : 255MB         |
| Embedded BIOS Date   : 08/25/00       | Serial Ports 1-2     : 03F8 02F8     |
+---------------------------------------+--------------------------------------+

Cisco Secure PIX Firewall BIOS (4.2) #1: Fri Mar 23 04:10:24 PST 2001
Platform PIX-525
System Flash=E28F128J3 @ 0xfff00000

Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Reading 5059072 bytes of image from flash.
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
########################################################
256MB RAM

Total NICs found: 8
mcwa i82559 Ethernet at irq 11  MAC: 0002.b945.b6d2
mcwa i82559 Ethernet at irq 10  MAC: 0002.b945.b6d1
mcwa i82559 Ethernet at irq 11  MAC: 0002.b308.7273
mcwa i82559 Ethernet at irq  5  MAC: 0002.b304.1a35
mcwa i82558 Ethernet at irq 11  MAC: 00e0.b600.d47a
mcwa i82558 Ethernet at irq 10  MAC: 00e0.b600.d479
mcwa i82558 Ethernet at irq  9  MAC: 00e0.b600.d478
mcwa i82558 Ethernet at irq  5  MAC: 00e0.b600.d477
BIOS Flash=e28f400b5t @ 0xd8000
Old file system detected. Attempting to save data in flash


Initializing flashfs...
flashfs[7]: Checking block 0...block number was (-14264)
flashfs[7]: erasing block 0...done.
flashfs[7]: Checking block 1...block number was (12668)
flashfs[7]: erasing block 1...done.
flashfs[7]: Checking block 2...block number was (15104)
flashfs[7]: erasing block 2...done.
flashfs[7]: Checking block 3...block number was (-18577)
flashfs[7]: erasing block 3...done.
flashfs[7]: Checking block 4...block number was (11973)
flashfs[7]: erasing block 4...done.
flashfs[7]: Checking block 5...block number was (-4656)
flashfs[7]: erasing block 5...done.
flashfs[7]: Checking block 6...block number was (-24944)
flashfs[7]: erasing block 6...done.
flashfs[7]: Checking block 7...block number was (23499)
flashfs[7]: erasing block 7...done.
flashfs[7]: Checking block 8...block number was (7137)
flashfs[7]: erasing block 8...done.
flashfs[7]: Checking block 9...block number was (20831)
flashfs[7]: erasing block 9...done.
flashfs[7]: Checking block 10...block number was (6185)
flashfs[7]: erasing block 10...done.
flashfs[7]: Checking block 11...block number was (25501)
```

```
flashfs[7]: erasing block 11...done.
flashfs[7]: Checking block 12...block number was (-5607)
flashfs[7]: erasing block 12...done.
flashfs[7]: Checking block 13...block number was (27450)
flashfs[7]: erasing block 13...done.
flashfs[7]: Checking block 14...block number was (-6772)
flashfs[7]: erasing block 14...done.
flashfs[7]: Checking block 15...block number was (-10286)
flashfs[7]: erasing block 15...done.
flashfs[7]: Checking block 16...block number was (2597)
flashfs[7]: erasing block 16...done.
flashfs[7]: Checking block 17...block number was (30610)
flashfs[7]: erasing block 17...done.
flashfs[7]: Checking block 18...block number was (20305)
flashfs[7]: erasing block 18...done.
flashfs[7]: Checking block 19...block number was (-29480)
flashfs[7]: erasing block 19...done.
flashfs[7]: Checking block 20...block number was (3742)
flashfs[7]: erasing block 20...done.
flashfs[7]: Checking block 21...block number was (10580)
flashfs[7]: erasing block 21...done.
flashfs[7]: Checking block 22...block number was (-2896)
flashfs[7]: erasing block 22...done.
flashfs[7]: Checking block 23...block number was (-812)
flashfs[7]: erasing block 23...done.
flashfs[7]: Checking block 24...block number was (23019)
flashfs[7]: erasing block 24...done.
flashfs[7]: Checking block 25...block number was (-32643)
flashfs[7]: erasing block 25...done.
flashfs[7]: Checking block 26...block number was (25350)
flashfs[7]: erasing block 26...done.
flashfs[7]: Checking block 27...block number was (-4434)
flashfs[7]: erasing block 27...done.
flashfs[7]: Checking block 28...block number was (-25787)
flashfs[7]: erasing block 28...done.
flashfs[7]: Checking block 29...block number was (8591)
flashfs[7]: erasing block 29...done.
flashfs[7]: Checking block 30...block number was (-25606)
flashfs[7]: erasing block 30...done.
flashfs[7]: Checking block 31...block number was (-26665)
flashfs[7]: erasing block 31...done.
flashfs[7]: Checking block 32...block number was (12429)
flashfs[7]: erasing block 32...done.
flashfs[7]: Checking block 33...block number was (18421)
flashfs[7]: erasing block 33...done.
flashfs[7]: Checking block 34...block number was (29655)
flashfs[7]: erasing block 34...done.
flashfs[7]: Checking block 35...block number was (-5147)
flashfs[7]: erasing block 35...done.
flashfs[7]: Checking block 36...block number was (21867)
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 38...block number was (0)
flashfs[7]: erasing block 38...done.
flashfs[7]: Checking block 125...block number was (0)
flashfs[7]: erasing block 125...done.
flashfs[7]: inconsistent sector list, fileid 8, parent_fileid 0
flashfs[7]: 8 files, 3 directories
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 16128000
flashfs[7]: Bytes used: 9728
flashfs[7]: Bytes available: 16118272
flashfs[7]: flashfs fsck took 80 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
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 : 10
Maximum VLANs               : 100
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.

  --------------------------------------------------------------------------
                                 .            .
                                 |            |
                                |||          |||
                              .|| ||.      .|| ||.
                           .:||| | |||:..:||| | |||:.
                            C i s c o  S y s t e m s
  --------------------------------------------------------------------------

Cisco PIX Security Appliance Software Version 7.0(4)

  ****************************** 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

Cryptochecksum(unchanged): 8931adaf a47b3649 c5954e72 212043a1
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 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 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.
```

After Upgrade

Output from the PIX Security appliance Version 7.0 image upgrade includes the assumptions in "Before Upgrade" section on page 4-33, with the following changes:

- Interface information is now grouped
- VLAN information appears as a subinterface of the trunk interface
- Fragment information appears for each VLAN
- Inspect statements are not present for **rsh** and **sqlnet**
- Connectivity established by the PIX Version 6.3(3) configuration is unchanged

After performing the PIX Security appliance Version 7.0 upgrade, enter the **enable** command to enter configuration mode, then enter your password, and finally enter the **show run** command. The output is as follows:

```
PixVlan> enable
Password:
PixVlan# show run
: Saved
:
PIX Version 7.0(4)
names
!
interface Ethernet0
 speed 100
 duplex full
 no nameif
 no security-level
 no ip address
!
interface Ethernet0.10
 vlan 10
 nameif outside
 security-level 0
 ip address 172.16.1.175 255.255.255.0
!
interface Ethernet0.20
 vlan 20
 nameif dmz0
 security-level 20
 ip address 192.168.1.175 255.255.255.0
!
interface Ethernet0.30
 vlan 30
 nameif dmz1
 security-level 30
 ip address 192.168.2.175 255.255.255.0
!
interface Ethernet1
 speed 100
 duplex full
 no nameif
 no security-level
 no ip address
!
interface Ethernet1.40
 vlan 40
 nameif dmz2
 security-level 40
 ip address 192.168.3.175 255.255.255.0
```

```
!
interface Ethernet1.50
 vlan 50
 nameif dmz3
 security-level 50
 ip address 192.168.4.175 255.255.255.0
!
interface Ethernet1.60
 vlan 60
 nameif inside
 security-level 100
 ip address 192.168.6.175 255.255.255.0
!
interface Ethernet2
 speed 100
 duplex full
 nameif intf2
 security-level 4
 no ip address
!
interface Ethernet3
 speed 100
 duplex full
 nameif intf3
 security-level 6
 no ip address
!
interface Ethernet4
 speed 100
 duplex full
 nameif intf4
 security-level 8
 no ip address
!
interface Ethernet5
 shutdown
 nameif intf5
 security-level 10
 no ip address
!
interface Ethernet6
 shutdown
 nameif intf6
 security-level 12
 no ip address
!
interface Ethernet7
 shutdown
 nameif intf7
 security-level 14
 no ip address
!
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PixVlan
boot system flash:/image.bin
ftp mode passive
access-list 1 extended permit ip any host 172.16.1.144
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu dmz2 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
mtu intf6 1500
mtu intf7 1500
mtu dmz0 1500
mtu inside 1500
mtu dmz3 1500
mtu dmz1 1500
no failover
monitor-interface intf2
monitor-interface intf3
monitor-interface intf4
monitor-interface intf5
monitor-interface intf6
monitor-interface intf7
asdm history enable
arp timeout 14400
nat-control
global (outside) 1 172.16.1.101-172.16.1.110
nat (inside) 1 0.0.0.0 0.0.0.0
static (dmz2,outside) 172.16.1.144 192.168.3.144 netmask 255.255.255.255
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 sunrpc 0:10:00
 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0
:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
http server enable
http 192.168.4.0 255.255.255.0 dmz3
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp
no sysopt connection permit-ipsec
telnet timeout 5
ssh timeout 5
ssh version 1
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect netbios
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:8931adafa47b3649c5954e72212043a1
: end
```

```
PixVlan#
```

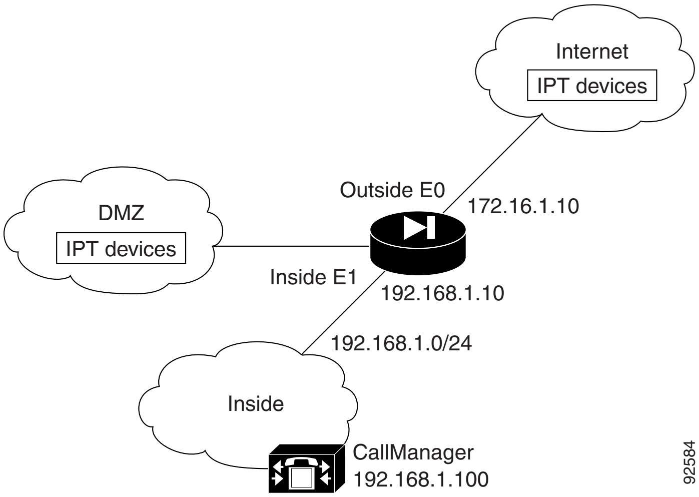
Upgrading to Security Appliance Version 7.0 with Voice Over IP

Assumptions

When performing an upgrade to PIX Security appliance Version 7.0 using Voice over IP, this configuration example assumes the following (see Figure 4):

- IP phones can be located on any interface (inside, outside, dmz)
- The CallManager is located on the inside interface
- NAT is in use, to handle the addressing
- Fixup SKINNY / 2000 is handling dynamic call traffic

Figure 4 Sample Voice over IP Configuration



Before Upgrade

The following is sample output from the **show run** command from your current PIX Version 6.3 configuration before upgrading to PIX Security appliance Version 7.0:

```
Migration# show run
: Saved
 :
 PIX Version 6.3(4)
 interface ethernet0 100full
 interface ethernet1 100full
 interface ethernet2 auto shutdown
 interface ethernet3 auto shutdown
 interface ethernet4 auto shutdown
 interface ethernet5 auto shutdown
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 nameif ethernet2 dmz security50
 nameif ethernet3 intf3 security6
 nameif ethernet4 intf4 security8
 nameif ethernet5 intf5 security10
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname VoipDhcp
 domain-name ciscopix.com
 fixup protocol dns maximum-length 512
 fixup protocol ftp 21
 fixup protocol h323 h225 1720
 fixup protocol h323 ras 1718-1719
 fixup protocol http 80
 <--- More --->

 fixup protocol rsh 514
 fixup protocol rtsp 554
 fixup protocol sip 5060
 fixup protocol sip udp 5060
 fixup protocol skinny 2000
 fixup protocol smtp 25
 fixup protocol sqlnet 1521
 fixup protocol tftp 69
 names
 name 172.16.1.75 Linux
 access-list outside permit udp any host 172.16.1.100 eq tftp
 access-list outside permit tcp any host 172.16.1.100 eq 2000
 access-list dmz permit udp any host 192.168.2.100 eq tftp
 access-list dmz permit tcp any host 192.168.2.100 eq 2000
 pager lines 24
 logging on
 logging trap informational
 logging host inside 192.168.1.99
 icmp permit any outside
 icmp permit any inside
 mtu outside 1500
 mtu inside 1500
 mtu dmz 1500
 mtu intf3 1500
 <--- More --->

 mtu intf4 1500
 mtu intf5 1500
 ip address outside 172.16.1.10 255.255.255.0
 ip address inside 192.168.1.10 255.255.255.0
 ip address dmz 192.168.2.10 255.255.255.0
 no ip address intf3
 no ip address intf4
 no ip address intf5
 ip audit info action alarm
 ip audit attack action alarm
 no failover
 failover timeout 0:00:00
 failover poll 15
 no failover ip address outside
 no failover ip address inside
 no failover ip address dmz
 no failover ip address intf3
 no failover ip address intf4
 no failover ip address intf5
 pdm location 192.168.1.99 255.255.255.255 inside
 pdm history enable
 arp timeout 14400
 global (outside) 1 172.16.1.101-172.16.1.200
 global (dmz) 1 192.168.2.101-192.168.2.200
 <--- More --->
```

```
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,dmz) 192.16.1.100 192.168.1.100 netmask 255.255.255.255 0 0
static (inside,outside) 172.16.1.100 192.168.1.100 netmask 255.255.255.255 0 0
access-group outside in interface outside
access-group dmz in interface dmz
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
http server enable
http 0.0.0.0 0.0.0.0 outside
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
<--- More --->

floodguard enable
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.100-192.168.1.102 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable inside
terminal width 80
Cryptochecksum:a02cd774d0d9c6a3c5f706afc763aee1
: end
```

Upgrade

Enter the **copy tftp://<***ip address***>/pix704.bin.<***image***>flash:image** command to upgrade to the new image. The following output reflects the upgrade procedure from your current PIX Version 6.3 configuration to PIX Security appliance Version 7.0:

```
 VoipDhcp# copy tftp://192.168.1.100/cdisk.7.0(4) flash:image
 copying tftp://192.168.1.100/cdisk.7.0(4) to flash:image

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!
 Received 5124096 bytes
 Erasing current image
 Writing 5062712 bytes of image

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
 Image installed
```

Enter the **reload** command to begin using the new PIX Security appliance Version 7.0 image, then press **Enter** at the next prompt to confirm the **reload** command.

```
VoipDhcp# 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 xxxxxx
 64 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  11  00   14E4   5823  Co-Processor       11
  00  13  00   8086   B154  PCI-to-PCI Bridge
  01  04  00   8086   1229  Ethernet           11
  01  05  00   8086   1229  Ethernet           10
  01  06  00   8086   1229  Ethernet           9
  01  07  00   8086   1229  Ethernet           5


Cisco Secure PIX Firewall BIOS (4.2) #0: Mon Dec 31 08:34:35 PST 2001
Platform PIX-515E
System Flash=E28F128J3 @ 0xfff00000


Use BREAK or ESC to interrupt flash boot.

Use SPACE to begin flash boot immediately.

Flash boot in 10 seconds.           9 seconds.

 Reading 5059072 bytes of image from flash.
```

```
##########################################################################################
##########################################################################################
##########################################################################################
##########################################################################################
##########################################################################################
######
64MB RAM

Total NICs found: 6
mcwa i82559 Ethernet at irq 11  MAC: 0011.937e.0650
mcwa i82559 Ethernet at irq 10  MAC: 0011.937e.064f
mcwa i82559 Ethernet at irq 11  MAC: 000d.88ee.dfa0
mcwa i82559 Ethernet at irq 10  MAC: 000d.88ee.dfa1
mcwa i82559 Ethernet at irq  9  MAC: 000d.88ee.dfa2
mcwa i82559 Ethernet at irq  5  MAC: 000d.88ee.dfa3
BIOS Flash=am29f400b @ 0xd8000
Old file system detected. Attempting to save data in flash


Initializing flashfs...
flashfs[7]: Checking block 0...block number was (-14264)
flashfs[7]: erasing block 0...done.
flashfs[7]: Checking block 1...block number was (12668)
flashfs[7]: erasing block 1...done.
flashfs[7]: Checking block 2...block number was (15104)
flashfs[7]: erasing block 2...done.
flashfs[7]: Checking block 3...block number was (-18577)
flashfs[7]: erasing block 3...done.
flashfs[7]: Checking block 4...block number was (11973)
flashfs[7]: erasing block 4...done.
flashfs[7]: Checking block 5...block number was (-4656)
flashfs[7]: erasing block 5...done.
flashfs[7]: Checking block 6...block number was (-24944)
flashfs[7]: erasing block 6...done.
flashfs[7]: Checking block 7...block number was (23499)
flashfs[7]: erasing block 7...done.
flashfs[7]: Checking block 8...block number was (7137)
flashfs[7]: erasing block 8...done.
flashfs[7]: Checking block 9...block number was (20831)
flashfs[7]: erasing block 9...done.
flashfs[7]: Checking block 10...block number was (6185)
flashfs[7]: erasing block 10...done.
flashfs[7]: Checking block 11...block number was (25501)
flashfs[7]: erasing block 11...done.
flashfs[7]: Checking block 12...block number was (-5607)
flashfs[7]: erasing block 12...done.
flashfs[7]: Checking block 13...block number was (27450)
flashfs[7]: erasing block 13...done.
flashfs[7]: Checking block 14...block number was (-6772)
flashfs[7]: erasing block 14...done.
flashfs[7]: Checking block 15...block number was (-10286)
flashfs[7]: erasing block 15...done.
flashfs[7]: Checking block 16...block number was (2597)
flashfs[7]: erasing block 16...done.
flashfs[7]: Checking block 17...block number was (30610)
flashfs[7]: erasing block 17...done.
flashfs[7]: Checking block 18...block number was (20305)
flashfs[7]: erasing block 18...done.
flashfs[7]: Checking block 19...block number was (-29480)
flashfs[7]: erasing block 19...done.
flashfs[7]: Checking block 20...block number was (3742)
flashfs[7]: erasing block 20...done.
flashfs[7]: Checking block 21...block number was (10580)
flashfs[7]: erasing block 21...done.
```

```
flashfs[7]: Checking block 22...block number was (-2896)
flashfs[7]: erasing block 22...done.
flashfs[7]: Checking block 23...block number was (-812)
flashfs[7]: erasing block 23...done.
flashfs[7]: Checking block 24...block number was (23019)
flashfs[7]: erasing block 24...done.
flashfs[7]: Checking block 25...block number was (-32643)
flashfs[7]: erasing block 25...done.
flashfs[7]: Checking block 26...block number was (25350)
flashfs[7]: erasing block 26...done.
flashfs[7]: Checking block 27...block number was (-4434)
flashfs[7]: erasing block 27...done.
flashfs[7]: Checking block 28...block number was (-25787)
flashfs[7]: erasing block 28...done.
flashfs[7]: Checking block 29...block number was (8591)
flashfs[7]: erasing block 29...done.
flashfs[7]: Checking block 30...block number was (-25606)
flashfs[7]: erasing block 30...done.
flashfs[7]: Checking block 31...block number was (-26665)
flashfs[7]: erasing block 31...done.
flashfs[7]: Checking block 32...block number was (12429)
flashfs[7]: erasing block 32...done.
flashfs[7]: Checking block 33...block number was (18421)
flashfs[7]: erasing block 33...done.
flashfs[7]: Checking block 34...block number was (29655)
flashfs[7]: erasing block 34...done.
flashfs[7]: Checking block 35...block number was (-5147)
flashfs[7]: erasing block 35...done.
flashfs[7]: Checking block 36...block number was (21867)
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 238, parent_fileid 0
flashfs[7]: 230 files, 11 directories
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 16128000
flashfs[7]: Bytes used: 8067584
flashfs[7]: Bytes available: 8060416
flashfs[7]: flashfs fsck took 53 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+ (Crypto5823 revision 0x1)
  --------------------------------------------------------------------------
                                 .            .
                                 |            |
                                |||          |||
                              .|| ||.      .|| ||.
                           .:||| | |||:..:||| | |||:.
                            C i s c o   S y s t e m s
  --------------------------------------------------------------------------

Cisco PIX Security Appliance Software Version 7.0(4)

  ****************************** 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

Cryptochecksum(unchanged): a02cd774 d0d9c6a3 c5f706af c763aee1
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.
```

After Upgrade

After performing the PIX Security appliance Version 7.0 upgrade, enter the **enable** command to enter configuration mode, then enter your password, and finally enter the **show run** command. The output is as follows:

```
VoipDhcp> enable
Password:
VoipDhcp# show run
 : Saved
 :
 PIX Version 7.0(4)
 names
 name 172.16.1.75 Linux
 !
 interface Ethernet0
  speed 100
  duplex full
  nameif outside
  security-level 0
  ip address 172.16.1.10 255.255.255.0
 !
 interface Ethernet1
  speed 100
  duplex full
  nameif inside
  security-level 100
  ip address 192.168.1.10 255.255.255.0
 !
 interface Ethernet2
  shutdown
  nameif dmz
  security-level 50
  ip address 192.168.2.10 255.255.255.0
 <--- More --->
```

```
!
interface Ethernet3
 shutdown
 nameif intf3
 security-level 6
 no ip address
!
interface Ethernet4
 shutdown
 nameif intf4
 security-level 8
 no ip address
!
interface Ethernet5
 shutdown
 nameif intf5
 security-level 10
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname VoipDhcp
domain-name ciscopix.com
boot system flash:/image.bin
<--- More --->

ftp mode passive
access-list outside extended permit udp any host 172.16.1.100 eq tftp
access-list outside extended permit tcp any host 172.16.1.100 eq 2000
access-list dmz extended permit udp any host 192.168.2.100 eq tftp
access-list dmz extended permit tcp any host 192.168.2.100 eq 2000
pager lines 24
logging enable
logging trap informational
logging host inside 192.168.1.99
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
no failover
monitor-interface outside
monitor-interface inside
monitor-interface dmz
monitor-interface intf3
monitor-interface intf4
monitor-interface intf5
icmp permit any outside
icmp permit any inside
<--- More --->

asdm history enable
arp timeout 14400
nat-control
global (outside) 1 172.16.1.101-172.16.1.200
global (dmz) 1 192.168.2.101-192.168.2.200
nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,dmz) 192.16.1.100 192.168.1.100 netmask 255.255.255.255
static (inside,outside) 172.16.1.100 192.168.1.100 netmask 255.255.255.255
access-group outside in interface outside
access-group dmz in interface dmz
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1
timeout xlate 3:00:00
```

```
 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 sunrpc 0:10:00 h323
0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
 timeout uauth 0:05:00 absolute
 aaa-server TACACS+ protocol tacacs+
 aaa-server RADIUS protocol radius
 http server enable
 http 0.0.0.0 0.0.0.0 outside
 http 0.0.0.0 0.0.0.0 inside
 no snmp-server location
 no snmp-server contact
 snmp-server community public
 snmp-server enable traps snmp
 no sysopt connection permit-ipsec
 <--- More --->

 telnet 192.168.1.0 255.255.255.0 inside
 telnet timeout 5
 ssh timeout 5
 ssh version 1
 console timeout 0
 dhcpd address 192.168.1.100-192.168.1.102 inside
 dhcpd lease 3600
 dhcpd ping_timeout 750
 dhcpd enable inside
 !
 class-map inspection_default
  match default-inspection-traffic
 !
 !
 policy-map global_policy
  class inspection_default
   inspect dns maximum-length 512
   inspect ftp
   inspect h323 h225
   inspect h323 ras
   inspect http
   inspect netbios
   inspect rsh
   inspect rtsp
 <--- More --->

   inspect skinny
   inspect esmtp
   inspect sqlnet
   inspect sunrpc
   inspect tftp
   inspect sip
   inspect xdmcp
 !
 service-policy global_policy global
 Cryptochecksum:a02cd774d0d9c6a3c5f706afc763aee1
 : end

 VoipDhcp#
```

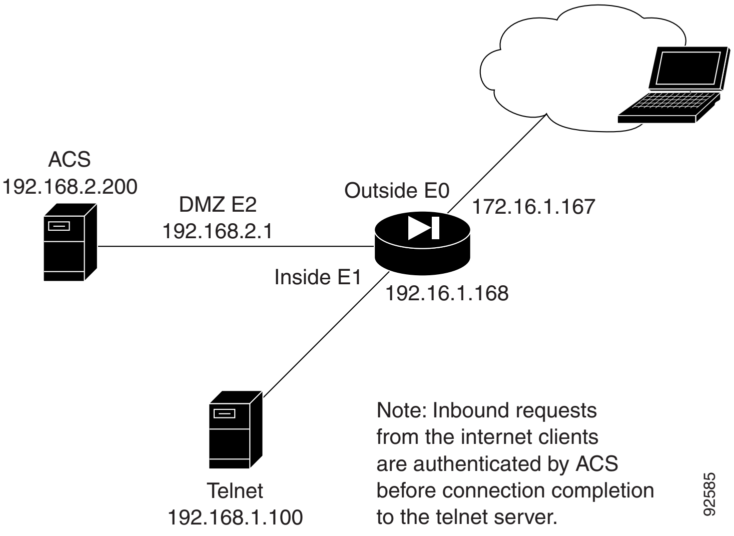
Upgrading to Security Appliance Version 7.0 with Authentication

Assumptions

When performing an upgrade to PIX Security appliance Version 7.0 with authentication, this configuration example assumes the following (see Figure 5):

- PIX with 3 interfaces
- Static inbound interfaces with a local and/or external AAA server
- No NAT
- Several ACLs with a logging option

Figure 5 Sample Authentication Configuration


ACS
192.168.2.200
DMZ E2
192.168.2.1
Outside E0
172.16.1.167
Inside E1
192.16.1.168
Telnet
192.168.1.100
Note: Inbound requests from the internet clients are authenticated by ACS before connection completion to the telnet server.
92585

Before Upgrade

The following is sample output from the **show run** command from your current PIX Version 6.3 configuration before upgrading to PIX Security appliance Version 7.0:

```
auth# show run
: Saved
:
PIX Version 6.3(4)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 100full shutdown
interface ethernet4 100full shutdown
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security20
nameif ethernet3 intf3 security6
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
```

```
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname auth
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list 110 permit ip any host 172.16.1.168 log 7 interval 1
pager lines 24
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
ip address outside 172.16.1.167 255.255.255.0
ip address inside 192.168.1.167 255.255.255.0
ip address dmz 192.168.2.1 255.255.255.0
no ip address intf3
no ip address intf4
no ip address intf5
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address dmz
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 172.16.1.168 192.168.1.100 netmask 255.255.255.255 0 0
access-group 110 in interface outside
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
aaa-server acs32 protocol tacacs+
aaa-server acs32 max-failed-attempts 3
aaa-server acs32 deadtime 10
aaa-server acs32 (dmz) host 192.168.2.200 cisco123 timeout 5
aaa authentication include telnet outside 192.168.1.100 255.255.255.255 0.0.0.0
```

```
0.0.0.0 acs32
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
ssh timeout 5
console timeout 0
username cisco password tLgC3MrTDBA//0RQ encrypted privilege 15
terminal width 80
Cryptochecksum:2c91baf69c09453693157eb911aa842e
: end
```

Upgrade

Enter the **copy tftp://<*ip address*>/pix704.bin.<*image*>flash:image** command to upgrade to the new image. The following output reflects the upgrade procedure from your current PIX Version 6.3 configuration to PIX Security appliance Version 7.0:

```
auth# copy tftp://192.168.1.100/cdisk.7.0(4) flash:image
copying tftp://192.168.1.100/cdisk.7.0(4) to flash:image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Received 5124096 bytes
Erasing current image
Writing 5062712 bytes of image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image installed
```

Enter the **reload** command to begin using the new PIX Security appliance Version 7.0 image, then press **Enter** at the next prompt to confirm the **reload** command.

```
auth# 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 xxxxxx
64 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  11  00   14E4   5823  Co-Processor       11
 00  13  00   8086   B154  PCI-to-PCI Bridge
 01  04  00   8086   1229  Ethernet           11
 01  05  00   8086   1229  Ethernet           10
 01  06  00   8086   1229  Ethernet           9
 01  07  00   8086   1229  Ethernet           5

Cisco Secure PIX Firewall BIOS (4.2) #0: Mon Dec 31 08:34:35 PST 2001
Platform PIX-515E
System Flash=E28F128J3 @ 0xfff00000

Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Reading 5059072 bytes of image from flash.
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
########################################################
64MB RAM

Total NICs found: 6
mcwa i82559 Ethernet at irq 11  MAC: 0011.937e.0650
mcwa i82559 Ethernet at irq 10  MAC: 0011.937e.064f
mcwa i82559 Ethernet at irq 11  MAC: 000d.88ee.dfa0
mcwa i82559 Ethernet at irq 10  MAC: 000d.88ee.dfa1
mcwa i82559 Ethernet at irq  9  MAC: 000d.88ee.dfa2
mcwa i82559 Ethernet at irq  5  MAC: 000d.88ee.dfa3
BIOS Flash=am29f400b @ 0xd8000
Old file system detected. Attempting to save data in flash


Initializing flashfs...
flashfs[7]: Checking block 0...block number was (-14264)
flashfs[7]: erasing block 0...done.
flashfs[7]: Checking block 1...block number was (12668)
flashfs[7]: erasing block 1...done.
flashfs[7]: Checking block 2...block number was (15104)
flashfs[7]: erasing block 2...done.
flashfs[7]: Checking block 3...block number was (-18577)
flashfs[7]: erasing block 3...done.
flashfs[7]: Checking block 4...block number was (11973)
flashfs[7]: erasing block 4...done.
flashfs[7]: Checking block 5...block number was (-4656)
flashfs[7]: erasing block 5...done.
flashfs[7]: Checking block 6...block number was (-24944)
flashfs[7]: erasing block 6...done.
flashfs[7]: Checking block 7...block number was (23499)
flashfs[7]: erasing block 7...done.
```

```
flashfs[7]: Checking block 8...block number was (7137)
flashfs[7]: erasing block 8...done.
flashfs[7]: Checking block 9...block number was (20831)
flashfs[7]: erasing block 9...done.
flashfs[7]: Checking block 10...block number was (6185)
flashfs[7]: erasing block 10...done.
flashfs[7]: Checking block 11...block number was (25501)
flashfs[7]: erasing block 11...done.
flashfs[7]: Checking block 12...block number was (-5607)
flashfs[7]: erasing block 12...done.
flashfs[7]: Checking block 13...block number was (27450)
flashfs[7]: erasing block 13...done.
flashfs[7]: Checking block 14...block number was (-6772)
flashfs[7]: erasing block 14...done.
flashfs[7]: Checking block 15...block number was (-10286)
flashfs[7]: erasing block 15...done.
flashfs[7]: Checking block 16...block number was (2597)
flashfs[7]: erasing block 16...done.
flashfs[7]: Checking block 17...block number was (30610)
flashfs[7]: erasing block 17...done.
flashfs[7]: Checking block 18...block number was (20305)
flashfs[7]: erasing block 18...done.
flashfs[7]: Checking block 19...block number was (-29480)
flashfs[7]: erasing block 19...done.
flashfs[7]: Checking block 20...block number was (3742)
flashfs[7]: erasing block 20...done.
flashfs[7]: Checking block 21...block number was (10580)
flashfs[7]: erasing block 21...done.
flashfs[7]: Checking block 22...block number was (-2896)
flashfs[7]: erasing block 22...done.
flashfs[7]: Checking block 23...block number was (-812)
flashfs[7]: erasing block 23...done.
flashfs[7]: Checking block 24...block number was (23019)
flashfs[7]: erasing block 24...done.
flashfs[7]: Checking block 25...block number was (-32643)
flashfs[7]: erasing block 25...done.
flashfs[7]: Checking block 26...block number was (25350)
flashfs[7]: erasing block 26...done.
flashfs[7]: Checking block 27...block number was (-4434)
flashfs[7]: erasing block 27...done.
flashfs[7]: Checking block 28...block number was (-25787)
flashfs[7]: erasing block 28...done.
flashfs[7]: Checking block 29...block number was (8591)
flashfs[7]: erasing block 29...done.
flashfs[7]: Checking block 30...block number was (-25606)
flashfs[7]: erasing block 30...done.
flashfs[7]: Checking block 31...block number was (-26665)
flashfs[7]: erasing block 31...done.
flashfs[7]: Checking block 32...block number was (12429)
flashfs[7]: erasing block 32...done.
flashfs[7]: Checking block 33...block number was (18421)
flashfs[7]: erasing block 33...done.
flashfs[7]: Checking block 34...block number was (29655)
flashfs[7]: erasing block 34...done.
flashfs[7]: Checking block 35...block number was (-5147)
flashfs[7]: erasing block 35...done.
flashfs[7]: Checking block 36...block number was (21867)
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 240, parent_fileid 0
flashfs[7]: 231 files, 11 directories
```

```
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 16128000
flashfs[7]: Bytes used: 8274944
flashfs[7]: Bytes available: 7853056
flashfs[7]: flashfs fsck took 53 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+ (Crypto5823 revision 0x1)
  --------------------------------------------------------------------------
                               .            .
                               |            |
                              |||          |||
                            .|| ||.      .|| ||.
                         .:||| | |||:..:||| | |||:.
                          C i s c o   S y s t e m s
  --------------------------------------------------------------------------

Cisco PIX Security Appliance Software Version 7.0(4)

  ****************************** 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

Cryptochecksum(unchanged): 2c91baf6 9c094536 93157eb9 11aa842e
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.
```

After Upgrade

After performing the PIX Security appliance Version 7.0 upgrade, enter the **enable** command to enter configuration mode, then enter your password, and finally enter the **show run** command. The output is as follows:

```
auth> enable
```

```
Password:
auth# show run
: Saved
:
PIX Version 7.0(4)
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.16.1.167 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 192.168.1.167 255.255.255.0
!
interface Ethernet2
 nameif dmz
 security-level 20
 ip address 192.168.2.1 255.255.255.0
!
interface Ethernet3
 speed 100
 duplex full
 shutdown
 nameif intf3
 security-level 6
 no ip address
!
interface Ethernet4
 speed 100
 duplex full
 shutdown
 nameif intf4
 security-level 8
 no ip address
!
interface Ethernet5
 shutdown
 nameif intf5
 security-level 10
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname auth
boot system flash:/image.bin
ftp mode passive
access-list 110 extended permit ip any host 172.16.1.168 log debugging interval
1
pager lines 24
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
no failover
monitor-interface outside
monitor-interface inside
monitor-interface dmz
monitor-interface intf3
monitor-interface intf4
```

```
monitor-interface intf5
asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 172.16.1.168 192.168.1.100 netmask 255.255.255.255
access-group 110 in interface outside
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 sunrpc 0:10:00
 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0
:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server acs32 protocol tacacs+
aaa-server acs32 (dmz) host 192.168.2.200
 timeout 5
 key cisco123
username cisco password tLgC3MrTDBA//0RQ encrypted privilege 15
aaa authentication include telnet outside 192.168.1.100 255.255.255.255 0.0.0.0 0.0.0.0
acs32
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp
no sysopt connection permit-ipsec
telnet timeout 5
ssh timeout 5
ssh version 1
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:2c91baf69c09453693157eb911aa842e
: end
auth#
```

Upgrading to Security Appliance Version 7.0 with Active/Standby Failover

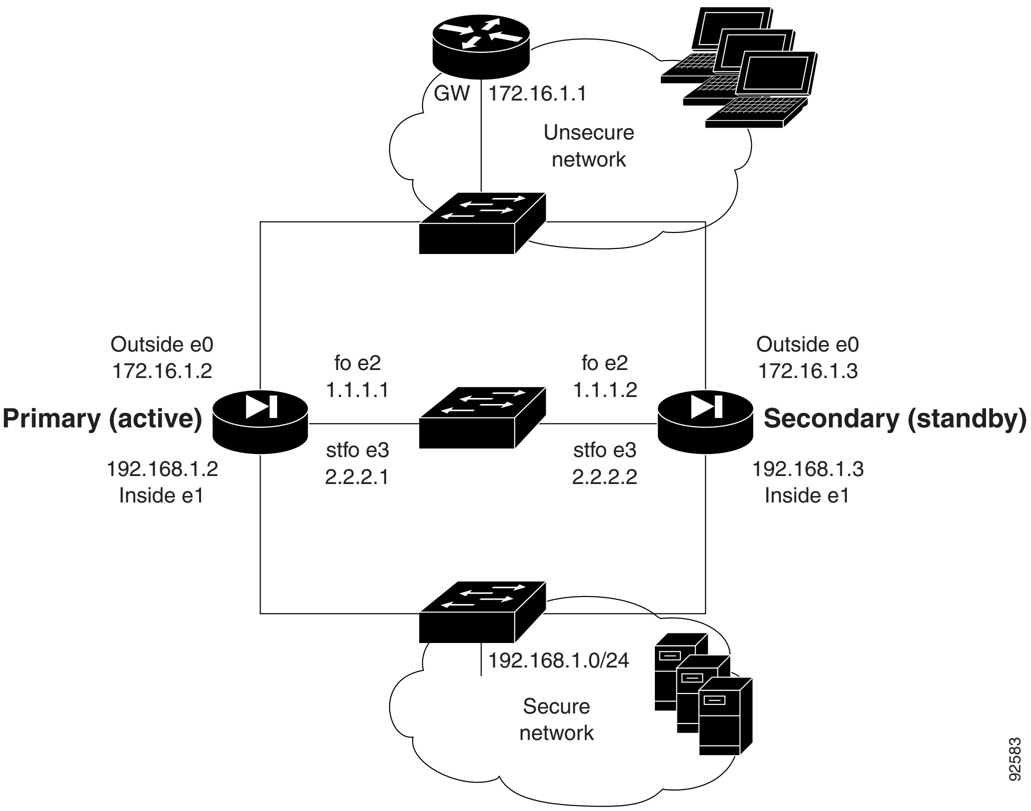
Assumptions

When performing an upgrade to PIX Security appliance Version 7.0 with Active/Standby Failover, this configuration example assumes the following (see Figure 6):

- Two PIX 525 units (4 interfaces each)
- LAN-based and Stateful Failover
- A failover configuration that has completed initialization and is ready for end user configuration (on the primary)

Note The PIX Security appliance Version 7.0 supports use of a crossover or a serial cable for Active/Active failover configurations.

Figure 6 Sample Active/Standby Failover Configuration



Overview

An overview of the upgrade procedure to PIX with an Active/Standby failover configuration follows:

- With a running failover security appliance configuration, log on to the Active PIX Version 6.3
  - Copy TFTP to Flash memory

  - Reboot
  - Enter either the **show version** or **show run** command to display the configuration
- The Standby PIX takes over at reboot; the Active PIX is unavailable
- The Active PIX reboots, converts to the Standby PIX, and restarts; the Standby PIX is still processing traffic
- Log on to the Standby PIX
  - Copy TFTP to Flash memory
  - Reboot (all connections are dropped)
  - Enter either the **show version** or **show run** command to display the configuration
- The Active PIX takes over at reboot of the Standby PIX; this is not a failover because each PIX unit is running a different Cisco IOS software release
- The Standby PIX reboots, converts to the Active PIX, and restarts:
  - The Standby PIX synchronizes with the Active PIX, reestablishing the failover configuration

Alternatively, you can power down the Standby PIX at the same time that you reboot the Active PIX. Then, restart the Standby PIX after the Active PIX begins passing traffic, and perform the upgrade to PIX Security appliance Version 7.0. Preload each PIX, using the **copy tftp** command, then reload the Active PIX. When the Active PIX is almost up, reload the Standby PIX. This minimizes down time.

Upgrading the Active PIX

Enter the **show run** command to display output from your current PIX Version 6.3 configuration on your Active PIX device before upgrading the device to PIX Security appliance Version 7.0. Output from the PIX Version 6.3 configuration follows:

```
failover# show run
: Saved
:
PIX Version 6.3(4)
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
interface ethernet3 100full
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 fo security10
nameif ethernet3 stfo security15
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname failover
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
pager lines 24
mtu outside 1500
mtu inside 1500
mtu fo 1500
mtu stfo 1500
mtu intf4 1500
mtu intf5 1500
ip address outside 172.16.1.2 255.255.255.0
ip address inside 192.168.1.2 255.255.255.0
ip address fo 1.1.1.1 255.255.255.0
ip address stfo 2.2.2.1 255.255.255.0
no ip address intf4
no ip address intf5
ip audit info action alarm
ip audit attack action alarm
failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 172.16.1.3
failover ip address inside 192.168.1.3
failover ip address fo 1.1.1.2
failover ip address stfo 2.2.2.2
no failover ip address intf4
no failover ip address intf5
failover link stfo
failover lan unit primary
failover lan interface fo
failover lan key ********
failover lan enable
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:75b1c49e64e3bef7d24326f49b428776
: end
```

Enter the **show failover** (**sho fail**) command to show the failover operational statistics.

```
failover# show failover
Failover On
Serial Failover Cable status: My side not connected
Reconnect timeout 0:00:00
Poll frequency 15 seconds
Last Failover at: 15:02:59 UTC Sun Mar 6 2005
        This host: Primary - Active
                Active time: 285 (sec)
                Interface outside (172.16.1.2): Normal
                Interface inside (192.168.1.2): Normal
                Interface stfo (2.2.2.1): Normal
                Interface intf4 (0.0.0.0): Link Down (Shutdown)
                Interface intf5 (0.0.0.0): Link Down (Shutdown)
        Other host: Secondary - Standby
                Active time: 0 (sec)
                Interface outside (172.16.1.3): Normal
                Interface inside (192.168.1.3): Normal
                Interface stfo (2.2.2.2): Normal
                Interface intf4 (0.0.0.0): Link Down (Shutdown)
                Interface intf5 (0.0.0.0): Link Down (Shutdown)

Stateful Failover Logical Update Statistics
        Link : stfo
        Stateful Obj    xmit       xerr       rcv        rerr
        General         32         0          31         0
        sys cmd         30         0          31         0
        up time         2          0          0          0
        xlate           0          0          0          0
        tcp conn        0          0          0          0
        udp conn        0          0          0          0
        ARP tbl         0          0          0          0
        RIP Tbl         0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       33
        Xmit Q:         0       1       34

LAN-based Failover is Active
        interface fo (1.1.1.1): Normal, peer (1.1.1.2): Normal
```

Enter the **copy tftp://<*ip address*>/pix704.bin.<*image*>flash:image** command to upgrade to the new image on the Active PIX device. The following output reflects the upgrade procedure from your current PIX Version 6.3 configuration to PIX Security appliance Version 7.0:

```
failover# copy tftp://192.168.1.100/cdisk.7.0(4) flash:image
copying tftp://192.168.1.100/cdisk.7.0(4) to flash:image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Received 5124096 bytes
Erasing current image
Writing 5062712 bytes of image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image installed
```

Enter the **reload** command to begin using the new PIX Security appliance Version 7.0 image on the Active PIX device, then press **Enter** at the next prompt to confirm the **reload** command.

```
failover# 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 xxxxxx
64 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  11  00   14E4   5823  Co-Processor       11
 00  13  00   8086   B154  PCI-to-PCI Bridge
 01  04  00   8086   1229  Ethernet           11
 01  05  00   8086   1229  Ethernet           10
 01  06  00   8086   1229  Ethernet           9
 01  07  00   8086   1229  Ethernet           5

Cisco Secure PIX Firewall BIOS (4.2) #0: Mon Dec 31 08:34:35 PST 2001
Platform PIX-515E
System Flash=E28F128J3 @ 0xfff00000

Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Reading 5059072 bytes of image from flash.
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
########################################################
64MB RAM

Total NICs found: 6
mcwa i82559 Ethernet at irq 11  MAC: 0011.937e.0650
mcwa i82559 Ethernet at irq 10  MAC: 0011.937e.064f
mcwa i82559 Ethernet at irq 11  MAC: 000d.88ee.dfa0
mcwa i82559 Ethernet at irq 10  MAC: 000d.88ee.dfa1
mcwa i82559 Ethernet at irq  9  MAC: 000d.88ee.dfa2
mcwa i82559 Ethernet at irq  5  MAC: 000d.88ee.dfa3
BIOS Flash=am29f400b @ 0xd8000
Old file system detected. Attempting to save data in flash


Initializing flashfs...
flashfs[7]: Checking block 0...block number was (-14264)
flashfs[7]: erasing block 0...done.
flashfs[7]: Checking block 1...block number was (12668)
flashfs[7]: erasing block 1...done.
flashfs[7]: Checking block 2...block number was (15104)
flashfs[7]: erasing block 2...done.
flashfs[7]: Checking block 3...block number was (-18577)
flashfs[7]: erasing block 3...done.
flashfs[7]: Checking block 4...block number was (11973)
flashfs[7]: erasing block 4...done.
flashfs[7]: Checking block 5...block number was (-4656)
flashfs[7]: erasing block 5...done.
flashfs[7]: Checking block 6...block number was (-24944)
flashfs[7]: erasing block 6...done.
flashfs[7]: Checking block 7...block number was (23499)
flashfs[7]: erasing block 7...done.
flashfs[7]: Checking block 8...block number was (7137)
flashfs[7]: erasing block 8...done.
flashfs[7]: Checking block 9...block number was (20831)
flashfs[7]: erasing block 9...done.
flashfs[7]: Checking block 10...block number was (6185)
flashfs[7]: erasing block 10...done.
flashfs[7]: Checking block 11...block number was (25501)
flashfs[7]: erasing block 11...done.
flashfs[7]: Checking block 12...block number was (-5607)
flashfs[7]: erasing block 12...done.
flashfs[7]: Checking block 13...block number was (27450)
flashfs[7]: erasing block 13...done.
flashfs[7]: Checking block 14...block number was (-6772)
flashfs[7]: erasing block 14...done.
flashfs[7]: Checking block 15...block number was (-10286)
flashfs[7]: erasing block 15...done.
flashfs[7]: Checking block 16...block number was (2597)
flashfs[7]: erasing block 16...done.
flashfs[7]: Checking block 17...block number was (30610)
flashfs[7]: erasing block 17...done.
flashfs[7]: Checking block 18...block number was (20305)
flashfs[7]: erasing block 18...done.
flashfs[7]: Checking block 19...block number was (-29480)
flashfs[7]: erasing block 19...done.
flashfs[7]: Checking block 20...block number was (3742)
flashfs[7]: erasing block 20...done.
flashfs[7]: Checking block 21...block number was (10580)
flashfs[7]: erasing block 21...done.
flashfs[7]: Checking block 22...block number was (-2896)
flashfs[7]: erasing block 22...done.
flashfs[7]: Checking block 23...block number was (-812)
flashfs[7]: erasing block 23...done.
flashfs[7]: Checking block 24...block number was (23019)
flashfs[7]: erasing block 24...done.
flashfs[7]: Checking block 25...block number was (-32643)
flashfs[7]: erasing block 25...done.
flashfs[7]: Checking block 26...block number was (25350)
flashfs[7]: erasing block 26...done.
flashfs[7]: Checking block 27...block number was (-4434)
flashfs[7]: erasing block 27...done.
flashfs[7]: Checking block 28...block number was (-25787)
```

```
flashfs[7]: erasing block 28...done.
flashfs[7]: Checking block 29...block number was (8591)
flashfs[7]: erasing block 29...done.
flashfs[7]: Checking block 30...block number was (-25606)
flashfs[7]: erasing block 30...done.
flashfs[7]: Checking block 31...block number was (-26665)
flashfs[7]: erasing block 31...done.
flashfs[7]: Checking block 32...block number was (12429)
flashfs[7]: erasing block 32...done.
flashfs[7]: Checking block 33...block number was (18421)
flashfs[7]: erasing block 33...done.
flashfs[7]: Checking block 34...block number was (29655)
flashfs[7]: erasing block 34...done.
flashfs[7]: Checking block 35...block number was (-5147)
flashfs[7]: erasing block 35...done.
flashfs[7]: Checking block 36...block number was (21867)
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]: relinked orphaned file into the fs as "/lost+found/00240".
flashfs[7]: 230 files, 11 directories
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 16128000
flashfs[7]: Bytes used: 8482304
flashfs[7]: Bytes available: 7645696
flashfs[7]: flashfs fsck took 53 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+ (Crypto5823 revision 0x1)
  --------------------------------------------------------------------------
                                 .            .
                                 |            |
                                |||          |||
                              .|| ||.      .|| ||.
                           .:||| | |||:..:||| | |||:.
                            C i s c o  S y s t e m s
  --------------------------------------------------------------------------

Cisco PIX Security Appliance Software Version 7.0(4)

  ****************************** 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

Cryptochecksum(unchanged): 75b1c49e 64e3bef7 d24326f4 9b428776
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
Type help or '?' for a list of available commands.
```

Enter the **show run** (**sho run**) command to display output from the **failover** command on the Active PIX.

```
failover> enable
Password:
failover# show run
: Saved
::
PIX Version 7.0(4)
names
!
interface Ethernet0
 speed 100
 duplex full
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0 standby 172.16.1.3
!
interface Ethernet1
 speed 100
 duplex full
 nameif inside
 security-level 100
 ip address 192.168.1.2 255.255.255.0 standby 192.168.1.3
!
interface Ethernet2
 description LAN Failover Interface
 speed 100
 duplex full
!
interface Ethernet3
 description STATE Failover Interface
 speed 100
 duplex full
!
interface Ethernet4
 shutdown
 nameif intf4
 security-level 8
 no ip address
!
interface Ethernet5
 shutdown
 nameif intf5
 security-level 10
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname failover
```

```
boot system flash:/image.bin
ftp mode passive
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf4 1500
mtu intf5 1500
no failover
failover lan unit primary
failover lan interface fo Ethernet2
failover lan enable
failover key *****
failover link stfo Ethernet3
failover interface ip fo 1.1.1.1 255.255.255.0 standby 1.1.1.2
failover interface ip stfo 2.2.2.1 255.255.255.0 standby 2.2.2.2
monitor-interface outside
monitor-interface inside
monitor-interface intf4
monitor-interface intf5
asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 sunrpc 0:10:00
 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0
:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp
no sysopt connection permit-ipsec
telnet timeout 5
ssh timeout 5
ssh version 1
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect ils
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
```

```
!
service-policy global_policy global
Cryptochecksum:75b1c49e64e3bef7d24326f49b428776
: end
```

Note Failover is off after the upgrade.

Upgrading the Standby PIX

Note The Active PIX is not detected and is considered failed by the Standby PIX.

Enter the **show run** command to display output from your current PIX Version 6.3 configuration on your Standby PIX device before upgrading the device to PIX Security appliance Version 7.0. Output from the PIX Version 6.3 configuration follows:

```
failover# show run
: Saved
failover# sho run
: Saved
:
PIX Version 6.3(4)
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
interface ethernet3 100full
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 fo security10
nameif ethernet3 stfo security15
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname failover
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
pager lines 24
mtu outside 1500
mtu inside 1500
mtu fo 1500
mtu stfo 1500
mtu intf4 1500
mtu intf5 1500
ip address outside 172.16.1.2 255.255.255.0
ip address inside 192.168.1.2 255.255.255.0
ip address fo 1.1.1.1 255.255.255.0
ip address stfo 2.2.2.1 255.255.255.0
no ip address intf4
no ip address intf5
ip audit info action alarm
ip audit attack action alarm
failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 172.16.1.3
failover ip address inside 192.168.1.3
failover ip address fo 1.1.1.2
failover ip address stfo 2.2.2.2
no failover ip address intf4
no failover ip address intf5
failover link stfo
failover lan unit secondary
failover lan interface fo
failover lan key ********
failover lan enable
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:6d45052a7f1c3d68dd10fa95a152eaa7
: end
```

Enter the **show failover** (**sho fail**) command to show the failover operational statistics for the Standby PIX.

```
failover# show failover
Failover On
Serial Failover Cable status: My side not connected
Reconnect timeout 0:00:00
Poll frequency 15 seconds
Last Failover at: 15:21:09 UTC Sun Mar 6 2005
        This host: Secondary - Active
                Active time: 300 (sec)
                Interface outside (172.16.1.2): Normal (Waiting)
                Interface inside (192.168.1.2): Normal (Waiting)
                Interface stfo (2.2.2.1): Normal (Waiting)
                Interface intf4 (0.0.0.0): Link Down (Shutdown)
                Interface intf5 (0.0.0.0): Link Down (Shutdown)
        Other host: Primary - Standby (Failed)
                Active time: 405 (sec)
                Interface outside (172.16.1.3): Unknown
                Interface inside (192.168.1.3): Unknown
                Interface stfo (2.2.2.2): Unknown
                Interface intf4 (0.0.0.0): Unknown (Shutdown)
                Interface intf5 (0.0.0.0): Unknown (Shutdown)
```

```
Stateful Failover Logical Update Statistics
        Link : stfo
        Stateful Obj    xmit       xerr       rcv        rerr
        General         50         0          50         0
        sys cmd         50         0          48         0
        up time         0          0          2          0
        xlate           0          0          0          0
        tcp conn        0          0          0          0
        udp conn        0          0          0          0
        ARP tbl         0          0          0          0
        RIP Tbl         0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       50
        Xmit Q:         0       1       50

LAN-based Failover is Active
        interface fo (1.1.1.2): Normal, peer (1.1.1.1): Unknown
```

Enter the **copy tftp://<*ip address*>/pix704.bin.<*image*>flash:image** command to upgrade to the new image on the Standby PIX. The following output reflects the upgrade procedure from your current PIX Version 6.3 configuration to PIX Security appliance Version 7.0:

```
failover# copy tftp://192.168.1.100/cdisk.7.0(4) flash:image
copying tftp://192.168.1.100/cdisk.7.0(4) to flash:image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Received 5124096 bytes
Erasing current image
Writing 5062712 bytes of image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image installed
```

Enter the **reload** command to begin using the new PIX Security appliance Version 7.0 image, then press **Enter** at the next prompt to confirm the **reload** command.

```
failover# 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 xxxxxx
64 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  11  00   14E4   5823  Co-Processor       11
 00  13  00   8086   B154  PCI-to-PCI Bridge
 01  04  00   8086   1229  Ethernet           11
 01  05  00   8086   1229  Ethernet           10
 01  06  00   8086   1229  Ethernet           9
 01  07  00   8086   1229  Ethernet           5

Cisco Secure PIX Firewall BIOS (4.2) #0: Mon Dec 31 08:34:35 PST 2001
Platform PIX-515E
System Flash=E28F128J3 @ 0xfff00000

Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Reading 5059072 bytes of image from flash.
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
########################################################
64MB RAM

Total NICs found: 6
mcwa i82559 Ethernet at irq 11  MAC: 0011.937e.0604
mcwa i82559 Ethernet at irq 10  MAC: 0011.937e.0603
mcwa i82559 Ethernet at irq 11  MAC: 000d.88ee.e1c4
mcwa i82559 Ethernet at irq 10  MAC: 000d.88ee.e1c5
mcwa i82559 Ethernet at irq  9  MAC: 000d.88ee.e1c6
mcwa i82559 Ethernet at irq  5  MAC: 000d.88ee.e1c7
BIOS Flash=am29f400b @ 0xd8000
Old file system detected. Attempting to save data in flash


Initializing flashfs...
flashfs[7]: Checking block 0...block number was (-14264)
flashfs[7]: erasing block 0...done.
flashfs[7]: Checking block 1...block number was (12668)
flashfs[7]: erasing block 1...done.
flashfs[7]: Checking block 2...block number was (15104)
flashfs[7]: erasing block 2...done.
flashfs[7]: Checking block 3...block number was (-18577)
flashfs[7]: erasing block 3...done.
flashfs[7]: Checking block 4...block number was (11973)
flashfs[7]: erasing block 4...done.
flashfs[7]: Checking block 5...block number was (-4656)
flashfs[7]: erasing block 5...done.
flashfs[7]: Checking block 6...block number was (-24944)
```

```
flashfs[7]: erasing block 6...done.
flashfs[7]: Checking block 7...block number was (23499)
flashfs[7]: erasing block 7...done.
flashfs[7]: Checking block 8...block number was (7137)
flashfs[7]: erasing block 8...done.
flashfs[7]: Checking block 9...block number was (20831)
flashfs[7]: erasing block 9...done.
flashfs[7]: Checking block 10...block number was (6185)
flashfs[7]: erasing block 10...done.
flashfs[7]: Checking block 11...block number was (25501)
flashfs[7]: erasing block 11...done.
flashfs[7]: Checking block 12...block number was (-5607)
flashfs[7]: erasing block 12...done.
flashfs[7]: Checking block 13...block number was (27450)
flashfs[7]: erasing block 13...done.
flashfs[7]: Checking block 14...block number was (-6772)
flashfs[7]: erasing block 14...done.
flashfs[7]: Checking block 15...block number was (-10286)
flashfs[7]: erasing block 15...done.
flashfs[7]: Checking block 16...block number was (2597)
flashfs[7]: erasing block 16...done.
flashfs[7]: Checking block 17...block number was (30610)
flashfs[7]: erasing block 17...done.
flashfs[7]: Checking block 18...block number was (20305)
flashfs[7]: erasing block 18...done.
flashfs[7]: Checking block 19...block number was (-29480)
flashfs[7]: erasing block 19...done.
flashfs[7]: Checking block 20...block number was (3742)
flashfs[7]: erasing block 20...done.
flashfs[7]: Checking block 21...block number was (10580)
flashfs[7]: erasing block 21...done.
flashfs[7]: Checking block 22...block number was (-2896)
flashfs[7]: erasing block 22...done.
flashfs[7]: Checking block 23...block number was (-812)
flashfs[7]: erasing block 23...done.
flashfs[7]: Checking block 24...block number was (23019)
flashfs[7]: erasing block 24...done.
flashfs[7]: Checking block 25...block number was (-32643)
flashfs[7]: erasing block 25...done.
flashfs[7]: Checking block 26...block number was (25350)
flashfs[7]: erasing block 26...done.
flashfs[7]: Checking block 27...block number was (-4434)
flashfs[7]: erasing block 27...done.
flashfs[7]: Checking block 28...block number was (-25787)
flashfs[7]: erasing block 28...done.
flashfs[7]: Checking block 29...block number was (8591)
flashfs[7]: erasing block 29...done.
flashfs[7]: Checking block 30...block number was (-25606)
flashfs[7]: erasing block 30...done.
flashfs[7]: Checking block 31...block number was (-26665)
flashfs[7]: erasing block 31...done.
flashfs[7]: Checking block 32...block number was (12429)
flashfs[7]: erasing block 32...done.
flashfs[7]: Checking block 33...block number was (18421)
flashfs[7]: erasing block 33...done.
flashfs[7]: Checking block 34...block number was (29655)
flashfs[7]: erasing block 34...done.
flashfs[7]: Checking block 35...block number was (-5147)
flashfs[7]: erasing block 35...done.
flashfs[7]: Checking block 36...block number was (21867)
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]: relinked orphaned file into the fs as "/lost+found/00013".
flashfs[7]: relinked orphaned directory into the fs as "/lost+found/00008".
flashfs[7]: relinked orphaned directory into the fs as "/lost+found/00006".
flashfs[7]: 18 files, 7 directories
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 16128000
flashfs[7]: Bytes used: 2384896
flashfs[7]: Bytes available: 13743104
flashfs[7]: flashfs fsck took 45 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+ (Crypto5823 revision 0x1)
  --------------------------------------------------------------------------
                                 .            .
                                 |            |
                                |||          |||
                              .|| ||.      .|| ||.
                           .:||| | |||:..:||| | |||:.
                            C i s c o  S y s t e m s
  -------------------------------------------------------------------------

Cisco PIX Security Appliance Software Version 7.0(4)

  ****************************** 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


Cryptochecksum(unchanged): 6d45052a 7f1c3d68 dd10fa95 a152eaa7
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
Type help or '?' for a list of available commands.
```

After performing the PIX Security appliance Version 7.0 upgrade on the Standby PIX, enter the **enable** command to enter configuration mode, then enter your password, and finally enter the **show run** (**sho run**) command. The output is as follows:

```
failover> enable
Password:
failover# show run
: Saved

PIX Version 7.0(4)
names
!
interface Ethernet0
 speed 100
 duplex full
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0 standby 172.16.1.3
!
interface Ethernet1
 speed 100
 duplex full
 nameif inside
 security-level 100
 ip address 192.168.1.2 255.255.255.0 standby 192.168.1.3
!
interface Ethernet2
 description LAN Failover Interface
 speed 100
 duplex full
!
interface Ethernet3
 description STATE Failover Interface
 speed 100
 duplex full
!
interface Ethernet4
 shutdown
 nameif intf4
 security-level 8
 no ip address
!
interface Ethernet5
 shutdown
 nameif intf5
 security-level 10
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname failover
boot system flash:/image.bin
ftp mode passive
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf4 1500
mtu intf5 1500
no failover
failover lan unit secondary
failover lan interface fo Ethernet2
failover lan enable
failover key *****
failover link stfo Ethernet3
failover interface ip fo 1.1.1.1 255.255.255.0 standby 1.1.1.2
failover interface ip stfo 2.2.2.1 255.255.255.0 standby 2.2.2.2
monitor-interface outside
monitor-interface inside
monitor-interface intf4
monitor-interface intf5
asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 sunrpc 0:10:00
 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0
:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp
no sysopt connection permit-ipsec
telnet timeout 5
ssh timeout 5
ssh version 1
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect ils
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:6d45052a7f1c3d68dd10fa95a152eaa7
: end
```

Note This completes the PIX Security appliance Version 7.0 upgrade on the Standby PIX. Failover is off after the reboot.

Connecting to the Active PIX

Enter the **show failover** (**sho fail**) command to confirm failover on the Active PIX.

```
failover# show failover
Failover Off
Cable status: My side not connected
Failover unit Primary
Failover LAN Interface: fo Ethernet2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
```

Enable failover on the Active PIX by entering the **configure terminal (conf t)** command; next enter the **failover** command; then enter the **exit** command; and finally enter the **show failover** (**sho failover**) command, as follows:

```
failover# configure terminal
failover(config)# failover
failover(config)# exit

failover# show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: fo Ethernet2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Last Failover at: 15:22:22 UTC Mar 6 2005
        This host: Primary - Negotiation
                Active time: 0 (sec)
                Interface outside (172.16.1.2): No Link (Waiting)
                Interface inside (192.168.1.2): No Link (Waiting)
                Interface intf4 (0.0.0.0): Link Down (Waiting)
                Interface intf5 (0.0.0.0): Link Down (Waiting)
        Other host: Primary - Not Detected
                Active time: 0 (sec)
                Interface outside (172.16.1.3): Unknown (Waiting)
                Interface inside (192.168.1.3): Unknown (Waiting)
                Interface intf4 (0.0.0.0): Unknown (Waiting)
                Interface intf5 (0.0.0.0): Unknown (Waiting)

Stateful Failover Logical Update Statistics
        Link : stfo Ethernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         0          0          0          0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     0          0          0          0
        VPN IPSEC upd   0          0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       0       0
        Xmit Q:         0       0       0
failover#
```

Connecting to the Standby PIX

To enter the connection to the Standby PIX device, enter the **show failover** (**sho fail**) command, as follows:

```
failover(config)# show failover
Failover Off
Cable status: My side not connected
Failover unit Secondary
Failover LAN Interface: fo Ethernet2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
```

Enable failover on the Standby PIX device by entering the **failover** command, as follows:

```
failover(config)# failover
        Detected an Active mate
Beginning configuration replication from mate.
```

Enter the **show failover** (**sho fail**) command, as follows:

```
failover(config)# show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Secondary
Failover End configuration replication from mate.
LAN Interface: fo Ethernet2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Last Failover at: 15:33:17 UTC Mar 6 2005
        This host: Secondary - Sync Config
                Active time: 210 (sec)
                Interface outside (172.16.1.3): Normal (Waiting)
                Interface inside (192.168.1.3): Normal (Waiting)
                Interface intf4 (0.0.0.0): Link Down (Waiting)
                Interface intf5 (0.0.0.0): Link Down (Waiting)
        Other host: Primary - Active
                Active time: 75 (sec)
                Interface outside (172.16.1.2): Unknown (Waiting)
                Interface inside (192.168.1.2): Unknown (Waiting)
                Interface intf4 (0.0.0.0): Unknown (Waiting)
                Interface intf5 (0.0.0.0): Unknown (Waiting)

Stateful Failover Logical Update Statistics
        Link : stfo Ethernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         2          0          2          0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          1          0
        Xlate_Timeout   0          0          0          0
```

```
VPN IKE upd     0          0          0          0
VPN IPSEC upd   0          0          0          0
VPN CTCP upd    0          0          0          0
VPN SDI upd     0          0          0          0
VPN DHCP upd    0          0          0          0

Logical Update Queue Information
                Cur     Max     Total
Recv Q:         0       1       12
Xmit Q:         0       1       2
```

This completes the upgrade procedure on a failover PIX.

Upgrading to Security Appliance Version 7.0 with Conduits

Note Conduit and outbound statements must be converted to access control list (**access-list**) commands before performing an upgrade to PIX Security appliance Version 7.0. See the "Conduits and Outbounds" section on page 3-11 before proceeding. Failure to do so will output errors.

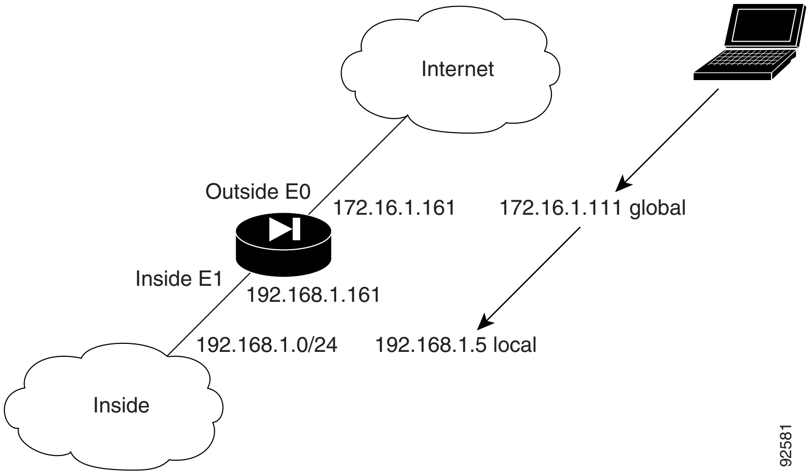
The configuration example in the "After Upgrade" section on page 4-92 displays missing conduit and outbound statements, which have been converted to access control lists.

Assumptions

When performing an upgrade to PIX Security appliance Version 7.0 from PIX Version 6.3 with **conduit** commands, this configuration example assumes the following (see Figure 7):

- Inside users on any network can create **outbound** commands to the Internet
- A web server is located on the inside interface at 192.168.1.5, accessed via **conduit** and **static** commands for web services
- An email server on the inside interface at 172.16.1.49, accessed via **conduit** commands, which only accepts connections from 209.165.201.2
- ICMP messages can freely flow across the PIX via a **conduit** command

Figure 7 Sample Conduits Configuration



Before Upgrade

The following is sample output from the **show run** command from your current PIX Version 6.3 configuration before upgrading to PIX Security appliance Version 7.0:

```
failover# show run
: Saved
 :
 PIX Version 6.3(4)
 interface ethernet0 100full
 interface ethernet1 100full
 interface ethernet2 auto shutdown
 interface ethernet3 auto shutdown
 interface ethernet4 auto shutdown
 interface ethernet5 auto shutdown
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 nameif ethernet2 dmz security50
 nameif ethernet3 intf3 security6
 nameif ethernet4 intf4 security8
 nameif ethernet5 intf5 security10
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname Conduit
 domain-name ciscopix.com
 fixup protocol dns maximum-length 512
 fixup protocol ftp 21
 fixup protocol h323 h225 1720
 fixup protocol h323 ras 1718-1719
 fixup protocol http 80
 fixup protocol rsh 514
 fixup protocol rtsp 554
 fixup protocol sip 5060
 fixup protocol sip udp 5060
 fixup protocol skinny 2000
 fixup protocol smtp 25
 fixup protocol sqlnet 1521
 fixup protocol tftp 69
 names
 name 172.16.1.75 Linux
```

```
no pager
logging on
logging trap informational
logging host inside 192.168.1.99
icmp permit any outside
icmp permit any inside
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
ip address outside 172.16.1.161 255.255.255.0
ip address inside 192.168.1.161 255.255.255.0
no ip address dmz
no ip address intf3
no ip address intf4
no ip address intf5
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address dmz
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
pdm location 192.168.1.99 255.255.255.255 inside
pdm history enable
arp timeout 14400
global (outside) 1 172.16.1.210-172.16.1.212
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 172.16.1.111 192.168.1.5 netmask 255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp host 172.16.1.111 eq www any
conduit permit tcp host 172.16.1.49 eq smtp host 209.165.201.2
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
http server enable
http 0.0.0.0 0.0.0.0 outside
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.100-192.168.1.102 inside
dhcpd lease 3600
```

```
 dhcpd ping_timeout 750
 dhcpd enable inside
 terminal width 80
 Cryptochecksum:629e8fc8b6e635161c253178e5d91814
 : end
```

Upgrade

Enter the **copy tftp://<*ip address*>/pix704.bin.<*image*>flash:image** command to upgrade to the new image. The following output reflects the upgrade procedure from your current PIX Version 6.3 configuration to PIX Security appliance Version 7.0:

```
Conduit# copy tftp://192.168.1.100/cdisk.7.0(4) flash:image
copying tftp://192.168.1.100/cdisk.7.0(4) to flash:image

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!
 Received 5124096 bytes
 Erasing current image
 Writing 5062712 bytes of image

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
 Image installed
```

Enter the **reload** command to begin using the new PIX Security appliance Version 7.0 image, then press **Enter** at the next prompt to confirm the **reload** command.

```
Conduit# 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 xxxxxx
 64 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  11  00   14E4   5823  Co-Processor        11
  00  13  00   8086   B154  PCI-to-PCI Bridge
  01  04  00   8086   1229  Ethernet            11
  01  05  00   8086   1229  Ethernet            10
  01  06  00   8086   1229  Ethernet            9
  01  07  00   8086   1229  Ethernet            5


Cisco Secure PIX Firewall BIOS (4.2) #0: Mon Dec 31 08:34:35 PST 2001
Platform PIX-515E
System Flash=E28F128J3 @ 0xfff00000


Use BREAK or ESC to interrupt flash boot.

Use SPACE to begin flash boot immediately.

Flash boot in 10 seconds.           9 seconds.          8 seconds.

 Reading 5059072 bytes of image from flash.

###########################################################################################
###########################################################################################
###########################################################################################
###########################################################################################
###########################################################################################
######
64MB RAM

Total NICs found: 6
mcwa i82559 Ethernet at irq 11  MAC: 0011.937e.0650
mcwa i82559 Ethernet at irq 10  MAC: 0011.937e.064f
mcwa i82559 Ethernet at irq 11  MAC: 000d.88ee.dfa0
mcwa i82559 Ethernet at irq 10  MAC: 000d.88ee.dfa1
mcwa i82559 Ethernet at irq  9  MAC: 000d.88ee.dfa2
mcwa i82559 Ethernet at irq  5  MAC: 000d.88ee.dfa3
BIOS Flash=am29f400b @ 0xd8000
Old file system detected. Attempting to save data in flash


Initializing flashfs...
flashfs[7]: Checking block 0...block number was (-14264)
flashfs[7]: erasing block 0...done.
flashfs[7]: Checking block 1...block number was (12668)
flashfs[7]: erasing block 1...done.
flashfs[7]: Checking block 2...block number was (15104)
flashfs[7]: erasing block 2...done.
flashfs[7]: Checking block 3...block number was (-18577)
flashfs[7]: erasing block 3...done.
flashfs[7]: Checking block 4...block number was (11973)
flashfs[7]: erasing block 4...done.
flashfs[7]: Checking block 5...block number was (-4656)
flashfs[7]: erasing block 5...done.
flashfs[7]: Checking block 6...block number was (-24944)
flashfs[7]: erasing block 6...done.
flashfs[7]: Checking block 7...block number was (23499)
flashfs[7]: erasing block 7...done.
```

```
flashfs[7]: Checking block 8...block number was (7137)
flashfs[7]: erasing block 8...done.
flashfs[7]: Checking block 9...block number was (20831)
flashfs[7]: erasing block 9...done.
flashfs[7]: Checking block 10...block number was (6185)
flashfs[7]: erasing block 10...done.
flashfs[7]: Checking block 11...block number was (25501)
flashfs[7]: erasing block 11...done.
flashfs[7]: Checking block 12...block number was (-5607)
flashfs[7]: erasing block 12...done.
flashfs[7]: Checking block 13...block number was (27450)
flashfs[7]: erasing block 13...done.
flashfs[7]: Checking block 14...block number was (-6772)
flashfs[7]: erasing block 14...done.
flashfs[7]: Checking block 15...block number was (-10286)
flashfs[7]: erasing block 15...done.
flashfs[7]: Checking block 16...block number was (2597)
flashfs[7]: erasing block 16...done.
flashfs[7]: Checking block 17...block number was (30610)
flashfs[7]: erasing block 17...done.
flashfs[7]: Checking block 18...block number was (20305)
flashfs[7]: erasing block 18...done.
flashfs[7]: Checking block 19...block number was (-29480)
flashfs[7]: erasing block 19...done.
flashfs[7]: Checking block 20...block number was (3742)
flashfs[7]: erasing block 20...done.
flashfs[7]: Checking block 21...block number was (10580)
flashfs[7]: erasing block 21...done.
flashfs[7]: Checking block 22...block number was (-2896)
flashfs[7]: erasing block 22...done.
flashfs[7]: Checking block 23...block number was (-812)
flashfs[7]: erasing block 23...done.
flashfs[7]: Checking block 24...block number was (23019)
flashfs[7]: erasing block 24...done.
flashfs[7]: Checking block 25...block number was (-32643)
flashfs[7]: erasing block 25...done.
flashfs[7]: Checking block 26...block number was (25350)
flashfs[7]: erasing block 26...done.
flashfs[7]: Checking block 27...block number was (-4434)
flashfs[7]: erasing block 27...done.
flashfs[7]: Checking block 28...block number was (-25787)
flashfs[7]: erasing block 28...done.
flashfs[7]: Checking block 29...block number was (8591)
flashfs[7]: erasing block 29...done.
flashfs[7]: Checking block 30...block number was (-25606)
flashfs[7]: erasing block 30...done.
flashfs[7]: Checking block 31...block number was (-26665)
flashfs[7]: erasing block 31...done.
flashfs[7]: Checking block 32...block number was (12429)
flashfs[7]: erasing block 32...done.
flashfs[7]: Checking block 33...block number was (18421)
flashfs[7]: erasing block 33...done.
flashfs[7]: Checking block 34...block number was (29655)
flashfs[7]: erasing block 34...done.
flashfs[7]: Checking block 35...block number was (-5147)
flashfs[7]: erasing block 35...done.
flashfs[7]: Checking block 36...block number was (21867)
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]: relinked orphaned file into the fs as "/lost+found/00233".
flashfs[7]: relinked orphaned directory into the fs as "/lost+found/00229".
```

```
flashfs[7]: 224 files, 9 directories
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 16128000
flashfs[7]: Bytes used: 8061952
flashfs[7]: Bytes available: 8066048
flashfs[7]: flashfs fsck took 53 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+ (Crypto5823 revision 0x1)
  --------------------------------------------------------------------------
                                 .            .
                                 |            |
                                |||          |||
                              .|| ||.      .|| ||.
                           .:||| | |||:..:||| | |||:.
                            C i s c o  S y s t e m s
  --------------------------------------------------------------------------

Cisco PIX Security Appliance Software Version 7.0(4)

  ****************************** 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

Cryptochecksum(unchanged): 629e8fc8 b6e63516 1c253178 e5d91814
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.
```

After Upgrade

Note The configuration example in this section displays missing conduit and outbound statements; they have been converted to access control lists.

After performing the PIX Security appliance Version 7.0 upgrade, enter the **enable** command to enter configuration mode, then enter your password, and finally enter the **show run** command. The output is as follows:

```
Conduit> enable
Password:

Conduit# show run

: Saved
 :
 PIX Version 7.0(4)
 names
 name 172.16.1.75 Linux
 !
 interface Ethernet0
  speed 100
  duplex full
  nameif outside
  security-level 0
  ip address 172.16.1.161 255.255.255.0
 !
 interface Ethernet1
  speed 100
  duplex full
  nameif inside
  security-level 100
  ip address 192.168.1.161 255.255.255.0
 !
 interface Ethernet2
  shutdown
  nameif dmz
  security-level 50
  no ip address
 !
 interface Ethernet3
  shutdown
  nameif intf3
  security-level 6
  no ip address
 !
 interface Ethernet4
  shutdown
  nameif intf4
  security-level 8
  no ip address
 !
 interface Ethernet5
  shutdown
  nameif intf5
  security-level 10
  no ip address
 !
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
```

```
hostname Conduit
domain-name ciscopix.com
boot system flash:/image.bin
ftp mode passive
no pager
logging enable
logging trap informational
logging host inside 192.168.1.99
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
no failover
monitor-interface outside
monitor-interface inside
monitor-interface dmz
monitor-interface intf3
monitor-interface intf4
monitor-interface intf5
icmp permit any outside
icmp permit any inside
asdm history enable
arp timeout 14400
nat-control
global (outside) 1 172.16.1.210-172.16.1.212
nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 172.16.1.111 192.168.1.5 netmask 255.255.255.255
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 sunrpc 0:10:00 h323
0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
http server enable
http 0.0.0.0 0.0.0.0 outside
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp
no sysopt connection permit-ipsec
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 5
ssh timeout 5
ssh version 1
console timeout 0
dhcpd address 192.168.1.100-192.168.1.102 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable inside
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:629e8fc8b6e635161c253178e5d91814
: end

Conduit#
```