Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco Security Appliance Software Version 7.0

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco Security Appliance Software Version 7.0

CONTENTS

About This Guide ix

Obtaining Documentation and Submitting a Service Request ix

CHAPTER 1 **Before You Begin** 1-1

CHAPTER 2 **New Features** 2-1

Advanced Firewall Services 2-1

Voice over IP and Mutlimedia Security Services 2-2

Robust IPSec VPN Services 2-2

Resilient Architecture 2-2

Intelligent Networking Services 2-2

Flexible Management Solutions 2-3

CHAPTER 3 **Changed and Deprecated Features and Commands** 3-1

Overview 3-2

Changes at a Glance 3-2

Changed and Deprecated Commands 3-3

CLI Command Processor 3-6

Affected Commands 3-6

Upgrade Requirements 3-6

Change Impact 3-6

Operational Changes 3-7

Context-Sensitive Help Changes 3-8

Command Syntax Checking 3-8

Mode Navigation and Terminology Changes 3-9

Licenses 3-10

Conduits and Outbounds 3-11

Affected Commands 3-11

Upgrade Requirements 3-11

Change Impact 3-11

Converting conduit Commands to access-list Commands 3-12

Converting outbound Commands to access-list Commands 3-13

Converting outbound Commands Applied to outgoing_src to access-list Commands 3-14

Converting outbound Commands Applied to outgoing_dest to access-list Commands 3-15

Converting outbound Commands Applied to both outgoing_src and outgoing_dest to access-list Commands 3-16
Fixups/Inspect 3-17
Affected Commands 3-18
Upgrade Requirements 3-18
Command Change Description 3-18
fixup 3-18
Change Impact 3-20
Interfaces 3-23
Affected Commands 3-23
Command Change Description 3-23
Upgrade Requirements 3-25
Change Impact 3-25
Access Control Lists (ACLs) 3-25
Affected Commands 3-26
Upgrade Requirements 3-26
Command Change Description 3-26
access-list 3-26
Change Impact 3-26
VPN 3-27
Affected Commands 3-27
Upgrade Requirements 3-28
Command Change Description 3-28
crypto ipsec 3-30
crypto map 3-31
isakmp 3-32
vpdn 3-33
vpngroup 3-35
Change Impact 3-37
Failover 3-39
Important Notes 3-39
Affected Commands 3-40
Upgrade Requirements 3-40
Command Change Description 3-40
failover 3-40
Change Impact 3-40
AAA 3-41
Affected Commands 3-42
Upgrade Requirements 3-42

Command Change Description 3-42
aaa-server 3-43
auth-prompt 3-43
floodguard 3-43
Change Impact 3-44
Management 3-45
Affected Commands 3-45
Upgrade Requirements 3-45
Command Change Description 3-45
copy 3-46
dhcpd 3-46
pager 3-46
ssh 3-46
telnet 3-47
tftp-server 3-47
Change Impact 3-47
OSPF 3-48
Affected Commands 3-48
Upgrade Requirements 3-48
Command Change Description 3-49
Change Impact 3-49
Media Gateway Control Protocol (MGCP) 3-49
Affected Commands 3-50
Upgrade Requirements 3-50
Configuring class-map, mgcp-map and policy-map for MGCP 3-50
Multicast 3-51
Background 3-51
Affected Commands 3-52
Upgrade Requirements 3-52
Command Change Description 3-52
mroute 3-52
igmp max-groups 3-52
multicast 3-52
Change Impact 3-53
mroute 3-53
igmp max-groups 3-53
multicast 3-53
NAT 3-54
NAT Control 3-54

Connection Limits 3-54
Reverse-Path Forwarding Check 3-55
Public Key Infrastructure (PKI) 3-55
Affected Commands 3-56
Upgrade Requirements 3-57
Command Change Description 3-57
ca generate/ ca zeroize 3-57
ca identify/ ca configure 3-58
ca authenticate 3-58
ca enroll 3-58
ca crl 3-58
ca subject-name 3-59
ca save all 3-59
ca verifycertdn 3-59
Change Impact 3-59
Miscellaneous 3-59
Affected Commands 3-60
Upgrade Requirements 3-60
Command Change Description 3-60
established 3-60
flashfs 3-61
sysopt 3-61
Change Impact 3-61

CHAPTER 4 **Upgrading** 4-1

Prerequisites to Upgrading 4-1
Minimum Hardware Requirements 4-1
Minimum Software Requirements 4-2
Minimum Memory Requirements 4-2
Client PC Operating System and Browser Requirements 4-3
Minimum Connectivity Requirements 4-4
Upgrade Procedure 4-4
Important Notes 4-4
Basic Upgrade Procedure 4-5
Upgrading in Monitor Mode 4-9
Important Notes 4-9
Procedure 4-9
Upgrade Examples 4-12
Basic Upgrade from PIX Version 6.3 to Security Appliance Version 7.0 4-12

Assumptions 4-12
Before Upgrade 4-13
Upgrade 4-15
After Upgrade 4-19
Upgrading to a VPN Client with Remote Access 4-22
Assumptions 4-22
Before Upgrade 4-22
Upgrade 4-24
After Upgrade 4-29
Upgrading to Security Appliance Version 7.0 Using VLAN 4-32
Assumptions 4-32
Before Upgrade 4-33
Upgrade 4-35
After Upgrade 4-40
Upgrading to Security Appliance Version 7.0 with Voice Over IP 4-43
Assumptions 4-43
Before Upgrade 4-43
Upgrade 4-45
After Upgrade 4-50
Upgrading to Security Appliance Version 7.0 with Authentication 4-53
Assumptions 4-53
Before Upgrade 4-53
Upgrade 4-55
After Upgrade 4-59
Upgrading to Security Appliance Version 7.0 with Active/Standby Failover 4-62
Assumptions 4-62
Overview 4-62
Upgrading the Active PIX 4-63
Upgrading the Standby PIX 4-73
Upgrading to Security Appliance Version 7.0 with Conduits 4-84
Assumptions 4-84
Before Upgrade 4-85
Upgrade 4-87
After Upgrade 4-92

CHAPTER 5 **Downgrade Procedure** 5-1
Guidelines for Downgrading 5-1
Downgrade Procedure 5-1
Downgrading Examples 5-3

Example of a Downgrade Procedure 5-4
Example with a Zero Actkey 5-9
Example with No Actkey in the Source Image 5-9
Example to Abort the Downgrade at the Final Prompt 5-9
Example Using an Invalid Actkey 5-9
Example Without Specifying an Actkey and No 4-Tuple Actkey Stored in Flash 5-10
Example Using a Security Appliance Version 7.0 5-10
Example Using an Image with No Verified Actkey 5-10
Example Using a Flash 4-Tuple Key without All the Features of the Current 5-Tuple Key 5-11
Example Where the Entered Actkey Does Not Have the Features of the Current 5-Tuple Key 5-11

CHAPTER 6 **Syslog Message Changes and Deletions** 6-1
Changed Syslog Messages 6-1
Deleted Syslog Messages 6-2

About This Guide

Revised: May 15, 2012

This guide describes how to upgrade from Cisco PIX Version 6.3 or 6.2 to Cisco PIX Security appliance Version 7.0. The upgrade to PIX Security appliance Version 7.0 is generally seamless, and requires little manual intervention on your part. This guide describes the changed and deprecated features and commands in detail. Examples of these changes are also included. New features added in PIX Security appliance Version 7.0 are briefly introduced in this guide.

The target audience for this guide is a security appliance administrator with an understanding of CLI commands and features, and experience configuring PIX.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

CHAPTER 1

Before You Begin

Caution You must review the "Prerequisites to Upgrading" section on page 4-1 and the "Upgrade Procedure" section on page 4-4 in this guide before downloading PIX Security appliance Version 7.0 to your security appliance. Failure to do so may result in installation failures.

- The PIX Security appliance Version 7.0 runs on PIX 515/515E, PIX 525, and PIX 535, but is not supported on the PIX 501 or PIX 506/506E platforms at this time.
- PIX 515/515E systems shipped before the general availability of PIX Security appliance Version 7.0 require a mandatory memory upgrade. See the "Minimum Memory Requirements" section on page 4-2 section for more information.
- Sharing a Stateful Failover interface with a regular firewall interface is not a supported configuration in PIX Security appliance Version 7.0. This restriction was true for PIX Version 6.3 and earlier versions, however, it was not enforced by the software. It is enforced in PIX Security appliance Version 7.0. If you do not have a dedicated interface for the Stateful Failover link, you must change your PIX Version 6.3 configuration manually before upgrading to PIX Security appliance Version 7.0. Failure to do so will result in errors during the configuration upgrade performed by PIX Security appliance Version 7.0. See the "Failover" section on page 3-39.
- 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. See the "Upgrading in Monitor Mode" section on page 4-9.
- Unless otherwise specified, all references in this guide that apply to PIX Version 6.3 also apply to PIX Version 6.2.
- PDM does not run on PIX Version 7.0. You must upgrade the device manager to ASDM 5.0. See the ASDM release notes for information about installing ASDM on the security appliance.

CHAPTER 2

New Features

This chapter includes an at-a-glance look at the new features. For more information on these features in PIX Security appliance Version 7.0 and their accompanying CLI commands, see the following documents:

- *Cisco PIX Security Appliance Command Reference, Version 7.0*
- *Cisco Security Appliance CLI Configuration Guide, Version 7.0*
- *Cisco ASA 5500 Series Release Notes*
- Adaptive Security Device Manager Online Help (previously known as PIX Device Manager, or PDM)

The PIX Security appliance Version 7.0 introduces the following new features:

Advanced Firewall Services

- Cisco Modular Policy Framework
- Advanced Web Security Services
- Tunneling Application Control
- Security Contexts
- Layer 2 Transparent Firewall
- FTP Session Command Filtering
- Extended Simple Mail Transport
- Protocol (ESMTP) Email Inspection Services
- 3G Mobile Wireless Security Services
- Sun RPC/NIS+ Inspection Services
- Internet Control Message Protocol (ICMP) Inspection Services
- Enhanced TCP Security Engine
- Outbound Access Control Lists (ACLs)
- Time-based ACLs
- Enable/Disable Individual ACL Entries
- Improved Websence URL Filtering Performance

Voice over IP and Mutlimedia Security Services

- T.38 Fax over IP (FoIP)
- Gatekeeper Routed Control Signaling (GKRCS)
- Fragmented and Segmented Multimedia Stream Inspection
- MGCP Address Translation Services
- RTSP Address Translation Services

Robust IPSec VPN Services

- VPN Client Security Posture Enforcement
- VPN Client Blocking by Operating System and Type
- Automatic VPN Client Software Updates
- Improved Support for Non-Split Tunneling Remote Access VPN Environments
- Enhanced VPN NAT Transparency
- Native Integration with Popular User Authentication Services
- OSPF Dynamic Routing over VPN Tunnels
- Enhanced Spoke-to-Spoke VPN Support
- Enhanced X.509 Certificate Support
- Cisco IOS Software Certificate Authority Support

Resilient Architecture

- Active/Active Stateful Failover
- VPN Stateful Failover
- Improved Failover Transition Times
- Zero-Downtime Software Upgrades

Intelligent Networking Services

- PIM Multicast Routing
- QoS Services
- IPv6 Networking
- Common Security Level for Multiple Interfaces
- Improved VLAN Capacity
- Optional Address Translation Services

Flexible Management Solutions

- Improved SNMP Monitoring
- SSHv2 and Secure Copy Protocol (SCP)
- Storage of Multiple Configurations in Flash Memory
- Secure Asset Recovery
- Scheduled System Reloads
- Dedicated Out-of-Band Management Interface
- Enhanced ICMP Ping Services
- Command Line Interface (CLI) Usability Enhancements
- SMTP Email Alerts
- Administrative TACACS+ Accounting
- RADIUS Accounting to Multiple Servers

CHAPTER 3

Changed and Deprecated Features and Commands

This chapter describes the changed and deprecated features and commands in detail.

Note The automatic conversion of commands results in a change in your configuration. You should review the configuration changes made by PIX Security appliance Version 7.0 after booting to verify that the automatic changes made by the software are satisfactory. You should then save the configuration to Flash memory. Saving the new configuration to Flash memory prevents the system from converting your configuration again the next time PIX Security appliance Version 7.0 is booted.

Many existing CLI commands have been extended with new keywords and other command line options, due to new functionality introduced in PIX Security appliance Version 7.0.

The changed and deprecated features are as follows:

- Overview, page 3-2
- CLI Command Processor, page 3-6
- Licenses, page 3-10
- Conduits and Outbounds, page 3-11
- Fixups/Inspect, page 3-17
- Interfaces, page 3-23
- Access Control Lists (ACLs), page 3-25
- VPN, page 3-27
- Failover, page 3-39
- AAA, page 3-41
- Management, page 3-45
- OSPF, page 3-48
- Media Gateway Control Protocol (MGCP), page 3-49
- Multicast, page 3-51
- NAT, page 3-54
- Public Key Infrastructure (PKI), page 3-55
- Miscellaneous, page 3-59

Overview

As a result of extensive enhancements and improvements made in PIX Security appliance Version 7.0, a number of existing CLI commands have been changed or deprecated (see Table 1). The PIX Security appliance Version 7.0 also includes over 50 new features, which are listed in Chapter 2, "New Features,", and described in greater detail in other PIX Security appliance Version 7.0 documents.

Deprecated commands generally are automatically converted to the new syntax. The PIX Security appliance Version 7.0 then accepts only the new commands; a syntax error results when using the old commands.

Changes at a Glance

Highlights of the changes in the PIX Security appliance Version 7.0 include:

- New minimum memory requirements for PIX 515/515E devices (see the "Upgrade Procedure" section on page 4-4).
- The **fixup** command has been deprecated and has been replaced with the **inspect** command. (see the "Fixups/Inspect" section on page 3-17).
- Support has been removed for the **outbound** and **conduit** commands (see the "Conduits and Outbounds" section on page 3-11).
- The operation of the **no**, **clear**, and **show** commands has changed significantly (see the "CLI Command Processor" section on page 3-6).
- Access lists no longer need to be compiled, affecting the **access-list** <*id*> **compiled**, **access-list compiled** commands (see the "Access Control Lists (ACLs)" section on page 3-25).
- The **aaa-server** command has added two new configuration modes: **key** and **timeout** (see "AAA" section on page 3-41).
- The **interface** command and the **isakmp**, **crypto-map**, and **vpngroup** commands have been enhanced to be hierarchical (see the "Interfaces" section on page 3-23 and the "VPN" section on page 3-27).
- The **failover** command has changed to create more uniformity within the command (see the "Failover" section on page 3-39).
- Commands, such as the AAA, have changed to allow configuration of more specific parameters (see the "AAA" section on page 3-41).
- The **mgcp** command has moved under the **mgcp-map** command (see the "Media Gateway Control Protocol (MGCP)" section on page 3-49).
- The **copy** command applies to the new Flash filesystem; the syntax has changed, with the **copy** options now at the beginning of the command, instead of at the end. (See the "Management" section on page 3-45).
- Configuration modes have been introduced to the **interface** command, with interface-specific OSPF parameters now configured in **interface** configuration mode (see the "OSPF" section on page 3-48).
- Multicast commands have changed to accommodate PIM Sparse Mode (PIM-SM) and to align the PIX Security appliance Version 7.0 and Cisco IOS software multicast implementations (see the "Multicast" section on page 3-51).
- The PIX Security appliance Version 7.0 default NAT posture allows hosts on high security interfaces to communicate with low security interfaces without configuring NAT. The **nat-control** command has been added to maintain existing PIX Version 6.3 NAT requirements and will be implemented by

default on systems upgrading to the PIX Security appliance Version 7.0. Using the **no nat-control** command will reinstate the default PIX Security appliance Version 7.0 posture (see the "NAT" section on page 3-54).

- Some of the keywords of the **established** command have been deprecated. Also, changes to the **sysopt** command have been introduced. In PIX Security appliance Version 7.0, the **flashfs** commands are not supported. In PIX Version 6.3, the TCP option 19 used by BGP MD5 was automatically allowed, but in PIX Security appliance Version 7.0, an extra configuration is required. See the "Miscellaneous" section on page 3-59.
- Command completion and mode navigation have changed.

Note The IPSec tunnel idle timeput behavior has changed between versions 6.3 and 7.0. In version 6.3, the idle timeout was appliable only to VPN client connections.. In Version 7.0, the 30-minute idle timeout applies to both client and LAN-to-LAN tunnels. To remove the idle timeout on LAN-to-LAN tunnels and restore the 6.3 behavior, you must create a new group-policy and specify **none** for the vpn-idle-timeout value. For example:

```
group-policy L2L internal
group-policy L2L attributes
vpn-idle-timeout none
```

Then, to ensure the new group-policy takes effect, you must apply it to each LAN-to-LAN tunnel-group. For example:

```
tunnel-group ip_address general-attributes
default-group-policy L2L
```

Changed and Deprecated Commands

Most changed and deprecated features and commands will be converted automatically when PIX Security appliance Version 7.0 boots on your system, with a few requiring manual intervention before or during the upgrade. See the "Licenses" section on page 3-10 for more details.

Table 1 lists the commands for both the automatic and manual conversions.

Table 1 Command Changes Overview

Command/Description	Brief Description	For More Information
aaa-server	Changed	AAA, page 3-41
aaa-server radius-authport	Changed	AAA, page 3-41
aaa-server radius-acctport	Changed	AAA, page 3-41
auth-prompt	Changed	AAA, page 3-41
access-list compiled	Deprecated	Access Control Lists (ACLs), page 3-25
access-list <*id*> **compiled**	Deprecated	Access Control Lists (ACLs), page 3-25
ca	Changed	Public Key Infrastructure (PKI), page 3-55
ca generate/ca zeroize	Deprecated	Public Key Infrastructure (PKI), page 3-55
ca identity/ca configure	Deprecated	Public Key Infrastructure (PKI), page 3-55
ca authenticate	Deprecated	Public Key Infrastructure (PKI), page 3-55

Table 1 Command Changes Overview (continued)

Command/Description	Brief Description	For More Information
ca enroll	Deprecated	Public Key Infrastructure (PKI), page 3-55
ca crl	Deprecated	Public Key Infrastructure (PKI), page 3-55
ca subject-name	Deprecated	Public Key Infrastructure (PKI), page 3-55
ca save all	Deprecated	Public Key Infrastructure (PKI), page 3-55
ca verifycertdn	Deprecated	Public Key Infrastructure (PKI), page 3-55
conduit	Deprecated	Conduits and Outbounds, page 3-11
copy capture	Changed	Management, page 3-45
crashinfo	Changed	Management, page 3-45
crypto dynamic-map	Changed	VPN, page 3-27
crypto ipsec	Changed	VPN, page 3-27
crypto-map	Changed	VPN, page 3-27
dhcpd auto_config	Changed	Management, page 3-45
duplex	Changed to a new **interface** configuration mode command	Interfaces, page 3-23
established	Changed	Miscellaneous, page 3-59
failover	Changed	Failover, page 3-39
fixup	Changed to **inspect** command	Fixups/Inspect, page 3-17
flashfs	Not supported	Miscellaneous, page 3-59
floodguard	Deprecated	AAA, page 3-41
interface	Used to enter **interface** configuration mode command	Interfaces, page 3-23
ipaddress	Converted to **interface** configuration mode command	Interfaces, page 3-23
igmp max-groups	Changed	Multicast, page 3-51
isakmp	Changed	VPN, page 3-27
mgcp	Changed	Media Gateway Control Protocol (MGCP), page 3-49
mroute	Changed	Multicast, page 3-51
multicast interface	Deprecated	Multicast, page 3-51
nameif	Converted to **interface** configuration mode command	Interfaces, page 3-23
nat-control	**no** version maintains NAT security on interfaces	NAT, page 3-54

Table 1 Command Changes Overview (continued)

Command/Description	Brief Description	For More Information
ospf configuration mode commands	Configuration mode commands under **routing interface** command - converted automatically to **interface** configuration mode	OSPF, page 3-48
pager	Changed	Management, page 3-45
pdm location	Changed	Management, page 3-45
pdm group	Changed	Management, page 3-45
pdm logging	Changed	Management, page 3-45
routing interface	See **ospf** configuration mode command	OSPF, page 3-48
security-level	New **interface** configuration mode command	Interfaces, page 3-23
set ip next-hop	Deprecated	OSPF, page 3-48
set metric-type	Changed	OSPF, page 3-48
show snmp-server	Changed	CLI Command Processor, page 3-6
shutdown	New **interface** configuration mode command	Interfaces, page 3-23
speed	New **interface** configuration mode command	Interfaces, page 3-23
ssh	Changed	Management, page 3-45
sysopt permit pptp | permit l2tp	Deprecated	Miscellaneous, page 3-59
telnet	Changed	Management, page 3-45
tftp-server	Changed	Management, page 3-45
url-server	Changed	Miscellaneous, page 3-59
vlan	New **interface** configuration mode command	Interfaces, page 3-23
vpdn	Changed	VPN, page 3-27
vpngroup	Changed	VPN, page 3-27

CLI Command Processor

As with PIX Version 6.3, PIX Security appliance Version 7.0 supports the CLI as a user interface for configuring, monitoring, and maintaining security appliances. The CLI parser capabilities have been enhanced in PIX Security appliance Version 7.0 to include Cisco IOS software-like parser services, such as context-sensitive Help and command completion, resulting in some minor behavior changes compared to PIX Version 6.3.

Also, the **show** and **clear** commands in PIX Version 6.3 were applied inconsistently. In some cases, these commands were used to show and clear configuration objects; in other cases they were used to show and clear operational data/statistics. To make the behavior consistent and distinguish between operations on configuration versus statistics, the **show** and **clear** commands have been modified to require additional keywords.

The PIX Security appliance Version 7.0 also introduces minor changes in mode navigation and terminology so that it is closer to the Cisco IOS software CLI.

This section includes the following topics:

- Affected Commands, page 3-6
- Upgrade Requirements, page 3-6
- Change Impact, page 3-6

Affected Commands

The following commands are affected in the upgrade to PIX Security appliance Version 7.0:

- **no**
- **show**
- **clear**

In addition to the preceding commands, command completion, and mode navigation have changed in PIX Security appliance Version 7.0.

Upgrade Requirements

You must use the new forms of the **no**, **show**, and **clear** commands. Your system will output errors, if you do not.

Change Impact

This section describes the impact that the changes will have on the CLI commands in PIX Security appliance Version 7.0.

- Operational Changes, page 3-7
- Context-Sensitive Help Changes, page 3-8
- Command Syntax Checking, page 3-8
- Mode Navigation and Terminology Changes, page 3-9

Operational Changes

The operation of the **no**, **clear**, and **show** commands has changed in PIX Security appliance Version 7.0, as follows:

- The **no** variant no longer removes multiple lines of configuration simultaneously. In PIX Security appliance Version 7.0, the **no** variant removes a single configuration line only. For example, a single **no access-list** <*access-list name*> removes the following commands in PIX Version 6.3:

  ```
  access-list myaccesslist extended permit tcp host 10.175.28.97 host 10.180.210.209 eq
  37000
  access-list myaccesslist extended permit tcp host 10.175.28.97 host 10.180.210.68 eq
  37000
  access-list myaccesslist extended permit tcp host 10.175.28.98 host 10.180.210.68 eq
  37000
  ```

  But in PIX Security appliance Version 7.0, the preceding commands are removed by using either the **clear configure access-list** <*access-list name*> command or by the following:

  ```
  no access-list myaccesslist extended permit tcp host 10.175.28.97 host 10.180.210.209
  eq 37000
  no access-list myaccesslist extended permit tcp host 10.175.28.97 host 10.180.210.68
  eq 37000
  no access-list myaccesslist extended permit tcp host 10.175.28.98 host 10.180.210.68
  eq 37000
  ```

  Second example: a single **no fixup protocol http** command removes the following commands in PIX Version 6.3:

  ```
  fixup protocol http 80
  fixup protocol http 8080
  ```

  But in PIX Security appliance Version 7.0, the preceding commands are removed by the following:

  ```
  no inspect protocol http 80
  no inspect protocol http 8080
  ```

  The **no** variant removes configuration mode commands; both the command and all its configuration mode commands are removed. This behavior is the same in both PIX Version 6.3 and PIX Security appliance Version 7.0.

- To clear a configuration, PIX Security appliance Version 7.0 supports only the use of the **clear configure** <cmd> command from configuration mode.

  The following examples illustrate the use of the **clear configure** command:

PIX Version 6.3	PIX Security appliance Version 7.0	Notes
clear access-list *<access-list name>*	**clear configure access-list** *<access-list name>*	If you use the **no access-list** <*access-list name*> command, you will receive an error message
clear ssh	**clear configure ssh**	—
clear crypto dynamic-map	**clear configure crypto dynamic-map**	—

Note In PIX Version 6.3, the **clear crypto** command removed all crypto configurations other than certification authority (CA) configurations, such as trustpoints, certificates, and certificate maps. In PIX Security appliance Version 7.0, the **clear configure crypto** command removes all crypto configurations, including CA configurations. CA information is also displayed in the **show crypto** command output.

- In PIX Version 6.3, the **show snmp-server** command displayed the running configuration. In PIX Security appliance Version 7.0, the **show running-config snmp-server** command displays the running configuration and the **show snmp-server statistics** command displays run-time information on SNMP.
- The **show** <cmd> command shows statistics/buffer/counters and others. All **show** commands adhere to the model shown in the following example:

PIX Version 6.3	PIX Security appliance Version 7.0
`show crypto map`	`show running-config crypto map`

Context-Sensitive Help Changes

Table 2 lists the context-sensitive Help changes in PIX Security appliance Version 7.0:

Table 2 Context-Sensitive Help Changes

Feature	PIX Version 6.3	PIX Security appliance Version 7.0
Command Completion	When TAB is entered, it is ignored. When **?** is entered, the following message is displayed: Type help or **?** for a list of available commands.	You can type a partial command, then enter TAB to complete the command, or type a partial command, then enter **?** to show all commands that begin with the partial command.
Command **?**	The usage text for the command is displayed.	You can enter a command, followed by a space, and then type **?** to show relevant input choices.
Command <*keyword*> **?**	The usage text for the command is displayed.	Lists arguments that are available for the keyword.

Command Syntax Checking

Table 3 lists changes that occur as a result of the upgrade to PIX Security appliance Version 7.0:

Table 3 Command Syntax Checking

Feature	PIX Version 6.3	PIX Security appliance Version 7.0
Syntax error	An error message may be displayed followed by the usage text for the command.	PIX displays a ^ symbol to indicate the location of a command syntax error.
Incomplete command	An error message "Not enough arguments." may be displayed, followed by the usage text for the command.	PIX displays an 'Incomplete command' message to indicate additional arguments are required.

Mode Navigation and Terminology Changes

The PIX Security appliance Version 7.0 introduces minor changes in mode navigation and terminology so that its behavior is more similar to the Cisco IOS software CLI.

Table 4 describes the mode navigation changes between PIX Version 6.3 and PIX Security appliance Version 7.0.

Table 4 Mode Terminology Changes

Mode/Command	PIX Version 6.3	PIX Security appliance Version 7.0
User EXEC Mode		
Terminology	Unprivileged mode	User EXEC mode
Exit Method	**^Z** logs you out from the console.	**^Z** not supported as an exit method; however, you can still use **exit**, **quit** or **logout** commands as in PIX Version 6.3. Entering **^Z** will give the following error message: ERROR:% Invalid input detected at '^' marker.
Privileged EXEC Mode		
Terminology	Privileged mode	Privileged EXEC mode
Exit Method	**^Z** logs you out from the console.	**^Z** not supported as an exit method; however, you can still use the **exit**, **quit** or **logout** commands as in PIX Version 6.3. Entering **^Z** will give the following error message: ERROR:% Invalid input detected at '^' marker.
Global Configuration Mode		
Terminology	Configuration mode	Global configuration mode
Command-Specific Configuration Mode		
Terminology	Subcommand mode	Command-specific configuration mode

Licenses

- The PIX Security appliance Version 7.0 supports two kinds of license keys.
  - Existing 4-tuple license key for PIX Version 6.3 or earlier
  - A new 5-tuple license key for PIX Security appliance Version 7.0 only
- When upgrading from PIX Version 6.3 to PIX Security appliance Version 7.0, the existing license key for PIX Version 6.3 is preserved and is saved in a central location on the Flash filesystem.
- When downgrading from PIX Security appliance Version 7.0 to PIX Version 6.2 or 6.3, the existing license key for the original PIX Version 6.2 or 6.3 that was saved during the upgrade procedure is retrieved and saved to the PIX Version 6.2 or 6.3 image.
- If neither a PIX Version 6.3 nor PIX Security appliance Version 7.0 license is installed, the PIX Security appliance Version 7.0 runs in the default setting, which is a Restricted license.

Conduits and Outbounds

The PIX Security appliance Version 7.0 does not support the **conduit** and **outbound** commands; however it does support the widely used **access list** commands. The **access list** commands look more like Cisco IOS software commands, and completely replace the **conduit** and **outbound** commands; they introduce more functionality. If a PIX Version 6.3 system containing a configuration with **conduit** and/or **outbound** commands is upgraded to PIX Security appliance Version 7.0, it will output errors if you do not first migrate the **conduit** and **outbound** commands.

This section includes the following topics:

- Affected Commands, page 3-11
- Upgrade Requirements, page 3-11
- Change Impact, page 3-11
- Converting conduit Commands to access-list Commands, page 3-12
- Converting outbound Commands to access-list Commands, page 3-13

Affected Commands

The following commands are affected in the upgrade to PIX Security appliance Version 7.0:

- **conduit**
- **outbound**

Upgrade Requirements

The PIX Security appliance Version 7.0 requires that you convert the **conduit** and **outbound** commands in your configuration to access control list (**access-list**) commands before performing an upgrade to PIX Security appliance Version 7.0.

Change Impact

Your system will output errors if you do not first migrate the **conduit** and **outbound** commands before performing an upgrade to PIX Security appliance Version 7.0. Use the following resources to assist you in this process:

- The step-by-step instructions to convert the **conduit** commands to **access-lists** commands and the **outbound** commands to **outgoing** command configurations are described in the "Converting conduit Commands to access-list Commands" section on page 3-12 and the "Converting outbound Commands to access-list Commands" section on page 3-13. For additional details, see the *Cisco PIX Firewall Command Reference, Version 6.3*.
- The PIX Outbound Conduit Converter is available to contracted users from the Cisco.com Software Center PIX directory at http://www.cisco.com/cisco/software/navigator.html. This is for registered customers only. To become a registered user, go to http://tools.cisco.com/RPF/register/register.do.

  This tool facilitates the conversion of **conduit** and **outbound** commands to access control list configurations. However, due to the different nature of these access control methods, there may be some changes to the actual functionality and behavior, so this must be considered an aid and only a

starting point. All configurations converted by the Outbound/Conduit Converter (OCC) tool must be verified and tested by the network security administrators familiar with the network in question and its security policies before being deployed.

Note The OCC tool does not support **alias** and **policy nat** commands. The OCC tool does not convert configuration combinations of both an exposure of all addresses behind an internal (higher security) interface, and either a default route to the same interface or commands enabling RIP/OSPF.

- The Output Interpreter provides a web interface that takes your existing configuration as input and produces a modified configuration as its output. This tool is available at the following URL: https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl. This is for registered customers only. To become a registered user, go to http://tools.cisco.com/RPF/register/register.do. To use the Output Interpreter, ensure word wrapping is off in your terminal client and paste the complete captured output from the **write terminal** command or the **show running-config** command into the Output Interpreter. To use Output Interpreter, you must have JavaScript enabled. The same caveats regarding verification and testing previously discussed hold true for Output Interpreter configuration conversions.
- With PIX Version 6.3, only inside hosts with last octet addresses of 0 and 255 could initiate a connection to an outside interface. If a host connected to the outside interface tried to initiated a connection to an inside host with .0 or .255 in the last octet of their IP address, PIX Version 6.3 denied it.

  With PIX Security appliance Version 7.0,connections from the outside hosts are not denied, if an access-list permits it.

Converting conduit Commands to access-list Commands

To convert **conduit** command statements to **access-list** commands, perform the following steps:

Step 1 View the **static** command format. This command normally precedes both the **conduit** and **access-list** commands. The **static** command syntax is as follows.

```
static (high_interface,low_interface) global_ip local_ip netmask mask
```

For example:

```
static (inside,outside) 209.165.201.5 192.168.1.5 netmask 255.255.255.255
```

This command maps the global IP address 209.165.201.5 on the outside interface to the web server 192.168.1.5 on the inside interface. The 255.255.255.255 is used for host addresses.

Step 2 View the **conduit** command format. The **conduit** command is similar to the **access-list** command in that it restricts access to the mapping provided by the **static** command. The **conduit** command syntax is as follows.

```
conduit action protocol global_ip global_mask global_operator global_port [global_port]
foreign_ip foreign_mask foreign_operator foreign_port [foreign_port]
```

For example:

```
conduit permit tcp host 209.165.201.5 eq www any
```

This command permits TCP for the global IP address 209.165.201.5 that was specified in the **static** command statement and permits access over port 80 (www). The "any" option lets any host on the outside interface access the global IP address.

The **static** command identifies the interface that the **conduit** command restricts access to.

Step 3 Create the **access-list** command from the **conduit** command options. The **acl_name** in the **access-list** command is a name or number you create to associate **access-list** command statements with an **access-group** or **crypto map** command statement.

Normally the **access-list** command format is as follows:

```
access-list acl_name [deny | permit] protocol src_addr src_mask operator port dest_addr
dest_mask operator port
```

However, using the syntax from the **conduit** command in the **access-list** command, you can see how the *foreign_ip* in the **conduit** command is the same as the *src_addr* in the **access-list** command and how the *global_ip* option in the **conduit** command is the same as the *dest_addr* in the **access-list** command. The **access-list** command syntax overlaid with the **conduit** command options is as follows.

```
access-list acl_name action protocol foreign_ip foreign_mask foreign_operator foreign_port
[foreign_port] global_ip global_mask global_operator global_port [global_port]
```

For example:

```
access-list acl_out permit tcp any host 209.165.201.5 eq www
```

This command identifies the **access-list** command statement group with the "acl_out" identifier. You can use any name or number for your own identifier. (In this example the identifier, "act" is from ACL, which means access control list and "out" is an abbreviation for the outside interface.) It makes your configuration clearer if you use an identifier name that indicates the interface to which you are associating the **access-list** command statements. The example **access-list** command, like the **conduit** command, permits TCP connections from any system on the outside interface. The **access-list** command is associated with the outside interface with the **access-group** command.

Step 4 Create the **access-group** command using the *acl_name* from the **access-list** command and the *low_interface* option from the **static** command. The format for the **access-group** command is as follows.

```
access-group acl_name in interface low_interface
```

For example:

```
access-group acl_out in interface outside
```

This command associates with the 'acl_out' group of **access-list** command statements and states that the **access-list** command statement restricts access to the outside interface.

This completes the procedure for converting **conduit** commands to **access-list** commands.

Converting outbound Commands to access-list Commands

The outbound command creates a list of access control rules that let you specify the following:

- Whether inside users can create outbound connections
- Whether inside users can access specific outside servers
- What services inside users can use for outbound connections and for accessing outside servers

See the outbound list rules in the *Cisco PIX Firewall Command Reference, Version 6.3*.

Converting outbound Commands Applied to outgoing_src to access-list Commands

To convert **outbound** command statements to create an access list, perform the following steps:

Step 1 Review the **access-list** command format using the following existing PIX outbound configuration example:

```
outbound 1 deny   10.10.10.0 255.255.255.0 0
outbound 1 permit 10.10.20.20 255.255.255.255 0
outbound 1 except 192.168.10.1 255.255.255.255 0
apply (inside) 1 outgoing_src
```

The **access-list** command format (simplified version) is as follows:

```
access-list acl_name [deny | permit] protocol src_addr src_mask dest_addr dest_mask
```

Step 2 Verify that the IP addresses listed in the outbound configuration when applied to the **outgoing_src** command corresponds to the source address (src_addr) of the access list. The destination address (dest_addr) is equal to ‘any’. The first two outbound configuration commands translate to the following:

```
access-list inside_acl permit ip host 10.10.20.20 any
access-list inside_acl deny ip 10.10.10.0 255.255.255.0 any
```

When there are exceptions in the configuration, they apply to the entire outbound configuration within that list. The IP address listed in the exception when applied to the outgoing_src, denotes the dest_addr of the access list. The third outbound configuration with **except** translates to the following:

```
access-list inside_acl deny ip host 10.10.20.20 host 192.168.10.1
access-list inside_acl permit ip 10.10.10.0 255.255.255.0 host 192.168.10.1
```

Step 3 Put the preceding access-list elements in the order that the **outbound** command statement is processed (see the outbound rules in the *Cisco PIX Firewall Command Reference, Version 6.3*). PIX first processes the exceptions, followed by the best match in **outbound** command statements. The access list should be applied in the following order:

```
access-list inside_acl permit ip 10.10.10.0 255.255.255.0 host 192.168.10.1
access-list inside_acl deny ip 10.10.10.0 255.255.255.0 any
access-list inside_acl permit ip 10.10.10.0 255.255.255.0 host 192.168.10.1
access-list inside_acl deny ip 10.10.10.0 255.255.255.0 any
```

Step 4 Add the following access-list element to preserve the default behavior of the PIX. Note that by default, PIX allows outbound traffic. When an access list is used to filter packets, traffic that does not match the access list is denied.

```
access-list inside_acl permit ip any any
```

Step 5 Add the following **access-list** command to reference the interface to which the outbound configuration is applied. Note that there should be a corresponding access-group to bind the access list to the interface.

```
access-group inside_acl in interface inside
```

Step 6 Verify the following configuration translated from **outbound** commands applied to outgoing_src to **access-list** commands.

```
access-list inside_acl permit ip 10.10.10.0 255.255.255.0 host 192.168.10.1
access-list inside_acl deny ip 10.10.10.0 255.255.255.0 any
access-list inside_acl permit ip 10.10.10.0 255.255.255.0 host 192.168.10.1
access-list inside_acl deny ip 10.10.10.0 255.255.255.0 any
access-list inside_acl permit ip any any
access-group inside_acl in interface inside
```

Converting outbound Commands Applied to outgoing_dest to access-list Commands

To convert **outbound** command statements to create an access list, perform the following steps:

Step 1 Review the access list format using the following existing PIX outbound configuration example:

```
outbound 1 deny   192.168.10.0 255.255.255.0 0
outbound 1 permit 192.168.20.20 255.255.255.255 0
outbound 1 except 10.10.10.10 255.255.255.255 0
apply (inside) 1 outgoing_dest
```

The **access-list** command format (simplified version) is:

```
access-list acl_name [deny | permit] protocol src_addr src_mask dest_addr dest_mask
```

Step 2 Verify that the IP addresses listed in the outbound configuration when applied to the **outgoing_dest** command corresponds to the destination address (dest_addr) of the access list. The source address (src_addr) is equal to 'any'. The first two outbound configuration commands translate to the following:

```
access-list inside_acl permit ip any host 192.168.20.20
access-list inside_acl deny ip any 192.168.10.0 255.255.255.0
```

When there are exceptions in the configuration, (as in the third line in our example), they apply to the entire outbound configuration within that list. The IP address listed in the exception when applied to the outgoing_dest, denotes the src_addr of the access list. The third outbound configuration with exceptions translates to the following:

```
access-list inside_acl deny ip host 10.10.10.10 host 192.168.20.20
access-list inside_acl permit ip host 10.10.10.10 192.168.10.0 255.255.255.0
```

Step 3 Put the preceding access-list elements in the order that the **outbound** command statement is processed (see the outbound rules in the *Cisco PIX Firewall Command Reference Guide, Version 6.3*). PIX first processes the exceptions, followed by the best match in **outbound** command statements. The access list should be applied in the following order:

```
access-list inside_acl deny ip host 10.10.10.10 host 192.168.20.20
access-list inside_acl permit ip any host 192.168.20.20
access-list inside_acl permit ip host 10.10.10.10 192.168.10.0 255.255.255.0
access-list inside_acl deny ip any 192.168.10.0 255.255.255.0
```

Step 4 Add the following access-list element to preserve the default behavior of the PIX. Note that by default, PIX allows outbound traffic. When an access list is used to filter packets, traffic that does not match the access list is denied.

```
access-list inside_acl permit ip any any
```

Step 5 Add the following **access-group** command to reference the interface to which the outbound configuration is applied. Note that there should be a corresponding access-group to bind the access list to the interface.

```
access-group inside_acl in interface inside
```

Step 6 Verify the following configuration translated from **outbound** commands applied to **outgoing_src** to **access-list** commands.

```
access-list inside_acl deny ip host 10.10.10.10 host 192.168.20.20
access-list inside_acl permit ip any host 192.168.20.20
access-list inside_acl permit ip host 10.10.10.10 192.168.10.0 255.255.255.0
access-list inside_acl permit ip any host 192.168.20.20
access-list inside_acl permit ip any any
access-group inside_acl in interface inside
```

Converting outbound Commands Applied to both outgoing_src and outgoing_dest to access-list Commands

To convert **outbound** command statements to create an access list, perform the following steps:

Step 1 Review the **access-list** command format using the following existing PIX outbound configuration example:

```
outbound 1 deny   10.10.10.0 255.255.255.0 0
outbound 1 permit 10.10.20.20 255.255.255.255 0
apply (inside) 1 outgoing_src

outbound 2 deny   192.168.10.0 255.255.255.0 0
outbound 2 permit 192.168.20.20 255.255.255.255 0
apply (inside) 2 outgoing_dest
```

The **access-list** command format (simplified version) is:

```
access-list acl_name [deny | permit] protocol src_addr src_mask dest_addr dest_mask
```

Step 2 Verify that the IP addresses listed in the outbound configuration when applied to the **outgoing_src** command corresponds to the source address (src_addr) of the access list. The destination address (dest_addr) is equal to ‘any’. The first two outbound configuration commands translate to the following:

```
access-list inside_acl permit ip host 10.10.20.20 any
access-list inside_acl deny ip 10.10.10.0 255.255.255.0 any
```

Step 3 Verify that the IP addresses listed in the outbound configuration when applied to the **outgoing_dest** command correspond to the destination address (dest_addr) of the access list. The source address (src_addr) is equal to ‘any’. The line fourth and fifth outbound configuration commands translate to the following:

```
access-list inside_acl permit ip any host 192.168.20.20
access-list inside_acl deny ip any 192.168.10.0 255.255.255.0
```

Step 4 When both outbound lists are applied to the same interface, the following rule applies: The outgoing_src option and outgoing_dest outbound lists are filtered independently. If any filter contains the deny option, the outbound packet is denied.The result is the following two access-list elements:

```
access-list inside_acl deny ip 10.10.10.0 255.255.255.0 host 192.168.20.20
access-list inside_acl permit ip host 10.10.20.20 host 192.168.20.20
```

Step 5 Add the following access-list element to preserve the default behavior of the PIX. Note that by default, PIX allows outbound traffic. When an access list is used to filter packets, traffic that does not match the access list is denied.

```
access-list inside_acl permit ip any any
```

Add the following **access-group** command to reference the interface to which the outbound configuration is applied. Note that there should be a corresponding access-group to bind the access list to the interface.

```
access-group inside_acl in interface inside
```

Step 6 Verify the following configuration translated from **outbound** commands applied to both **outgoing_src** and **outgoing_dest** to **access-list** commands are applied in the order it appears.

```
access-list inside_acl deny ip 10.10.10.0 255.255.255.0 host 192.168.20.20
access-list inside_acl permit ip host 10.10.20.20 host 192.168.20.20
access-list inside_acl permit ip any host 192.168.20.20
access-list inside_acl deny ip any 192.168.10.0 255.255.255.0
```

```
access-list inside_acl permit ip host 10.10.20.20 any
access-list inside_acl deny ip 10.10.10.0 255.255.255.0 any
access-list inside_acl permit ip any any
access-group inside_acl in interface inside
```

Fixups/Inspect

PIX uses stateful application inspection, known as fixups, to ensure secure use of applications and services. In PIX Security appliance Version 7.0, the **fixup** command has been deprecated and replaced with the **inspect** command under the Modular Policy Framework (MPF) infrastructure.

MPF is a CLI framework that lets you define traffic classes and apply feature-specific actions (policies) on them, providing greater granularity and flexibility in configuring network policies. For more information about MPF, see the *Cisco Security Appliance Command Line Configuration Guide* and the *Cisco Security Appliance Command Reference*.

This section includes the following topics:

- Affected Commands, page 3-18
- Upgrade Requirements, page 3-18
- Command Change Description, page 3-18
- Change Impact, page 3-20

Affected Commands

The following command is affected in the upgrade to PIX Security appliance Version 7.0:

- **fixup**

Upgrade Requirements

The **fixup** commands migrate automatically to MPF **inspect** commands when you upgrade to PIX Security appliance Version 7.0. No manual intervention is required.

- All existing **fixup** commands in the configuration will automatically convert to MPF commands.
- All **fixups** that are currently non-configurable (such as NetBIOS) are also made configurable and converted to MPF commands.

Command Change Description

Table 5 lists changes in the **fixup** command, and Table 6 lists the default portals for the commands in Table 5.

fixup

Note In the PIX Security appliance Version 7.0 column of Table 5, note that the **inspect** commands do not have port numbers, unlike the corresponding **fixup** commands in PIX Version 6.3. The port numbers in this example are included in the ‘class inspection-default’ implicitly. When an inspect is configured for a protocol on ‘class inspection-default’, the protocol is automatically inspected on its default port, because this class matches the ‘default-inspection-traffic’ for each protocol. Table 6 lists the default ports for each inspect shown in Table 5.

Table 5 Changes in the fixup Command

PIX Version 6.3	PIX Security appliance Version 7.0
`fixup protocol esp-ike`	Not Supported

`fixup protocol dns maximum-length 512`
`fixup protocol h323 h225 1720`
`fixup protocol http 80`
`fixup protocol rsh 514`
`fixup protocol sip 5060`
`fixup protocol smtp 25`
`fixup protocol ftp 21`
`fixup protocol h323 ras 1718-1719`
`fixup protocol ils 389`
`fixup protocol rtsp 554`
`fixup protocol skinny 2000`
`fixup protocol sqlnet 1521`
	`class-map inspection_default`
	`match default-inspection-traffic`
	`policy-map global_policy`
	`class inspection_default`
	`inspect ftp`
	`inspect h323 h225`
	`inspect h323 ras`
	`inspect ils`
	`inspect rsh`
	`inspect rtsp`
	`inspect smtp`
	`inspect sqlnet`
	`inspect sip`
	`inspect skinny`
	`inspect netbios`
	`inspect ctiqbe`
	`inspect icmp`
	`inspect http`
	`inspect dns`
	`!`
	`service-policy global_policy global`

Note The **fixup protocol esp-ike** command is not supported in PIX Security appliance Version 7.0. This feature is suited for the PIX 501 and 506/506E platforms, which PIX Security appliance Version 7.0 does not currently support. The workaround requires that the client and head-end be NAT-T capable.

The **inspect** command introduced in PIX Security appliance Version 7.0 is not the same as the Cisco IOS command **ip inspect**.

Table 6 Default Ports for Table 5 Commands

Inspected Protocol Name	Protocol	Source Port	Destination Port
ctiqbe	tcp	N/A	2748
dns	udp	53	53
ftp	tcp	N/A	21
gtp	udp	2123,3386	2123,3386
h323 h225	tcp	N/A	1720
h323 ras	udp	N/A	1718-1719
http	tcp	N/A	80
icmp	icmp	N/A	N/A
ils	tcp	N/A	389
mgcp	udp	2427,2727	2427,2727
netbios	udp	137-138	N/A
rpc	udp	111	111
rsh	tcp	N/A	514
rtsp	tcp	N/A	554
sip	tcp, udp	N/A	5060
skinny	tcp	N/A	2000
smtp	tcp	N/A	25
sqlnet	tcp	N/A	1521
tftp	udp	N/A	69
xdmcp	udp	177	177

Change Impact

This section describes the impact that the changes will have on the CLI commands in PIX Security appliance Version 7.0.

- In PIX Security appliance Version 7.0, the **fixup** commands are still accepted at the CLI, however, they are converted to their MPF equivalents in the configuration. In other words, you can enter **fixup** commands at the CLI, but the configuration only shows the converted MPF style commands. Additionally, when a **fixup** command is entered at the CLI, an informational message similar to the following will appear:

```
pix1(config)# fixup protocol http 8080
INFO: converting 'fixup protocol http 8080' to MPF commands
```

- In the next release, the **fixup** command will be deprecated and only MPF commands will be accepted for all inspection engines.

Table 7 describes the changes in **fixup** command behavior in PIX Security appliance Version 7.0:

Table 7 Changes in fixup Command Behavior

Command	Description of Change
fixup	It is converted to MPF commands.
no fixup	The converted MPF commands are removed.
clear fixup	This command converts to the **clear configure fixup** command. As with any **clear configure** command, the default configuration (in this case, default configuration of inspection engines) is restored when this command is applied.
write memory	**Fixup** commands are no longer written to the Flash memory. Only converted MPF commands are written.

  - New fixups introduced in PIX Security appliance Version 7.0 will only support MPF style CLI commands.
  - When a **fixup** command is converted to a MPF **inspect** command, the **inspect** command is created in the enabled global policy. If no global policy is enabled, one is created.
- To disable an inspection, remove the **inspect** command from the policy-map or issue the corresponding **fixup** command with the default port value.
- To add an inspection that is not enabled by default such as MGCP, simply add the **inspect** command to the policy-map or issue the corresponding **fixup** command (if one is supported before PIX Security appliance Version 7.0) with the default port value.
- If an additional, non-default port is needed for an inspection:
  - use a separate class-map to include the new port and then add the new class and **inspect** command to the policy-map,

    or
  - issue the corresponding **fixup** command.

    For example, if port 8080 is to be added for HTTP inspection, enter the following **fixup** command:

```
fixup protocol http 8080
```

    or, enter the following MPF commands:

```
class-map non_default_http_inspection <==== define a new class-map
    match port tcp eq 8080 <==== match tcp port 8080 traffic

policy-map global_policy       <==== select the policy-map
    class non_default_http_inspection     <==== add the new class
        inspect http                          <==== add the action to the new class
```

    If the configuration before entering the MPF commands is:

```
class-map inspection_default
    match default-inspection-traffic

policy-map global_policy
   class inspection_default
     inspect ftp
     inspect http
```

The resulting configuration after entering the MPF commands will be:

```
class-map inspection_default
    match default-inspection-traffic

 class-map non_default_http_inspection
    match port tcp 8080

 policy-map global_policy
   class inspection_default
     inspect ftp
     inspect http
   class non_default_http_inspection
     inspect http
```

- If the default port is to be replaced by a new port for an inspection:
  - the corresponding **inspect** command must be removed from the policy-map and then follow the previous example to add the new port for inspection,

    or

  - issue a no **fixup** command with the default port then issue a **fixup** command with the new port.

    For example, if port 8080 is to replace port 80 for HTTP inspection, then enter the following **fixup** commands:

    ```
    no fixup protocol http 80
    fixup protocol http 8080
    ```

    or, enter the following MPF commands:

    ```
    policy-map global_policy       <==== select the policy-map
        class inspection_default              <==== select the class
            no inspect http                       <==== remove http from the class
        class-map non_default_http_inspection <==== define a new class-map
            match port tcp 8080                   <==== match tcp port 8080 traffic

    policy-map global_policy       <==== select the policy-map
     class non_default_http_inspection     <==== add the new class
        inspect http                          <==== add the action to the new class
    ```

- If the configuration before entering the MPF commands is:

```
class-map inspection_default
    match default-inspection-traffic

 policy-map global_policy
   class inspection_default
     inspect ftp
     inspect http
```

The resulting configuration after entering the MPF commands will be:

```
ss-map inspection_default
    match default-inspection-traffic

 class-map non_default_http_inspection
    match port tcp 8080

 policy-map global_policy
   class inspection_default
     inspect ftp
   class non_default_http_inspection
     inspect http
```

Interfaces

In PIX Security appliance Version 7.0, the interface CLI and related commands are enhanced to be hierarchical. The concepts of 'main interface,' such as Ethernet0, and 'subinterface,' such as Ethernet0.10, are introduced. An **interface** configuration mode command is created with several commands migrated or added to the configuration mode command. The benefits of the change are:

- The main/subinterface notation provides an easy and consistent way to represent multiple physical interfaces and VLAN logical interfaces on the security appliances.
- On platforms supporting security contexts, a PIX Security appliance Version 7.0 feature, it is easier to define and allocate interfaces to contexts with the new interface structure.
- The **interface** configuration mode command facilitates other feature enhancements such as support for IPv6.
- The hierarchical output improves the readability of a configuration file compared with the flat structure.

This section includes the following topics:

- Affected Commands, page 3-23
- Command Change Description, page 3-23
- Upgrade Requirements, page 3-25
- Change Impact, page 3-25

Affected Commands

The following commands are affected in the upgrade to PIX Security appliance Version 7.0:

- **interface**
- **nameif**
- **ip address**

Command Change Description

The **auto** keyword in PIX Version 6.3 is converted to two configuration lines in PIX Security appliance Version 7.0: **speed auto** and **duplex auto**. Both lines are default configuration, and will not be displayed.

Table 8 provides a configuration upgrade example, Table 9 lists changes in the **interface** command, and Table 10 lists interface configuration mode changes.

Table 8 Configuration Upgrade Example

PIX Version 6.3	PIX Security appliance Version 7.0

interface ethernet0 auto
interface ethernet1 auto
interface ethernet1 vlan101 logical
interface ethernet1 vlan102 physical
interface ethernet2 auto shutdown
 	
nameif ethernet0 outside security0
nameif vlan101 dmz security50
nameif vlan102 inside security100
 	
ip address outside 171.45.0.13
ip address dmz 10.1.32.12
ip address inside 192.168.15.12
	interface Ethernet0
	  nameif outside
	  security-level 0
	  ip address 171.45.0.13
	interface Ethernet1
	  no nameif
	  no security-level
	  no ip address
	interface Ethernet1.101
	  vlan 101
	  nameif dmz
	  security-level 50
	  ip address 10.1.32.12
	interface Ethernet1.102
	  vlan 102
	  nameif inside
	  security-level 100
	  ip address 192.168.15.12
	interface Ethernet2
	  shutdown
	  no nameif
	  no security-level
	  no ip address

Table 9 Changes in the interface Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
interface	**interface** <*hardware_id*> [<*hardware_speed*> [**shutdown**]]	**interface** <*type*><*port*>	<*hardware_speed*> is configured by the **duplex** and **speed** configuration mode commands [**shutdown**] is performed by the **shutdown** configuration mode command
	[no] interface <*hardware_id*> <*vlan_id*> [**logical** | **physical**] [**shutdown**]	**[no] interface** <*type*><*port*>.<*subif_number*>	<*vlan_id*> is configured by the **vlan** configuration mode command
	interface <*hardware_id*> **change-vlan** <*old_vlan_id*> <*new_vlan_id*>	Use the **vlan** <*new_vlan_id*> configuration mode command	—

Table 10 Interface Configuration Mode Commands

Interface Configuration Mode Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
duplex	Part of the **interface** command, <*hardware_speed*> option	**duplex** {**auto** | **full** | **half**} **no duplex** [**auto** | **full** | **half**]	New **interface** configuration mode command
ip address	[**no**] **ip address** <*if_name*> <*ip_address*> [<*netmask*>]	**[no]** *ip address* <*ip_address*> *[<netmask>]* [**standby** <*stdby_address*>]	Converted to **interface** configuration mode command
	[no] ip address <*if_name*> **dhcp** [**setroute**] [**retry** <*retry_cnt*>]	**[no] ip address dhcp** [**setroute**] [**retry** <*retry_cnt*>]	—
nameif	**[no] nameif** {<*hardware_id*> | <*vlan_id*>} <*if_name*> <*security_level*>	**nameif** <*if_name*> **[no] nameif** [<*if_name*>]	Converted to **interface** configuration mode command. <*security_level*> is configured by the **security-level** configuration mode command
security-level	Part of the **nameif** command, <*security_level*> option	**security-level** <*level*> **[no] security-level** [<*level*>]	New **interface** configuration mode command
shutdown	Part of the **interface** command, shutdown option	[**no**] **shutdown**	New **interface** configuration mode command
speed	Part of the **interface** command, <*hardware_speed*> option	**speed** {**auto** | **10** | **100** | **1000**} **no speed** [**auto** | **10** | **100** | **1000**]	New **interface** configuration mode command
vlan	Part of the **interface** command, <*vlan_id*> option	**vlan** <*id*> **no vlan** [<*id*>]	New **interface** configuration mode command

Upgrade Requirements

The **interface, nameif,** and **ip address** commands from the PIX Version 6.3 configuration file are automatically converted when upgrading to PIX Security appliance Version 7.0. No manual intervention is required.

Both the **sysopt connection permit-pptp** and the **sysopt connection permit-l2tp** commands are no longer supported in PIX Security appliance Version 7.0.

Change Impact

After booting the system with the PIX Security appliance Version 7.0 image, the software only accepts the new interface CLIs. A syntax error results when you attempt to use the old CLI format.

Access Control Lists (ACLs)

In PIX Security appliance Version 7.0, there is no longer a need to compile access lists. The system now automatically optimizes access list processing.

This section includes the following topics:

- Affected Commands, page 3-26
- Upgrade Requirements, page 3-26
- Command Change Description, page 3-26
- Change Impact, page 3-26

Affected Commands

The following commands are affected in the upgrade to PIX Security appliance Version 7.0:

- **access-list** <*id*> **compiled**
- **access-list compiled**

Upgrade Requirements

Access control list (ACL) commands convert automatically when upgrading to PIX Security appliance Version 7.0. No manual intervention is required, and no functionality is affected.

Command Change Description

Table 11 lists changes in the **access-list** command.

access-list

Table 11 Changes in the access-list Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
`access-list`	`[no] access-list compiled`	Not supported	—
	`[no] access-list <id> compiled`	Not supported	—

Change Impact

This section describes the impact that the changes will have on the ACLs in PIX Security appliance Version 7.0.

- Any access list configuration statements with the **compiled** option are ignored by the parser which has no effect because access lists are always maintained in a state where lookups are very efficient. All other statements in the access list configuration will be accepted and behave as they did in PIX Version 6.3.

The configuration lines in PIX Version 6.3 with the **compiled** keyword are no longer accepted by the new parser. An error message is printed and the statement is not stored in the running configuration, as shown in the following example:

```
pix(config)# access-list compiled
ERROR:% Incomplete command
```

The preceding error statement occurs because **compiled** is no longer a keyword and is treated as a name of an access list.

```
pix(config)# access-list 888 compiled

WARNING:% This command has been DEPRECATED. The access-lists are always maintained in
optimized form
```

As the **compiled** keyword has been removed, the configuration line is not valid and is not accepted by the parser.

- All the other access list configurations will update seamlessly.

VPN

VPN commands, such as **username**, **group-policy**, and **tunnel-group** commands, have been added to support a user/group hierarchy that gives you flexibility to define security policy information per groups of users with the ability to override group policies with user-specific policies. Tunnel group and group policy distinctions also make it possible to offload much of the policy information to an external server as opposed to configuring it entirely on the security appliance.

In addition, the **ca** and **vpdn** commands were changed, as follows (see the "Command Change Description" section on page 3-28):

- **ca** command—The certification authority (**ca**) commands were modified to incorporate more PKI features and to make them look more like Cisco IOS software commands. See the "Public Key Infrastructure (PKI)" section on page 3-55 for more information on the changes to the **ca** command.
- **vpdn** command—The **vpdn** command was removed because support for L2TP/PPTP/PPPoE was removed in PIX Security appliance Version 7.0. The configuration of old VPDN objects at the group level is accomplished via the **tunnel-group** and **group-policy** commands.

This section includes the following topics:

- Affected Commands, page 3-27
- Upgrade Requirements, page 3-28
- Command Change Description, page 3-28
- Change Impact, page 3-37

Affected Commands

The following commands are affected in the upgrade to PIX Security appliance Version 7.0:

- **ca** (see the "Public Key Infrastructure (PKI)" section on page 3-55)
- **crypto dynamic-map**
- **crypto ipsec**
- **crypto-map**

- **isakmp**
- **url-server**
- **vpdn**
- **vpngroup**

Upgrade Requirements

Most VPN commands convert automatically when upgrading to PIX Security appliance Version 7.0, without manual intervention.

Command Change Description

Table 12 lists changes in the **ca** command, Table 13 lists changes in the **crypto ipsec** command, Table 14 lists changes in the **crypto map** command, Table 15 lists changes to the **isakmp** command, Table 16 lists changes in **vpdn** command, and Table 17 lists changes in the **vpngroup** command.

Table 12 Changes in the ca Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
ca	**ca authenticate** <*ca_nickname*> [<*fingerprint*>]	**crypto ca authenticate** <trustpoint> [**fingerprint** <hex value>] [nointeractive]	—
	[no] ca crl request <*ca_nickname*>	**crypto ca crl request** <trustpoint>	—
	[no] ca enroll <*ca_nickname*> <*challenge_password*> [**serial**] [*ipaddress*]	**crypto ca trustpoint** <name> **[no] ip-address** <address> **[no] serial-number** **password** <password> exit **crypto ca enroll** <name>	—
	ca generate rsa {key | specialkey} <*key_modulus_size*>	**crypto key generate rsa** [**usage-keys** | **general-keys**] [**label** <*key-pair-label*>] [**modulus** <size>] [**noconfirm**]	—
	[no] ca identity <*ca_nickname*> [<*ca_ipaddress*> | <*hostname*> [:<*ca_script_location*>] [<*ldap_ip address*> | <*hostname*>]]	**crypto ca trustpoint** <name> **enroll url** <ip_address|hostname>[:<ca_script_location>] **crl** **ldap_defaults** <ldap_ip|hostname> **exit** exit	—
	[no] ca save all	Not supported	Certificates and keys will be saved whenever the configuration is saved
	[no] ca subject-name <*ca_nickname*> <*X.500_string*>	**crypto ca trustpoint** <name> **[no] subject-name** <X.500 string>	—

Table 12 Changes in the ca Command (continued)

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
	ca zeroize rsa [<*keypair_name*>]	**crypto key zeroize rsa|dsa** [**label** <*key-pair-label*>] [**noconfirm**]	—
	ca generate rsa key <*modulus*>	**crypto key generate rsa** [**usage-keys** | **general-keys**] [**label** <*key-pair-label*>] [**modulus** <size>] [**noconfirm**]	—
	ca generate rsa specialkey <size>	**crypto key generate rsa usage-keys modulus** <size>	—
	[no] ca configure <*ca_nickname*> **ca** | **ra** <*retry_period*> <*retry_count*> [**crloptional**]	**crypto ca trustpoint** <trustpoint name> **enrollment retry period** <minutes> **enrollment retry count** <num> **crl configure**	The retry period and count are now configured via the trustpoint configuration mode. The crl configuration is an additional configuration mode accessible from the trustpoint configuration mode.
	[no] ca verifycertdn <x.500 string>	**crypto ca verifycertdn** <x.500 string>	—

crypto ipsec

Table 13 Changes in the crypto ipsec Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
crypto ipsec	**[no] crypto ipsec security-association lifetime seconds** *<seconds>* | **kilobytes** *<kilobytes>*	**[no] [crypto] ipsec security-association lifetime seconds** *<seconds>* | **kilobytes** *<kilobytes >*	Authentication Header (AH) support has been removed **Note** The standalone version of this **ipsec** command works the same as the **crypto** version Added the following commands: • [**crypto**] **ipsec df-bit** [**clear-df** | **copy-df** | **set-df**] *<interface-name>* • **[crypto] ipsec fragmentation [after-encryption | before-encryption]** *<interface-name>* • **clear configure** [*crypto*] **ipsec transform-set** *<transform-set-name>* • **show** [**crypto**] **ipsec stats** • **show** [**crypto**] **ipsec df-bit** *<interface-name>* • **show** [**crypto**] **ipsec fragmentation** *<interface-name>*
	crypto ipsec transform-set *<transform-set-name>* *<transform1>* [*<transform2>* [*<transform3>*]]	**[no] [crypto] ipsec transform-set** *<transform-set-name>* **transform1** [**transform3**]	
	[no] crypto ipsec transform-set *<trans-name>* [**ah-md5-hmac | ah-sha-hmac] [esp-aes | esp-aes-192 | esp-aes-256| esp-des | esp-3des| esp-null] [esp-md5-hmac | esp-sha-hmac | esp-none]**	**[no] [crypto] ipsec transform-set** *<transform-set-name>* [**esp-aes** |**esp-aes-192** | **esp-aes-256**| **esp-des** | **esp-3des**| **esp-null**] [**esp-md5-hmac** | **esp-sha-hmac** | **esp-null**]	
	crypto ipsec transform-set *<transform-set-name>* **mode transport**	**[no] [crypto] ipsec transform-set** *<transform-set-name>* **mode transport** [**crypto**] **ipsec df-bit** [**clear-df** | **copy-df** | **set-df**] *<interface-name>*	

crypto map

Table 14 Changes in the crypto map Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
crypto map	[**no**] **crypto map** <*map-name*> **interface** <*interface-name*>	[**no**] **crypto map** <*map-name*> **interface** <*interface-name*>	Removed support for the following commands: **[no] crypto map** <*map-name*> <*seq-num*> **set session-key inbound** | **outbound ah** <*spi*> <*hex-key-string*> **[no] crypto map** <*map-name*> <*seq-num*> **set session-key inbound** | **outbound esp** <*spi*> <*cipher hex-key-string*> [**authenticator** <*hex-key-string*>] Added new group numbers to the Diffie-Hellman (DH) group specification Added limit of 10 to the number of peers specified. The 9 additional peers are used as fallback peers when the device is used in "originate only" mode via the connection-type parameter. **Note** The standalone version of the **map** command works the same as its **crypto** version.
	[**no**] **crypto map** <*map-name*> **client** [**token**] **authentication** <*aaa-server-name*>	Deprecated	
	[**no**] **crypto map** <*map-name*> <*seq-num*> **ipsec-isakmp** | **ipsec-manual** [**dynamic** <*dynamic-map-name*>]	[**no**] **crypto map** <*map-name*> <*seq-num*> **ipsec-isakmp dynamic** <*dynamic-map-name*>	
	[**no**] **crypto map** <*map-name*> <*seq-num*> **set pfs** [**group1** | **group2**]	[**no**] **crypto map** <*map-name*> <*seq-num*> **set pfs** [**group1** | **group2** | **group5** |**group7**]	
	[**no**] **crypto map** <*map-name*> <*seq-num*> **match address** <*acl_name*>	[**no**] **crypto map** <*map-name*> <*seq-num*> **match address** <*acl_name*>	
	[**no**] **crypto map** <*map-name*> <*seq-num*> **set peer** {<*ip_address*> | <*hostname*>}	[**no**] **crypto map** <*map-name*> <*seq-num*> **set peer** {**ip_address1** | **hostname1**} [..**ip_address10** | **hostname10**]	
	[**no**] **crypto map** <*map-name*> <*seq-num*> **set security-association lifetime seconds** <*seconds*> | **kilobytes** <*kilobytes*>	[**no**] **crypto map** <*map-name*> <*seq-num*> **set security-association lifetime seconds** <*seconds*> | **kilobytes** <*kilobytes*>	
	[**no**] **crypto map map-name seq-num set transform-set** <*transform-set-name1*> [<*transform-set-name6*>]	[**no**] **crypto map** <*map-name*> <*seq-num*> **set transform-set** <*transform-set-name1*> [.. <*transform-set-name6*>]	
	[**no**] **crypto map** <*map-name*> **client configuration address initiate** | **respond**	Not supported	

isakmp

Table 15 Changes in the isakmp Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
isakmp	**isakmp keepalive** <*seconds*> [<*retry-seconds*>]	**tunnel-group** <*group name*> **type ipsec-ra**|**ipsec-l2l** **tunnel-group** <*group name*> **ipsec-attributes** **isakmp keepalive** [***threshold*** <*seconds*>][***retry*** <*seconds*>]	—
	isakmp key <*keystring*> **address** <*peer-address*> [**netmask** <*mask*>] [**no-xauth**] [**no-config-mode**]	**tunnel-group** <*group name*> **type ipsec-l2l** **tunnel-group** <*group name*> **ipsec-attributes** **pre-shared-key** <*preshared key*>	The **isakmp** command was used to set a preshared key for LAN-to-LAN tunnels. This is now done generically for both LAN-to-LAN and remote access tunnels via the **tunnel-group** command.
	isakmp client configuration address-pool local <*pool-name*> [<*interface-name*>]	**tunnel-group** <*group name*> **type ipsec-l2l** **tunnel-group** <*group name*> **general-attributes** **address-pool** [(**interface name**)] <*address_pool1*> [...<*address-pool6*>]	—
	isakmp peer fqdn | **ip** <**fqdn** | **ip-address**> {**no-xauth** |**no-config-mode**}	**tunnel-group** <*group name*> **type ipsec-l2l**|**ipsec-ra**	The exclusion of Xauth and modecfg is implicit in the definition of the tunnel group. If a tunnel group is defined as ipsec-l2l, it automatically excludes Xauth and modecfg.

Note that in PIX Security appliance Version 7.0, the ISAKMP default policy is no longer hidden. The ISAKMP default policy is now visible in the running-configuration, and you can retain, modify, or remove it.

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 rsa-sig
isakmp policy 65535 encryption des
isakmp policy 65535 hash sha
isakmp policy 65535 group 1
```

```
isakmp policy 65535 lifetime 86400
```

vpdn

Table 16 Changes in the vpdn Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
vpdn	**vpdn group** <*group_name*> **pptp echo** <*echo_time*>	Not supported	PPTP is not supported in PIX Security appliance Version 7.0
	vpdn group <*group_name*> **accept dialin l2tp**	Not supported	L2TP and L2TP over IPSec are not supported in PIX Security appliance Version 7.0.
	vpdn group <*group_name*> **accept dialin pptp**	Not supported	PPTP is not supported in PIX Security appliance Version 7.0
	vpdn group <*group_name*> [**client configuration address local** <*address_pool_name*>]	Not supported	—
	vpdn group <*group_name*> **client configuration** <*dns dns_ip1*> [<*dns_ip2*>]	Not supported	—
	vpdn group <*group_name*> **client configuration wins** <*wins_ip1*> [<*wins_ip2*>]	Not supported	—
	vpdn group <*group_name*> **client authentication local** | **aaa** <*auth_aaa_group*>	Not supported	—

Table 16 Changes in the vpdn Command (continued)

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
	vpdn group *<group_name>* **client accounting aaa** *<auth_aaa_group>*	Not supported	—
	vpdn group *<group_name>* **l2tp tunnel hello** *<hello_timeout>*	Not supported	—
	vpdn enable *<if_name>*	Not supported	Not needed; all PPP traffic is encapsulated by IPSec
	vpdn group *<group_name>* **ppp authentication pap**|**chap**|**mschap**	Not supported	—
	vpdn group *<group_name>* **ppp encryption mppe 40** | **128**| **auto** [**required**]	Not supported	Not needed; all PPP traffic is encapsulated by IPSec
	show vpdn tunnel [**l2tp**|**pptp**|**pppoe**] [**id** *<tnl_id>* | **packets** | **state** | **summary** | **transport**]	Not supported	Functionality replaced by **vpn-sessiondb** command
	show vpdn session [**l2tp**|**pptp**|**pppoe**] [**id** *<sess_id>* | **packets** | **state**| **window**]	Not supported	Functionality replaced by **vpn-sessiondb** command
	show vpdn pppinterface [**id** *<dev_id>*]	Not supported	Functionality replaced by **vpn-sessiondb** command
	clear vpdn [**group** | **interface**| **tunnel** *<tnl_id>* | **username**]	Not supported	Functionality replaced by **vpn-sessiondb** command
	vpdn group *<group_name>* **request dialout pppoe**	Not supported	Used only for PPOE, which is not supported in this release
	show vpngroup [*<group_name>*]	Not supported	—

vpngroup

Table 17 Changes in the vpngroup Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
vpngroup	**vpngroup** *<group_name>* **address-pool** *<pool_name>*	**tunnel-group** *<group name>* **type ipsec-l2l** **tunnel-group** *<group name>* **general-attributes** **address-pool** [(**interface name**)] *<address_pool1>* [*...<address-pool6>*]	Converted to **tunnel-group** syntax
	vpngroup *<group_name>* **authentication-server** *<servers>*	Not supported	Used on PIX Version 6.3 to pass a AAA server address for Individual User Authentication (IUA), a feature used on the hardware client; PIX Security appliance Version 7.0 proxies the AAA request for the hardware client, and therefore always sends its own address.
	vpngroup *<group_name>* **backup-server** {<{**ip1**> [*<ip2> ... <ip10>*]} | **clear-client-cfg**}	In the group-policy attribute configuration mode: [**no**] **backup-servers** *<peer1 peer2 …..peer10>* | **clear-client-config** | **keep-client-config**	Converted to **group-policy** syntax
	vpngroup *<group_name>* **default-domain** *<domain_name>*	In the group-policy attribute configuration mode: [**no**] **default-domain value** *<domain-name>*	Converted to **group-policy** syntax

Table 17 Changes in the vpngroup Command (continued)

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
	vpngroup *<group_name>* **device-pass-through**	In the group-policy attribute configuration mode: **ip-phone-bypass** <enable|disable> **leap-bypass** <enable|disable>	Converted to **group-policy** syntax. The IUA exemption is no longer MAC address based. The administrator can choose to exempt Cisco IP Phones and/or any LEAP data from Individual User Authentication.
	vpngroup *<group_name>* **dns-server** *<dns_ip_prim>* [*<dns_ip_sec>*]	In the group-policy attribute configuration mode: [**no**] **dns-server value** *<ip_address>* [*ip_address*]	Converted to **group-policy** syntax
	vpngroup *<group_name>* **idle-time** *<idle_seconds>*	In the group-policy attribute configuration mode: [**no**] **vpn-idle-timeout** *<minutes>* | **none**	Converted to **group-policy** syntax
	vpngroup *<group_name>* **max-time** *<max_seconds>*	In the group-policy attribute configuration mode: [**no**] **vpn-session-timeout** *<minutes>* | **none**	Converted to **group-policy** syntax
	vpngroup *<group_name>* **password** *<preshared_key>*	**tunnel-group** *<group name>* **type ipsec-ra** **tunnel-group** *<group name>* **ipsec-attributes** **pre-shared-key** *<preshared key>*	Converted to **tunnel-group** syntax
	vpngroup *<group_name>* **pfs**	In the group-policy attribute configuration mode: **pfs** <enable|disable>	Converted to **group-policy** syntax
	vpngroup *<group_name>* **secure-unit-authentication**	In the group-policy attribute configuration mode: **secure-unit-authentication** <enable|disable>	Converted to **group-policy** syntax
	vpngroup *<group_name>* **split-dns** *<domain_name1>* [*<domain_name2> ... <domain_name8>*]	In the group-policy attribute configuration mode: [**no**] **split-dns value** *<domain_name1 domain_name2 ... domain_nameN>*	Converted to **group-policy** syntax
	vpngroup *<group_name>* **split-tunnel** *<access_list>*	In the group-policy attribute configuration mode: **[no] split-tunnel-network-list value** *<access-list name>*	Converted to **group-policy** syntax

Table 17 Changes in the vpngroup Command (continued)

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
	vpngroup <*group_name*> **user-authentication**	In the group-policy attribute configuration mode: **user-authentication** <enable|disable>	Converted to **group-policy** syntax
	vpngroup <*group_name*> **user-idle-timeout** <*user_idle_seconds*>	In the group-policy attribute configuration mode: [**no**] **user-authentication-idle-timeout** <*minutes*> | **none**	Converted to **group-policy** syntax
	vpngroup <*group_name*> **wins-server** <*wins_ip_prim*> [<*wins_ip_sec*>]	In the group-policy attribute configuration mode: [**no**] **wins-server value** <*ip_address*> [ip_address]	Converted to **group-policy** syntax
	show vpngroup [<*group_name*>]	**show running-config** [default] **tunnel-group** [<name> [**general-attributes** | **ipsec-attributes** | **ppp-attributes**]] **show running-config** [**default**] **group-policy** [<name> [**attributes**]]	Converted to **tunnel-group** and **group-policy** syntax; both commands are used to replace the **vpngroup** command.

Change Impact

This section describes the impact that the changes will have on the CLI commands in PIX Security appliance Version 7.0.

- **Trustpoints**—The concept and syntax of a trustpoint are new for PIX Security appliance Version 7.0. A trustpoint consists of a CA certificate/identity certificate pair and allows the configuration and use of multiple CA certificates and therefore multiple identity certificates on PIX Security appliance Version 7.0. PIX Version 6.3 only supported the configuration and use of a single identity certificate. The following is an example of how the CLI has changed:

  PIX Version 6.3 syntax:

  ```
  ca identity myca 10.10.10.100 10.10.10.110
  ca configure myca ca 3 3
  ```

  The PIX Security appliance Version 7.0 syntax:

  ```
  crypto ca trustpoint myca
      enroll url 10.10.10.100
      enrollment mode ca
      enrollment retry period 3
      enrollment retry count 3
      crl required
      crl
          ldap_defaults 10.10.10.110
          exit
     exit
  ```

- **Group Management**—The **vpngroup** command is being replaced by the **tunnel-group** and **group-policy** commands. The split of configuration data between the tunnel-group and group-policy is intended to facilitate the sharing of group policies. The tunnel group is generally tied to a VPN peer or group of peers. The group policy is then applied to either a single tunnel group or several tunnel groups.

An additional benefit is that the group policy can be stored or maintained on an external policy server. All uses of the **vpngroup** command automatically convert to **tunnel-group** and **group-policy** commands. Here is an example of some **vpngroup** commands converted to the new syntax:

PIX Version 6.3 syntax:

```
vpngroup group1 address-pool pool1
vpngroup group1 password mypassword
```

The PIX Security appliance Version 7.0 syntax:

```
tunnel-group group1 type ipsec-ra
tunnel-group group1 general-attributes
address-pool pool1
tunnel-group group1 ipsec-attributes
pre-shared-key mypassword
```

PIX Version 6.3 syntax:

```
crypto map map_name client authenticate aaa_server_group_name
```

The PIX Security appliance Version 7.0 syntax:

```
tunnel-group group1 type ipsec-ra
tunnel-group group1 general-attributes
authentication-server-group myservergroup
```

- **PPP User Configuration**—The configuration of PPP users through the **vpdn** command is no longer supported, and the command is not supported in PIX Security appliance Version 7.0.
- **Remote Peers**— After upgrading from PIX Version 6.3 to PIX Security appliance Version 7.0, connections fail on the PIX terminating the remote connections from the IOS peers on the dynamic crypto map with certificates. The solution is to change the configuration to force the connecting IOS peers into the ipsec-l2l group.

  The following example shows the output when you enter the **debug crypto isakmp 50** command, after you perform an upgrade to PIX Security appliance Version 7.0:

  ```
  ...
  [IKEv1], IP = x.x.x.x , Connection landed on tunnel_group DefaultRAGroup
  [IKEv1], Group = DefaultRAGroup, IP = x.x.x.x Xauth
  required but selected Proposal does not support xauth,  Check
  priorities of ike xauth proposals in ike proposal list,
  ...
  ```
- **Xauth Disabled/Enabled**—In PIX Version 6.3, Xauth was disabled by default for dynamic or remote access (client) tunnels, so unless you were using Xauth, there would be no indication of it in your configuration. When you upgrade to PIX Security appliance Version 7.0, the default remote access tunnel-group has Xauth enabled by default, and attempts to authenticate tunnels to the local database. PIX Version 6.3 if you terminate dynamic VPN tunnels without Xauth, you must add the following information to your configuration after upgrading to stop Xauth:

For the default group:

```
tunnel-group DefaultRAGroup general-attributes
   authentication-server-group none
```

If any additional tunnel-groups were converted, you should add the following command to each tunnel-group:

```
tunnel-group <group_name> general-attributes
   authentication-server-group none
```

Failover

A number of changes have been introduced in the commands used to manage high availability on your security appliance. The primary reason for changes to the **failover** commands in PIX Security appliance Version 7.0 is to unify the command interface of the Cisco Service Module and the security appliance.

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, as PIX Security appliance Version 7.0 does not support this configuration. The PIX Security appliance Version 7.0 treats the LAN failover and Stateful Failover update interfaces as special interfaces. In PIX Version 6.3 when an interface shares both regular traffic and Stateful Failover updates, the configuration related to the regular traffic interface will be lost after the upgrade if you do not change your configuration. The lost configuration may prevent you from connecting to the security appliance over the network.**

This section includes the following topics:

- Important Notes, page 3-39
- Affected Commands, page 3-40
- Upgrade Requirements, page 3-40
- Command Change Description, page 3-40

Important Notes

Sharing a Stateful Failover failover interface with a regular firewall interface is not a supported configuration in PIX Security appliance Version 7.0. This restriction was not enforced in PIX Version 6.3 and earlier versions. If you have configured your PIX for shared use, the configuration related to the firewall interface will be lost after upgrade to PIX Security appliance Version 7.0.

For example, if you upgrade the PIX with a configuration file containing the following lines:

```
nameif ethernet1 inside security100
failover link inside
static (inside,outside) 172.33.12.10 192.168.10.1 netmask 255.255.255.255 0 0
```

interface ‘inside’ is used for both Stateful Failover and regular traffic. The line with the **static** command or any other commands which use interface ‘inside’ will be lost after an upgrade.

To avoid configuration loss, before upgrading to PIX Security appliance Version 7.0, move the Stateful Failover to a separate physical interface, or disable Stateful Failover by issuing the **no failover link** <*interface*> command and save the configuration to Flash memory using the **write memory** command.

Affected Commands

The following command is affected in the upgrade to PIX Security appliance Version 7.0:

- **failover**

Upgrade Requirements

All **failover** commands convert automatically when upgrading to PIX Security appliance Version 7.0. No manual intervention is required.

Note In PIX Security appliance Version 7.0, both the crossover cable and serial failover cable are supported in Active/Active failover configurations.

Command Change Description

Table 18 lists the changes in the **failover** command.

failover

Table 18 Changes in the failover Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
failover	**failover poll** *<sec>*	**failover polltime** [**unit**] [**msec**] *<sec_and_msec>* [**holdtime** *<sec>*]	—
	no failover poll [*<sec>*]	**no failover polltime unit**| **interface** [*<sec>*]	—
	[no] failover ip address *<intf>* [*<ipaddr>*]	Not supported	Use the IP address ‘standby’ option of the **interface** command
	failover lan interface *<intf>*	**[no] failover lan interface** *<intf>* *<main_or_sub_intf>*	—
	failover link <intf>	**failover link** <intf> [<main_or_sub_intf>]	—
	failover lan key *<secret>*	**[no] failover key** *<key>*	—

Change Impact

This section describes the effect that the failover changes will have on the CLI commands in PIX Security appliance Version 7.0.

- The **failover ip address** command has been replaced with the standby option of the **ip address** configuration mode command under the **interface** command. For example:

  PIX Version 6.3 syntax:

  ```
  interface ethernet0 100full
  ```

```
nameif ethernet0 outside security0
ip address outside 10.0.1.1 255.255.0.0
failover ip address outside 10.0.1.11
```

The PIX Security appliance Version 7.0 syntax:

```
interface e0
  nameif outside
  ip address 10.0.1.1 255.255.255.0 standby 10.0.1.11
  exit
!
```

- The **failover lan** interface and **failover link** command also have similar changes.

  PIX Version 6.3 syntax:

  ```
  interface ethernet3 auto
  nameif ethernet3 stlink security0
  ip address stlink 10.0.4.1 255.255.0.0
  failover ip address stlink 10.0.4.11
  failover link stlink
  interface ethernet4 auto
  nameif ethernet4 folink security0
  ip address folink 10.0.5.1 255.255.0.0
  failover ip address outside 10.0.5.11
  failover lan int folink
  ```

  The PIX Security appliance Version 7.0 syntax:

  ```
  failover lan interface folink e4
  failover link stlink e3
  failover interface ip folink 10.0.5.1 255.255.255.0 standby 10.0.5.11
  failover interface ip stlink 10.0.4.1 255.255.255.0 standby 10.0.4.11
  ```

- In PIX Security appliance Version 7.0, the **failover lan key** <*key*> command changed to the **failover key** <*key*> command. In PIX Version 6.3, the failover encryption message was applicable only to LAN failover. In PIX Security appliance Version 7.0, the failover encryption message is also applicable to a serial cable failover. The **lan** keyword has been removed, since the **failover key** <*key*> command now supports both LAN and serial encryption failover.
- In PIX Version 6.3, the **failover poll** command specified only the unit setting; the **unit** keyword was omitted because it was implied. In PIX Security appliance Version 7.0, support for **holdtime** has been added, so **unit** and the **holdtime** keywords have been added. PIX Version 6.3 syntax (**failover poll 3,** for example) is still accepted, and will be automatically converted (**failover polltime unit 3 holdtime 9**, for example) in PIX Security appliance Version 7.0.
- In PIX Security appliance Version 7.0, the failover key must be configured for VPN Failover to be enabled. If the key is not configured, VPN Failover is automatically disabled. Once the key is configured, VPN Failover is functional again. This change was implemented for security reasons.

AAA

The AAA CLI includes configuration of parameters for the following functions, although not all functions are directly affected by the changes:

- VPN Remote Access users (IPSec, L2TP over IPSec)
- Cut-through authentication proxies for FTP, Telnet, HTTP, and HTTPS
- Device management

There are a number of changes to the AAA commands as well as a paradigm shift that will impact how you configure AAA in PIX Security appliance Version 7.0. The paradigm shift is a change in how server specific parameters are set. In PIX Version 6.3, server parameters were configured per server group. In PIX Security appliance Version 7.0, server parameters can be configured per AAA host with some parameters being configurable only for the entire AAA server group.

There is also a paradigm shift in the way that AAA server groups are mapped to VPN tunnels. (See the "VPN" section on page 3-27 for information on these changes).

This section breaks down the AAA migration, and includes the following topics:

- Affected Commands, page 3-42
- Upgrade Requirements, page 3-42
- Command Change Description, page 3-42
- Change Impact, page 3-44

Affected Commands

The following commands are affected in the upgrade to PIX Security appliance Version 7.0:

- **aaa-server**
- **aaa-server radius-acctport**
- **aaa-server radius-authport**
- **auth-prompt**
- **floodguard**

Upgrade Requirements

The **aaa** commands convert automatically when upgrading to PIX Security appliance Version 7.0. No manual intervention is required.

Note In PIX Security appliance Version 7.0, the FTP connection is reset immediately when authorization deny is configured. In PIX Version 6.3, PIX provided an FTP login before denying authorization.

Command Change Description

Table 19 lists changes in the **aaa-server** command, Table 20 lists changes in the **auth-prompt** command, and Table 21 lists changes in the **floodguard** command.

aaa-server

Table 19 Changes in the aaa-server Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
aaa-server	**[no] aaa-server radius-acctport** [<*acct_port*>]	**aaa-server** <*group tag*> [<(*if_name*)>] **host** <server ip> [**no**] **accounting-port** <*port*>	The radius-acctport and radius-authport values are now configured as part of the **aaa-server** host-specific configuration mode commands These settings are now host-based; they were server-group based previously.
	[no] aaa-server radius-authport [<*auth_port*>]	**aaa-server** <*group tag*> [<(*if_name*)>] **host** <*server ip*> [**no**] **authentication-port** <*port*>	
	aaa-server <group name> [(if_name)] **host server_ip** [key] [timeout seconds]	**aaa-server** <group name> [(if_name)] **host server_ip** **key** <key> **timeout** <seconds>	The **aaa-server** configuration mode command has added the two new configuration mode commands (**key** and **timeout**)

auth-prompt

Table 20 Changes in the auth-prompt Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
auth-prompt	**auth-prompt** {<*prompt*> | **accept** | **reject**} **<***text***>**	**auth-prompt** {**prompt** | **accept** | **reject**} <*text*>	One of the following keywords is now mandatory: **{prompt | accept | reject}**
	no auth-prompt [<*prompt*> | **accept** | **reject**][<*text*>]	**no auth-prompt** {**prompt** | **accept** | **reject**} [<*text*>]	One of the following keywords is now mandatory: **{prompt | accept | reject}**

floodguard

Table 21 Changes in the floodguard Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
floodguard	**[no] floodguard [enable|disable]**	Not supported	The following message will be displayed: "This command is no longer needed. The **floodguard** feature is always enabled."
	show run floodguard		
	clear config floodguard		

Change Impact

This section describes the impact that the changes will have on the CLI commands in PIX Security appliance Version 7.0.

- The PIX Security appliance Version 7.0 allows most AAA server configuration parameters to be configured per host. This has resulted in the **aaa server** command having two configuration modes, a host configuration mode for configuring AAA host specific parameters and a group configuration mode for configuring parameters that can only be applied to the entire AAA server group.

  Here is an example:

```
aaa-server svrgrp1 protocol radius
aaa-server svrgrp1 host 10.10.10.1
timeout 30
retry 3
exit
aaa-server svrgrp1 host 10.10.10.2
timeout 60
retry 3
exit
```

- In PIX Security appliance Version 7.0, the following command forms have been deprecated:
  - **[no] aaa-server radius-authport [auth_port]**
  - **[no] aaa-server radius-acctport [acct_port]**

  These commands, which only apply to server groups that contain RADIUS servers, have changed semantically. Because they are being deprecated, they will not be written to the configuration file. These commands can be used to override the default RADIUS authentication and accounting ports for all servers (the implicit defaults are port 1645 and 1646 respectively). This global port setting can then be overridden by the host-specific configuration mode command.
- In PIX Version 6.3, cut-through proxies intercepted traffic going to ports 80 or 8080. With PIX Security appliance Version 7.0, cut-through proxies check local ports in static mode, then intercept and launch web authentication for traffic destined to any global port, only if the local port is port 80.

  Examples:
  - Case 1:

    If the outside PAT port is set up as 666 (and ACLs are set up accordingly)

    static (inside, outside) tcp tcp 10.48.66.155

    666 192.168.123.10 www.netmask 255.255.255.255

    When a client web browser attempts to access 10.48.66.155 on port 666, the authentication prompt appears.
  - Case 2:

    If the local port is different than port 80, instead of an authentication prompt, the following standard error message appears: 'must be authenticated before using that service'

    static (inside,outside) tcp 10.48.66.155 666 192.168.123.10 111 netmask 255.255.255.255

Management

A number of changes have been introduced in the commands used to manage your PIX system, along with the introduction of a new Flash filesystem. For more information on the new Flash filesystem and its commands and features, go to the *Cisco PIX Security Appliance Command Reference, Version 7.0* guide and the *Cisco Security Appliance CLI Configuration Guide, Version 7.0*.

This section includes the following topics:

- Affected Commands, page 3-45
- Upgrade Requirements, page 3-45
- Command Change Description, page 3-45
- Change Impact, page 3-47

Affected Commands

The following commands are affected in the upgrade to PIX Security appliance Version 7.0:

- **clear flashfs**
- **copy capture**
- **crashinfo**
- **dhcpd auto_config**
- **pager**
- **pdm location**
- **pdm group**
- **pdm logging**
- **show flashfs**
- **ssh**
- **telnet**
- **tftp-server**

Upgrade Requirements

The management commands convert automatically when upgrading to PIX Security appliance Version 7.0. No manual intervention is required.

Command Change Description

Table 22 lists changes in the **copy** command, Table 23 lists changes in the **dhcp** command, Table 24 lists changes in the **pager** command, Table 25 lists changes in the **ssh** command, Table 26 lists changes in the **telnet** command, and Table 27 lists changes in the **tftp-server** command.

copy

Table 22 Changes in copy Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
copy	**copy capture:buffer name tftp URL [pcap]**	**copy** [/**pcap**] **capture**:<*bufferSpec*> <*URL*>	<*bufferSpec*>:= <*buffername*> in single mode [<*context name*>/]<*buffername*> in multimode

Note The **copy** command in PIX Version 6.3 has been extended to the new Flash filesystem, and has been implemented using the new parser. The syntax has changed for the **copy** options in PIX Security appliance Version 7.0. The **copy** options were at the end of the **copy** command in PIX Version 6.3.

dhcpd

Table 23 Changes in the dhcpd Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
dhcpd	**[no] dhcpd auto_config** [<*intf*>]	**[no] dhcpd auto_config** <*intf*>	'intf' is now a mandatory parameter

pager

Table 24 Changes in the pager Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
pager	**terminal pager lines** <*lines*>	**terminal pager** [lines] <*lines*>	Modification in existing EXEC mode command to make **lines** keyword optional
	[no] pager lines <*lines*>	**[no] pager [lines]** <*lines*>	

ssh

Table 25 Changes in the ssh Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
ssh	[**no**] **ssh** <*local_ip*> [<*mask*> [<*if_name*>]]	[**no**] **ssh** <*local_ip*> <*mask*> <*if_name*>	'mask' and 'if_name' are now mandatory parameters

telnet

Table 26 Changes in telnet Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
telnet	**[no] telnet** <*local_ip*> [<*mask*> [<*if_name*>]]	**[no] telnet** <*local_ip*> <*mask*> <*if_name*>	'mask' and 'if_name' are now mandatory parameters

In PIX Security appliance Version 7.0, the **no telnet timeout** [<num>] command sets the telnet timeout back to the default, which is 5. The **clear conf telnet** command also returns the telnet timeout back to the default.

In PIX Security appliance Version 7.0, the output for the **help telnet** and **telnet timeout ?** commands has been augmented to include the default value.

Example of output for the **telnet timeout ?** command:

```
sw1-535(config)# telnet timeout 1
sw1-535(config)# telnet 0 0 inside
sw1-535(config)# sho run telnet
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 1
sw1-535(config)# no telnet timeout
sw1-535(config)# sho run telnet
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 5
sw1-535(config)# telnet timeout 1
sw1-535(config)# sho run telnet
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 1
sw1-535(config)# clear conf telnet
sw1-535(config)# sho run telnet
telnet timeout 5
sw1-535(config)#
```

tftp-server

Table 27 Changes in the tftp-server Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
tftp-server	**tftp-server** [<*if_name*>] <*ip*> <*dir*>	**[no] tftp-server** <*if_name*> <*ip*> <*dir*>	'if_name' is now a mandatory parameter
	clear tftp-server	Deprecated	Use the **no** command to clear the TFTP server

Change Impact

This section details the changes in Flash filesystem commands and caveats.

- For all of the commands, if a full path is not provided, then the path is assumed to be relative to the current working directory.
- The **/noconfirm** option suppresses the confirmation prompts for filesystem commands.

- Filesystem commands are replicated to the standby unit in PIX Security appliance Version 7.0.These are **rename**, **mkdir**, **rmdir**, **delete**, **copy running-config startup- config** commands.

  Following are salient features of implementation in PIX Security appliance Version 7.0:

  - Both the **write memory** and the **copy running start** commands are replicated.
  - Replication is disabled for the **write memory** command as the **copy** command is in turn replicated.
  - No configuration sync occurs between the active and standby devices when a filesystem command fails on the standby device. A configuration sync would not help because the filesystem commands are not part of the configuration. When a filesystem command fails on the standby device, an informational message is displayed, noting that the filesystem may be out of sync.
  - The **format** command is not replicated.

Note For compatibility with PIX, [flash:image] matches the first local file, configured using the **boot system** command, and [flash:pdm] matches the file configured using **pdm image** command.

OSPF

With the introduction of **interface** configuration mode in PIX Security appliance Version 7.0, interface specific OSPF parameters are now configured in the **interface** configuration mode.

This section includes the following topics:

- Affected Commands, page 3-48
- Upgrade Requirements, page 3-48
- Command Change Description, page 3-49
- Change Impact, page 3-49

Affected Commands

The following commands are affected in the upgrade to PIX Security appliance Version 7.0:

- **ospf** configuration mode commands under the **routing interface** command
- **set ip next-hop**
- **set metric-type**

Upgrade Requirements

The **ospf** configuration mode commands under the **routing interface** command convert automatically when upgrading to PIX Security appliance Version 7.0. No manual intervention is necessary.

Command Change Description

- The **set ip next-hop** command was used only for policy routing and has been removed because the PIX Security appliance Version 7.0 does not support policy routing.
- The **set metric-type** command is used to set the metric type for OSPF route redistribution in PIX Security appliance Version 7.0, as follows:

  ```
  Pix(config-route-map)# set metric-type {type-1 | type-2}
  ```

  Example:

  ```
  hostname(config)# route-map 1-to-2 permit
  hostname(config-route-map)# match metric 1
  hostname(config-route-map)# set metric 5
  hostname(config-route-map)# set metric-type type-1
  ```

- The following example illustrates the difference in syntax for the **ospf** configuration mode commands:

  PIX Version 6.3

  ```
  routing interface outside
  ospf ...
  ```

  The PIX Security appliance Version 7.0

  ```
  interface ethernet0
  ospf ...
  ```

Note Note the difference in interface names; PIX Version 6.3 specifies the interface name as provided by the **nameif** command, while PIX Security appliance Version 7.0 uses physical interface names.

Change Impact

The **ospf** configuration mode commands under the **routing interface** command are converted automatically to the interface configuration mode when upgrading to PIX Security appliance Version 7.0. The **set ip next-hop** and **set metric-type** commands are automatically dropped.

Media Gateway Control Protocol (MGCP)

With the introduction of Modular Policy Framework (MPF), all **fixup** commands including **fixup mgcp** have been converted to **inspect** commands under MPF (see the "Fixups/Inspect" section on page 3-17). Also, the existing Media Gateway Control Protocol (MGCP) commands have been moved under the **mgcp-map** command to fit into the MPF framework.

This section includes the following topics:

- Affected Commands, page 3-50
- Upgrade Requirements, page 3-50
- Configuring class-map, mgcp-map and policy-map for MGCP, page 3-50

Affected Commands

The following command is affected in the upgrade to PIX Security appliance Version 7.0:

- **mgcp**

Upgrade Requirements

The existing **mgcp** commands have been deprecated, and the commands under **mgcp-map** in the MPF framework are replacing them. In PIX Security appliance Version 7.0, the **mgcp** commands convert automatically. No manual intervention is required.

The **mgcp-map** command (shown in the following example) is optional and needs to be configured only if call-agents/gateways/command-queue are specified.

mgcp-map mgcp-policy (Optional)

```
[no] call-agent <ip-address> <group-id>
[no] gateway <ip-address> <group-id>
command-queue <limit>
```

PIX Version 6.3	PIX Security appliance Version 7.0
mgcp call-agent *<ip-address> <group-id>* **mgcp gateway** *<ip-address> <group-id>* **mgcp command-queue** *<limit>*	**mgcp-map mgcp-policy** **call-agent** *<ip-address> <group-id>* **gateway** *<ip-address>* **<group-d>** **command-queue** *<limit>*

The **mgcp-policy** configured as shown in the preceding table is then included in the **inspect mgcp** command:

```
inspect mgcp mgcp-policy
```

See the following procedure for a complete configuration steps.

Configuring class-map, mgcp-map and policy-map for MGCP

To configure **class-map**, **mgcp-map** and **policy-map** for MGCP, perform the following steps:

Step 1 Define a traffic class to match all traffic on port 2427:

```
class-map f1_mgcp_class
match port 2427
```

or,

create an ACL to classify all MGCP traffic. MGCP traffic uses ports 2427 and 2727:

```
access-list f1_mgcp_class permit udp any any eq 2427
access-list f1_mgcp_class permit udp any eq 2427 any
class-map f1_mgcp_class
match access-list f1_mgcp_class
access-list f1_mgcp_class1 permit udp any any eq 2727
access-list f1_mgcp_class1 permit udp any eq 2727 any
class-map f1_mgcp_class1
match access-list f1_mgcp_class1
```

The following **mgcp-map** command is the new CLI for the existing **mgcp** commands:

```
mgcp-map mgcp-policy (optional)
call-agent <ip-address> <group-id>
gateway <ip-address> <group-id>
command-queue <limit>
```

Step 2 Configure the policy-map on the traffic class to perform an MGCP inspection.

```
policy-map inspection_policy
class f1_mgcp_class
inspect mgcp mgcp-policy
```

Step 3 Activate the policy by applying it globally.

```
service-policy inspection-policy global
```

The existing **show** command for **mgcp** will be carried over to PIX Security appliance Version 7.0.

```
show mgcp {commands|sessions} [detail]
```

The same output should also be shown in the **show service-policy inspect mgcp** command.

Multicast

To accommodate PIM Sparse Mode (PIM-SM) in PIX Security appliance Version 7.0 and to align the PIX and Cisco IOS software multicast implementations, a few changes have been made to the CLI **multicast** commands.

This section includes the following topics:

- Background, page 3-51
- Affected Commands, page 3-52
- Upgrade Requirements, page 3-52
- Command Change Description, page 3-52
- Change Impact, page 3-53

Background

PIX Version 6.2 introduced Stub Multicast Routing (SMR) with native multicast support including IGMP, static multicast routes, driver enhancements, a multicast forwarding information base (MFIB), and a multicast-forwarding engine (MFWD) to make forwarding and policy decisions. This allowed directly connected receivers to dynamically join multicast groups and receive data by forwarding host reports to an upstream router running a multicast routing protocol like PIM. The upstream router would notify the multicast traffic sources of the receivers interest in receiving data. The host reports were added directly to the MFIB to set up delivery. Static mroutes were provided to facilitate sourcing of multicast data. These mechanisms presented some scaling challenges for sites which did not have directly connected receivers. In addition, directly-connected multicast traffic sources required NAT and the operation of dense mode protocols.

Affected Commands

The following commands are affected when you upgrade to PIX Security appliance Version 7.0:

- **mroute**
- **multicast interface**
- **igmp max-groups**

Upgrade Requirements

You should review your multicast configuration and leverage PIM-SM, now that PIX supports PIM-SM. If you had deployed PIX Version 6.2 or PIX Version 6.3 and were providing a firewall for directly-connected multicast traffic sources, you should migrate to a PIM-SM configuration.

Command Change Description

Table 28 lists the changes to the **mroute** command, Table 29 lists changes in the **igmp max-groups** command, and Table 30 lists changes to the **multicast** command.

mroute

Table 28 Changes in the mroute Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
mroute	**mroute** <src> <smask> <interface-name> <dst> <dmask> <interface-name>	**mroute** <src> <smask> <interlace-name> [dense <interface-name>] [distance]	Automatically converted upon upgrade.

igmp max-groups

Table 29 Changes in the igmp max-groups Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
igmp max-groups	**igmp max-groups** <number>	**igmp limit** <number>	Automatically converted upon upgrade. New default of 500 groups.

multicast

Table 30 Changes in the multicast Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
multicast	**multicast interface** <interface-name>	Not Supported	Automatically converted upon upgrade.

Change Impact

The changes to the **mroute**, **igmp max-groups**, and **multicast** commands bring them inline with the Cisco IOS software CLI.

mroute

When upgrading from PIX Version 6.3, the **mroute** command is converted automatically to the new format. You can leverage the extended **mroute** syntax that supports **multicast** sources directly connected to the PIX, and change the syntax to leverage PIM-SM to avoid dense mode flooding and related scalability issues. See the PIM-SM section in the *Cisco Security Appliance Command Line Configuration Guide* for further information.

When removing the <dst> <dmask> option, all multicast groups sourced from the <src> IP address are converted automatically to the new format.

The following configurations are converted automatically to the new format, however, the behavior may differ slightly from the original intent.

```
mroute 1.0.0.0 255.0.0.0 inside 224.1.1.0 255.255.255.0 outside
mroute 1.0.0.0 255.0.0.0 inside 224.2.2.0 255.255.255.0 dmz
```

Assuming IGMP forwarding had not been configured, the converted configuration will be as follows:

```
mroute 1.0.0.0 255.0.0.0 dmz
```

The **dense** mode option is only relevant when using PIX Security appliance Version 7.0 Stub Multicast Routing (SMR). The **dense** keyword is accepted for all **mroute** commands, but is only effective when SMR is enabled.

If you enable PIM-SM, the output interface on the **mroute** command is ignored from a functional standpoint.

igmp max-groups

When upgrading from PIX Version 6.3, the **igmp max-groups** command is converted automatically to the new **igmp limit** command. The default limit has changes from 2000 to 500. If the configuration limit has not been specified, the default is 500. If the configuration specifies a limit, it carries forward seamlessly.

multicast

The **multicast** command and its related **multicast** configuration mode commands are converted automatically to **interface** configuration mode.

For example, if a PIX 515E device running a PIX Version 6.3 configuration includes the following multicast configuration snippet:

```
.
multicast interface outside
multicast interface inside
igmp forward interface outside
.
.
.
```

then, the configuration is converted to the following upon upgrade to PIX Security appliance Version 7.0:

```
multicast-routing
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.3.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 igmp forward interface outside
!
```

The preceding assumes that you have ethernet0 as your outside interface and ethernet1 as your inside interface with the example security levels and IP addresses. The conversion result may differ slightly depending on the specific interface, security level and IP addresses of the affected interfaces.

NAT

This section describes the following changes for the NAT feature:

- NAT Control, page 3-54
- Connection Limits, page 3-54
- Reverse-Path Forwarding Check, page 3-55

NAT Control

In PIX Version 6.3, you must configure NAT on the inside hosts, when hosts on a higher security interface (inside) communicate with hosts on a lower security interface (outside). In PIX Security appliance Version 7.0, this NAT control can be disabled; you can still configure NAT, but NAT is not required for communication. For example, if you disable NAT control, you do not need to configure a static NAT statement for outside hosts to connect to an inside host.

The **nat-control** command introduced in PIX Security appliance Version 7.0 automatically incorporates PIX Version 6.3 NAT control functionality into PIX Security appliance Version 7.0. To disable NAT control, enter the **no nat-control** command.

When you upgrade to PIX Security appliance Version 7.0, the new **nat-control** command is automatically incorporated into the configuration. No manual intervention is required.

Connection Limits

In PIX Security appliance Version 7.0, the tcp_max_conns and udp_max_conns arguments to the **nat** and **static** commands are applied to the last configuration entity that includes a local_host in the scope of its real_ip range. Since the static statements follow the nat statements; if there is an overlap in the real_ip ranges of the nat and static statements, the static limits take precedence because they are listed after the nat statements in the configuration.

For example, if you have the following configuration in the PIX Security appliance Version 7.0:

```
nat (inside) 1 10.10.12.0 255.255.255.0 50 10
```

```
static (inside,dmz) 10.0.0.0 10.0.0.0 netmask 255.0.0.0
```

The tcp_max_conns, udp_max_conns, and emb_limit variables will be applied according to the static statement (unlimited) because the static section follows the nat section in the configuration.

For PIX Version 6.3 and earlier, the max_conns and emb_limit variables (there was no udp_max_conns before PIX Security appliance Version 7.0) were applied to a local-host depending upon which xlate was created for a local host. So in PIX Version 6.3, if you have the following configuration:

```
global (outside) 1 interface
nat (inside) 1 10.10.12.0 255.255.255.0 50 10
static (inside,dmz) 10.0.0.0 10.0.0.0 netmask 255.0.0.0
```

In the above example, assume that the local_host addressed at 10.10.12.99 does not have an xlate created yet. If that host initiates a connection to the outside first, that local_host will have the 50 and 10 max_conns and emb_limit limits applied. If that host initiates a connection to the dmz first, it will have the unlimited max_conns and emb_limit limits applied.

Reverse-Path Forwarding Check

In Version 6.3 and earlier, some NAT misconfigurations went unnoticed because the software did not check the reverse-path forwarding; specifically, if you try to connect directly to the real address when there is a NAT rule for that address, the packet should be dropped. In PIX Security appliance Version 7.0, reverse-path forwarding is enforced.$

For example, the following configuration is a misconfiguration because the NAT exemption rule addresses overlap with a static rule:

```
access-list NONAT permit 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0
nat (inside) 0 access-list NONAT
static (inside,dmz) 209.165.201.1 10.1.100.67 netmask 255.255.255.255
```

If a host on DMZ, 10.2.2.2, Telnets to a server on the inside using mapped address 209.165.201.1, then the packet hits the static NAT rule, and 209.165.201.1 is translated to the real server address, 10.1.100.67. When the server responds to the DMZ host, the packet from 10.1.100.67 to 10.2.2.2 hits the (higher priority) NAT exemption rule, so the source address is not mapped back to 209.165.201.1. Version 6.3 and earlier let the return traffic back to the DMZ host, even though the source address was the real address instead of the mapped address. PIX Security appliance Version 7.0 enforces the reverse-path forwarding, and drops the packet.

Public Key Infrastructure (PKI)

The certification authority (**ca**) commands have been modified to incorporate more PKI features and to make them look more like Cisco IOS software commands. To do this, the Cisco IOS software concept of trustpoints was introduced in PIX Security appliance Version 7.0. A trustpoint is the representation of a certification authority (CA) certificate/identity certificate pair and contains:

- The identity of the CA
- CA specific configuration parameters
- An association with one enrolled identity certificate

In PIX Security appliance Version 7.0, there are two key changes:

- In PIX Version 6.3, the PKI commands were rooted on the **ca** keyword, but in PIX Security appliance Version 7.0, the commands are now rooted in the **crypto** keyword.

- In PIX Version 6.3, the certificates were stored in a private hidden data file, but in PIX Security appliance Version 7.0, they are in the configuration file and are rooted on the **crypto** command tree.

  The behavior of any **clear config** <*keyword*> command is to remove all lines from the running configuration that are rooted on <*keyword*>. In PIX Security appliance Version 7.0, the **clear config crypto** command removes the certificates, trustpoints, and certificate maps, because they are in this command tree.

  In PIX Security appliance Version 7.0, the **clear configure crypto** command has been introduced and is replacing the **clear crypto** command. Trustpoints, introduced in PIX Security appliance Version 7.0, were referred to as CA identities in PIX Version 6.3, and were configured using the **ca identity** command.

Table 31 lists the deprecated PKI commands and their reason for becoming deprecated:

Table 31 PKI Deprecated Commands and the Rationale for Deprecation

PIX Version 6.3 Command	Reason for Deprecation in PIX Security appliance Version 7.0
ca generate rsa key <size>	Replaced by the **crypto key** command to align more closely with Cisco IOS CLI command syntax and functionality
ca generate rsa specialkey <size>	
ca zeroize rsa	
ca identity <name> **<**ip_address|hostname> [:<ca_script_location>] [<ldap_ip|hostname>]	Replaced by the **crypto ca trustpoint** command to align more closely with the Cisco IOS CLI command syntax and functionality
no ca identity <name>	
ca configure <name> [**ca|ra** <retry_period> <retry_count> [**crloptional**]]	
ca enroll <name> <password> **[serial] [ipaddress]**	
[no] ca subject name <name><X.500 string>	
ca authenticate <name> [<fingerprint>]	Replaced by the **crypto ca** command to align more closely with the Cisco IOS CLI **PKI** command syntax and functionality
ca crl request <id_name>	
ca verifycertdn <x.500 string>	

This section includes the following topics:

- Affected Commands, page 3-56
- Upgrade Requirements, page 3-57
- Command Change Description, page 3-57
- Change Impact, page 3-59

Affected Commands

- **ca generate/ca zeroize**
- **ca identity/ca configure**
- **ca authenticate**
- **ca enroll**
- **ca crl**

- **ca subject-name**
- **ca save all**
- **ca verifycertdn**

Upgrade Requirements

The affected **ca** commands have been deprecated or support has been removed. In PIX Security appliance Version 7.0, the **ca** commands convert automatically. No manual intervention is required.

Command Change Description

Table 32 lists changes to the **ca generate** and **ca zeroize** commands, Table 33 lists changes to the **ca identity** and **ca configure** commands, Table 34 lists changes to the **ca authenticate** command, Table 35 lists changes in the **ca enroll** command, Table 36 lists changes in the **ca crl** command, Table 37 lists changes in the **ca subject-name** command, and Table 38 lists changes in the **ca verifycertdn** command.

ca generate/ ca zeroize

Table 32 Changes in the ca generate and ca zeroize Commands

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
ca generate	**ca generate rsa key** <size>	**crypto key generate rsa general-keys modulus** <size>	Deprecated
	ca generate rsa specialkey <size>	**crypto key generate rsa usage-keys modulus** <size>	
ca zeroize	**ca zeroize rsa**	**crypto key zeroize rsa**	

ca identify/ ca configure

Table 33 Changes in the ca identify and ca configure Commands

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
ca identity	**ca identity** <name> <ip_address|hostname> [:<ca_script_location>] [<ldap_ip|hostname>]	**crypto ca trustpoint** <name> **enroll url** <ip_address|hostname>[:<ca_script_location>] crl **ldap_defaults** <ldap_ip|hostname> exit exit	Deprecated
	no ca identity <name>	**no crypto ca trustpoint** <name>	
ca configure	**ca configure** <name> [**ca|ra** <retry_period> <retry_count> [**crloptional**]]	**crypto ca trustpoint** <name> enrollment mode <ca|ra> **enrollment retry period** <retry_period> **enrollment retry count** <retry_count> crl <optional|required> exit	

ca authenticate

Table 34 Changes in the ca authenticate Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
ca authenticate	**ca authenticate** <name> [<fingerprint>]	**crypto ca authenticate** <name> [<fingerprint>]	Deprecated

ca enroll

Table 35 Changes in the ca enroll Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
ca enroll	**ca enroll** <name> <password> **[serial] [ipaddress]**	**crypto ca trustpoint** <name> **[no] ip-address** <address> [no] serial-number **password** <password> exit **crypto ca enroll** <name>	Deprecated

ca crl

Table 36 Changes in the ca crl Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
ca crl	**ca crl request** <id_name>	**crypto ca crl request** <trustpoint>	Deprecated

ca subject-name

Table 37 Changes in the ca subject-name Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
ca subject-name	**[no] ca subject name** <name> <X.500 string>	**crypto ca trustpoint** <name> **[no] subject-name <**X.500 string>	Deprecated

ca save all

This command has been removed and like Cisco IOS commands, keys and certificate data are saved at the same time that the configuration is written to memory.

ca verifycertdn

Table 38 Changes in the ca verifycertdn Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
ca verifycertdn	**ca verifycertdn** <x.500 string>	**crypto ca verifycertdn** <x.500 string>	Deprecated
	no ca verifycertdn	**no crypto ca verifycertdn**	

Change Impact

The deprecated **ca** commands are converted automatically when upgrading to PIX Security appliance Version 7.0. There are also additional new **ca** commands. See the *Cisco PIX Security Appliance Command Reference, Version 7.0* for more information on the new **ca** commands.

Miscellaneous

Some other features and commands in PIX Security appliance Version 7.0 have changed, as described in this section.

- In PIX Version 6.3, the **clear flashfs** and **flashfs downgrade** *x.x* commands cleared the filesystem part of Flash memory in the PIX Security appliance Version 7.0, and the **show flashfs** command displayed the size in bytes of each filesystem sector and the current state of the filesystem.

  In PIX Security appliance Version 7.0, the **flashfs** commands are not supported; use the **show flash** command instead. The abbreviation for both the **show flashfs** and the **show flash** commands is **show flash**.
- In PIX Security appliance Version 7.0, some of the keywords of the **established** command have been deprecated.
- Some changes to the **sysopt** command have been introduced in PIX Security appliance Version 7.0.
- If you use PIX Version 6.3 with URL filtering, and you accepted the default timeout of 5 seconds for the **url-server** command, the **url-server** command is removed when upgrading to PIX Security appliance Version 7.0. The minimum timeout in PIX Security appliance Version 7.0 is 10 seconds, whereas the default timeout in PIX Version 6.3 was 5 seconds. Because the **url-server** command is

rejected, any **filter** commands will also be rejected. The solution is to re-enter the **url-server** command using a higher timeout value, such as 30 seconds, which is the default on PIX Security appliance Version 7.0, and then add back all the filter statements.

- In PIX Version 6.3, the TCP option 19 used by BGP MD5 was automatically allowed; however, in PIX Security appliance Version 7.0, an additional configuration is required to allow it.
- In PIX Version 6.3, the security appliance learned ARP entries for hosts that used SNAP encapsulation. In Version 7.0, SNAP encapsulation is not supported for ARP.

This section includes the following topics:

- Affected Commands, page 3-60
- Upgrade Requirements, page 3-60
- Command Change Description, page 3-60
- Change Impact, page 3-61

Affected Commands

- **established**
- **flashfs**
- **sysopt permit pptp | permit l2tp**

Upgrade Requirements

The **flashfs**, **clear flashfs**, and **show flashfs** commands in PIX Version 6.3 are EXEC mode commands, and are not saved in the configuration, therefore there is no need to convert them when upgrading to PIX Security appliance Version 7.0.

Command Change Description

Table 39 lists changes in the **established** command,Table 40 lists changes in the **flashfs** command, and and Table 41 lists changes in the **sysopt** command.

established

Table 39 Changes in the established Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
established	[**to** | **permitto** *<protocol> <port1>*[*-<port2>*]]	[**permitto** *<protocol> <port1>*[*-<port2>*]]	Keywords **to** and **from** have been deprecated; use **permitto** and **permitfrom** instead
	[**from** | **permitfrom** *<protocol> <port1>*[*-<port2>*]]}	[**permitfrom** *<protocol> <port1>*[*-<port2>*]]}	

flashfs

Table 40 Changes in flashfs Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
`flashfs`	`clear flashfs`	Not supported	—
	`flashfs`	Not supported	Use the **downgrade** command to load PIX Version 6.3 version
	`show flashfs`	`show flash`	The abbreviation for both the **show flashfs** and the **show flash** commands is **show flash**

sysopt

Table 41 Changes in the sysopt Command

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
`sysopt`	`[no] sysopt connection permit-pptp | permit-l2tp`	Not Supported	—

Change Impact

This section describes the impact that the changes will have in PIX Security appliance Version 7.0.

- The **to** and **from** keywords were removed from the **established** command, because although **to** and **from** were accepted in PIX Version 6.3, they were stored in **permitto** and **permitfrom** format. This allows the old configuration to be updated seamlessly. However, you now need to use **permitto** in place of **to** and **permitfrom** in place of **from**.
- There is no equivalent for the **clear flashfs** command in PIX Security appliance Version 7.0. Instead, use the **downgrade** command to load a PIX Version 6.3 version (See the "Guidelines for Downgrading" section on page 5-1 and the"Downgrade Procedure" section on page 5-1).

  For more information on the **clear** and **show** commands, see the "CLI Command Processor" section on page 3-6.
- The **permit-l2tp** and **permit-pptp** options in the **sysopt** command have been deprecated, and the **uauth allow-http-cache** option has been deprecated.
- In PIX Security appliance Version 7.0, the **sysopt connection permit-ipsec** option is enabled by default, and no longer allows VPN traffic to bypass the user/group ACLs; however, it does allow VPN traffic to bypass interface ACLs.

  If you had the **sysopt connection permit-ipsec** option set as a new line in your PIX Version 6.3 setting, that line will be automatically removed from your PIX Security appliance Version 7.0 configuration. Because the **sysopt connection permit-ipsec** option is enabled by default, you no longer need to specify it explicitly on a separate line. In PIX Security appliance Version 7.0, you use the **show running-configuration sysopt** command to display **sysopt** configurations settings which are set to their default value.

If you did not have the **sysopt connection permit-ipsec** option on a separate line in PIX Version 6.3, it is automatically added to your PIX Security appliance Version 7.0 configuration [DAA] if running in single firewall mode[/DAA]. The **sysopt connection permit-ipsec** option remains disabled (the PIX Version 6.3 default) and the behavior remains the same in PIX Security appliance Version 7.0.

- To enhance security for BGP, TCP option number 19 is used to carry an MD5 digest in a TCP segment. TCP option 19 is cleared by default by PIX Security appliance Version 7.0. In order to allow this TCP option, use the following configuration:

```
class-map BGP-MD5-CLASSMAP
     match port tcp eq 179
  tcp-map BGP-MD5
     tcp-options range 19 19 allow

  policy-map global_policy
   class BGP-MD5-CLASSMAP
    set connection advanced-options BGP-MD5
service-policy global_policy global
```

For more information, see http://www.cisco.com/warp/public/459/bgp-pix.html.

CHAPTER 4

Upgrading

- Prerequisites to Upgrading, page 4-1
- Upgrade Procedure, page 4-4
- Upgrade Examples, page 4-12

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 address*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.

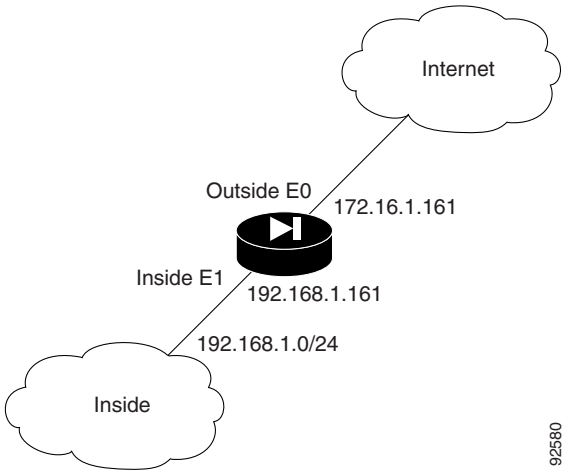
Basic Upgrade from PIX Version 6.3 to Security Appliance Version 7.0

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:513c9e26685650270411a7f884e68f7
: end

Migration1#
```

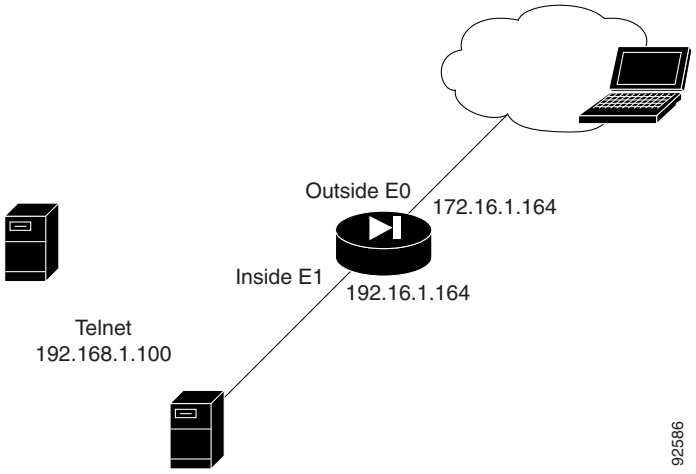
Upgrading to a VPN Client with Remote Access

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#
```

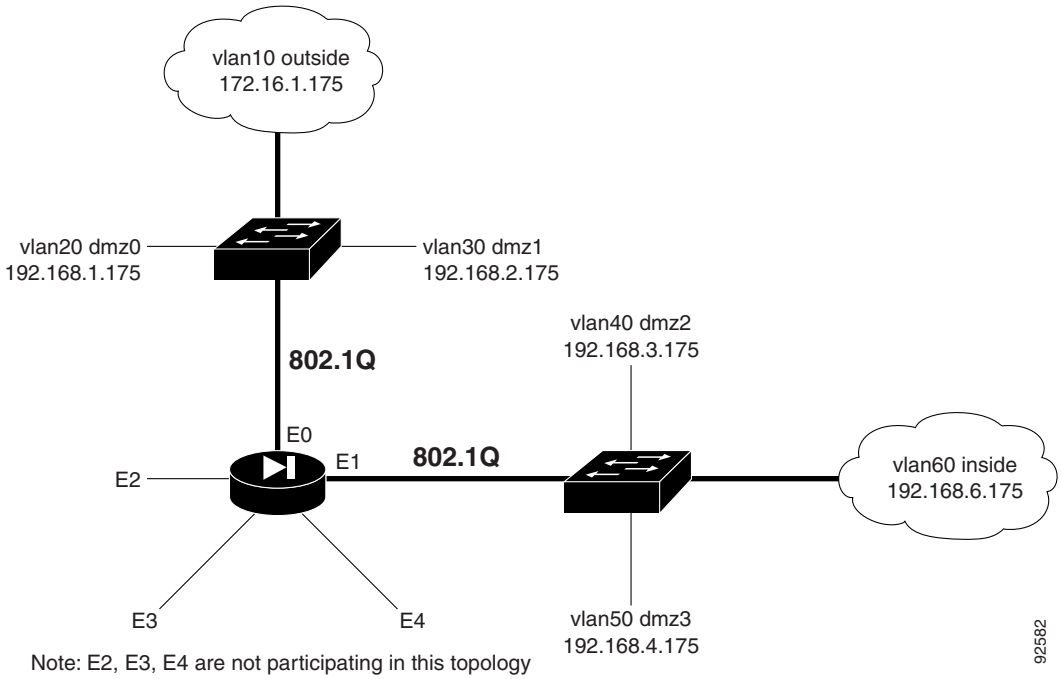
Upgrading to Security Appliance Version 7.0 Using VLAN

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



Note: E2, E3, E4 are not participating in this topology

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#
```

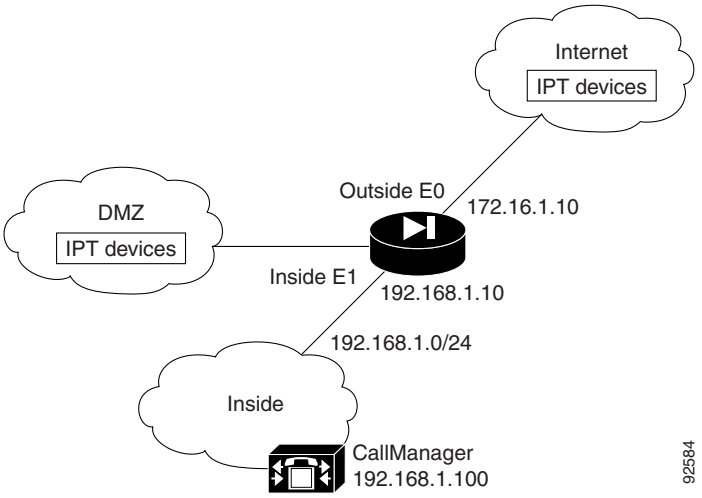
Upgrading to Security Appliance Version 7.0 with Voice Over IP

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#
```

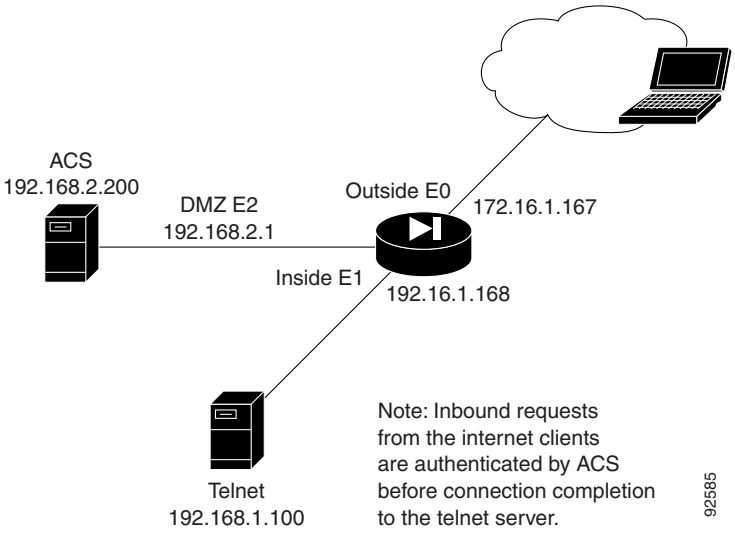
Upgrading to Security Appliance Version 7.0 with Authentication

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



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

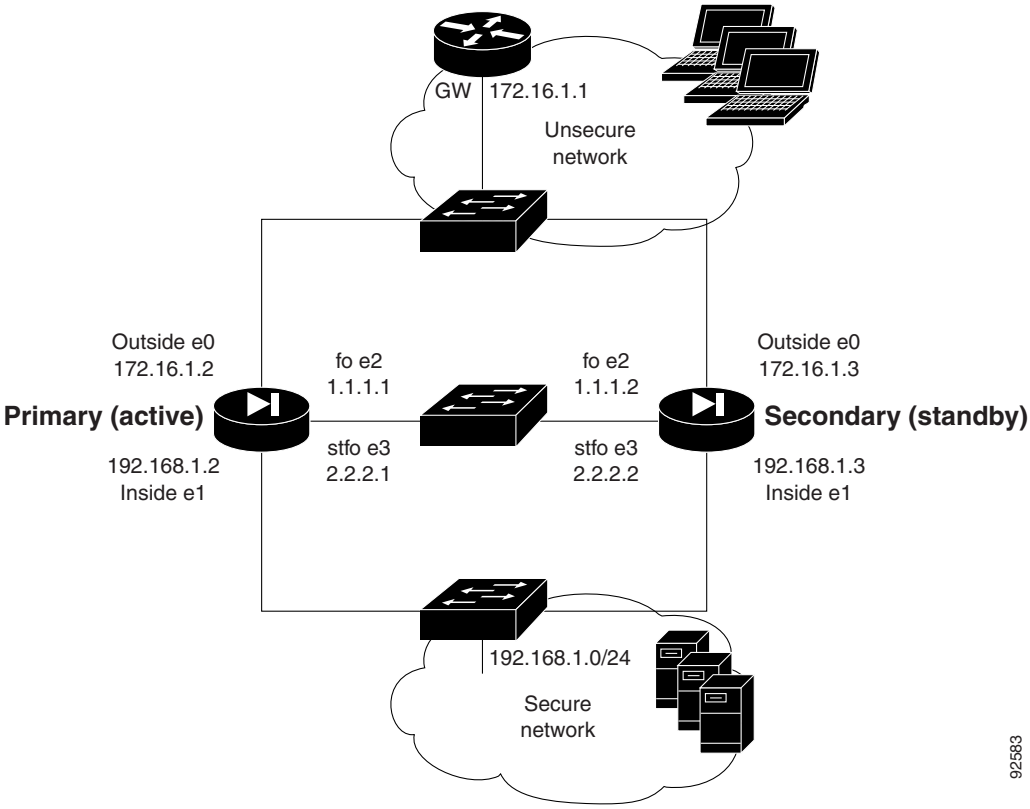
Assumptions

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.

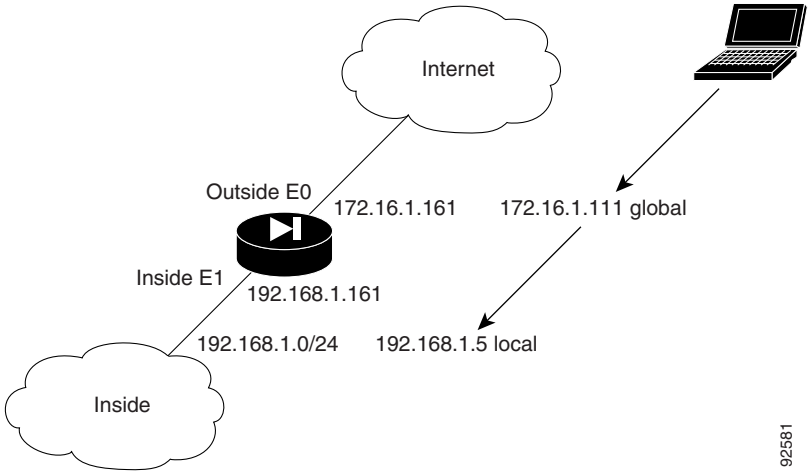
The configuration example in the "After Upgrade" section on page 4-92 displays missing conduit and outbound statements, which have been converted to access control lists.

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#
```

CHAPTER 5

Downgrade Procedure

You can downgrade from a PIX Security appliance Version 7.0 image to return to a PIX Version 6.3 image, using the **downgrade** command. This command changes the Flash layout to a format that the PIX images can understand.

This chapter includes the following topics:

- Guidelines for Downgrading, page 5-1
- Downgrade Procedure, page 5-1
- Downgrading Examples, page 5-3

Guidelines for Downgrading

- A PIX downgrade is not possible from the monitor prompt. The **downgrade** command must be used from a running PIX Security appliance Version 7.0 image to perform the downgrade.
- A PIX upgrade/downgrade can be done remotely only if there is no interruption to the process. A power failure during the process may result in a corrupt Flash that requires console access to recover. To prevent loss of data, it is recommended that all data be stored externally before starting the process.
- If the PIX had previously been upgraded from a PIX Version 6.3 version, the 4-tuple activation key is stored in Flash and does not need to be reentered. Even if the PIX Security appliance Version 7.0 code license had been subsequently updated using a 5-tuple activation key, the 4-tuple key is still saved.

  The **downgrade** command verifies and uses the 4-tuple key, if it exists. Otherwise, the activation key needs to be input in the CLI for the command to succeed.
- We recommend using the **show activation-key** command to display the current activation key.
- The **downgrade** command automatically reloads the PIX after it is complete.

Downgrade Procedure

To perform a downgrade to a PIX Version 6.3 image, use the **downgrade** command from a running PIX Security appliance Version 7.0 image as follows:

```
downgrade [/noconfirm] <image_url> [activation-key (flash|file|<4-part-actkey>)] [config
<start_config_url>]
```

Note The **downgrade** command is not available in user context mode.

where:

- <*image_url*>—A filename in Flash or a network URL (all network URL are supported by the **copy** command) that points to a PIX image. This must be an image that is before PIX Security appliance Version 7.0 release.
- <*start_config_url*>—Any URL which could be a network or local Flash that points to a start up configuration file to be used after the reboot. The configuration must be for the version of the image file used in the downgrade.
- *activation-key*—Specifies the activation key to be used on the downgraded image, using one of the following methods:
  - *flash*—Use the 4-tuple activation key that may have been used in the device. This is the default if the activation-key is not specified in the command line.
  - *file—A*llowed only on a PIX Version 6.3 image that was stored in Flash memory during the upgrade process. Such an image contains the activation key in the image itself and could be used after downgrade as well.
  - <*4-part-actkey*>—The activation key to be written to the image.

Note If the **activation-key** keyword is present, then you must enter one of the three options: *flash*, *file*, or <*4-part-actkey*>.

- */noconfirm*—The presence of this option suppresses the confirmation dialogue.

Note In most cases, you use the **downgrade** <*image_url*> command to downgrade, where <*image_url*> is the TFTP server location of the downgraded image. If the TFTP server is 192.168.1.20 and the filename in the TFTP root directory is pix633.bin, the command would look like the following:

downgrade tftp://192.168.1.20/pix633.bin

If the *activation-key* keyword is not specified in the command line and there is no default activation key for the image, the command will be rejected. If the activation key is found and could be used with the image, it will be stored in the image for use after the downgrade. If you are using an image file that was saved during the upgrade process (file image_old.bin), you could use the activation-key file option.

The data file containing cryptographic keys used before upgrading to PIX Security appliance Version 7.0 will be restored if the Flash has not been formatted or erased since the upgrade.

The *flash* option for the activation key is the last 4-tuple activation key used in the system. This key might have been overridden by a 5-tuple key, in which case, a warning with the list of features that might be potentially lost by going back to the 4-tuple key will be generated. If the system Flash has been reformatted or erased for some reason, the last 4-tuple key used will not be available and there will be no default key for the downgrade. The CLI notifies you to enter an activation key in the command line.

If the *config* keyword is not present, then the default is to use the downgrade.cfg file, if present. Otherwise, the PIX will boot without a configuration file.

If the downloaded image is not a PIX image or is lower than PIX Version 6.2, the command fails and an error message is generated.

If */noconfirm* is not present, the CLI prompts for confirmation and reboots the device after the downgrade operation is complete.

To downgrade using the CLI perform the following steps:

Step 1 Download the image from the network to RAM and check for validity. Proceed to Step 2 if the image passes.

Step 2 Get the activation key using the *flash*, *file*, or *<4-part-actkey>* method previously described.

Step 3 Verify the activation key if possible, and write it on the downloaded image.

Step 4 Obtain the startup configuration from the URL or downgrade.cfg file, if any exists.

Step 5 Read the data files from the downgrade.dat file (raw read, no format) and buffer it in RAM.

Step 6 Erase the entire Flash.

Step 7 Write the PIX image in RAM at the beginning of the Flash (sector 0).

Step 8 Write the startup configuration in RAM to the next sector(s) after the image (raw write).

Step 9 Write the data files in RAM to the next sector(s) (raw write).

Step 10 Reboot.

When the PIX image boots up, it checks for the PIX filesystem magic. As the magic is not present, the system rebuilds the filesystem by gleaning the data from Flash. It detects the image, startup configuration file, and data files by the presence of the respective magics. The appropriate filesystem header is created in Flash using the information discovered.

The startup configuration is specified in the CLI in case there is no downgrade.cfg file in the Flash and remote connectivity is desired after the reboot.

The design assumes that the downgrade procedure has been successful only if there are no interruptions to the process, such as no user or power interruptions, and the Flashfs filesystem in Flash is not corrupt. PDM and crash information are not copied over.

Downgrading Examples

This section includes the following configuration examples:

- Example of a Downgrade Procedure, page 5-4
- Example with a Zero Actkey, page 5-9
- Example with No Actkey in the Source Image, page 5-9
- Example to Abort the Downgrade at the Final Prompt, page 5-9
- Example Using an Invalid Actkey, page 5-9
- Example Without Specifying an Actkey and No 4-Tuple Actkey Stored in Flash, page 5-10
- Example Using a Security Appliance Version 7.0, page 5-10
- Example Using an Image with No Verified Actkey, page 5-10
- Example Using a Flash 4-Tuple Key without All the Features of the Current 5-Tuple Key, page 5-11
- Example Where the Entered Actkey Does Not Have the Features of the Current 5-Tuple Key, page 5-11

Example of a Downgrade Procedure

The following example is for a downgrade going from PIX Security appliance Version 7.0 to PIX Version 6.3(4). The PIX Version 6.3 image is coming from a TFTP server.

```
Conduit# downgrade tftp://192.168.1.100/pix634.bin
 This command will reformat the flash and automatically reboot the system.
 Do you wish to continue? [confirm]
 Buffering image

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

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

 Buffering startup config

 All items have been buffered successfully.
 If the flash reformat is interrupted or fails, data in flash will be lost
 and the system might drop to monitor mode.
 Do you wish to continue? [confirm]
 Acquiring exclusive access to flash
 Installing the correct file system for the image and saving the buffered data

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
 Flash downgrade succeeded


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.

Flash boot in 10 seconds.          9 seconds.         8 seconds.         7 seconds.
6 seconds.         5 seconds.         4 seconds.         3 seconds.         2 seconds.
1 seconds.

 Reading 1962496 bytes of image from flash.

############################################################################################
######################
64MB RAM
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
System Flash=E28F128J3 @ 0xfff00000
BIOS Flash=am29f400b @ 0xd8000
Crypto5823 (revision 0x1)

  ------------------------------------------------------------------------
                              ||        ||
                              ||        ||
                             ||||      ||||
                         ..:||||||:..:||||||:..
                        c i s c o S y s t e m s
                       Private Internet eXchange
  ------------------------------------------------------------------------
                       Cisco PIX Firewall

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

This PIX has an Unrestricted (UR) license.


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

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

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

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

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

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

                Restricted Rights Legend

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

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

.
Cryptochecksum(unchanged): 629e8fc8 b6e63516 1c253178 e5d91814
Type help or '?' for a list of available commands.
```

After performing the PIX Security appliance Version 7.0 downgrade, 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 version

 Cisco PIX Firewall Version 6.3(4)

 Compiled on Fri 02-Jul-04 00:07 by xxxxxx

 Conduit up 23 secs

 Hardware:   PIX-515E, 64 MB RAM, CPU Pentium II 433 MHz
 Flash E28F128J3 @ 0x300, 16MB
 BIOS Flash AM29F400B @ 0xfffd8000, 32KB

 Encryption hardware device : VAC+ (Crypto5823 revision 0x1)
 0: ethernet0: address is 0011.937e.064f, irq 10
 1: ethernet1: address is 0011.937e.0650, irq 11
 2: ethernet2: address is 000d.88ee.dfa0, irq 11
 3: ethernet3: address is 000d.88ee.dfa1, irq 10
 4: ethernet4: address is 000d.88ee.dfa2, irq 9
 5: ethernet5: address is 000d.88ee.dfa3, irq 5
 Licensed Features:
 Failover:                 Enabled
 VPN-DES:                  Enabled
 VPN-3DES-AES:             Enabled
```

```
Maximum Physical Interfaces: 6
Maximum Interfaces:          10
Cut-through Proxy:           Enabled
Guards:                      Enabled
URL-filtering:               Enabled
Inside Hosts:                Unlimited
Throughput:                  Unlimited
IKE peers:                   Unlimited

This PIX has an Unrestricted (UR) license.

Serial Number: 808300261 (0x302daee5)
Running Activation Key: 0x8a9a2457 0xd91de491 0x48534d65 0xa648750a
Configuration has not been modified since last system restart.
```

Enter the **show run** command to display output from your PIX Version 6.3 configuration. Output from the PIX Version 6.3 configuration follows:

```
Conduit# 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

Conduit#
```

Example with a Zero Actkey

Enter a zero actkey:

```
PIX# downgrade tftp://17.13.2.25//tftpboot/mananthr/pix704.bin.6.3.3 activation-key 0 0 0
0
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm] [Press Enter to confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
Error: activation key entered is invalid.
```

Example with No Actkey in the Source Image

Enter the file option when there is no actkey in the source image, which happens if the source is in TFTP server:

```
PIX# downgrade tftp://17.13.2.25//tftpboot/mananthr/pix704.bin.6.3.3 activation-key file
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
Activation key does not exist in the source image.
Please use the activation-key option to specify an activation key.
```

Example to Abort the Downgrade at the Final Prompt

Abort the downgrade at the final prompt:

```
PIX# downgrade tftp://17.13.2.25//tftpboot/mananthr/pix704.bin.6.3.3
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm] [Press Enter to confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!

Buffering startup config

All items have been buffered successfully.
If the flash reformat is interrupted or fails, data in flash will be lost
and the system might drop to monitor mode.
Do you wish to continue? [confirm] ===<typed n here>
Downgrade process terminated.
```

Example Using an Invalid Actkey

Enter an invalid actkey for the platform:

```
PIX# downgrade tftp://17.13.2.25//tftpboot/mananthr/pix704.bin.6.3.3 activation-key
0xaaf93e75 0xc1d21188 c2e18f2 0x162a8a80
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm] [Press Enter to confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
Warning: activation key entered is invalid
Do you wish to continue? [confirm]
Downgrade process terminated.
```

Example Without Specifying an Actkey and No 4-Tuple Actkey Stored in Flash

Downgrade without specifying an actkey in the command line when there is no 4-tuple actkey stored in Flash:

```
PIX# downgrade tftp://17.13.2.25//tftpboot/mananthr/pix704.bin.6.3.3
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm] [Press Enter to confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
Warning: 4 tuple activation key in flash is invalid.
Do you wish to continue? [confirm]
Downgrade process terminated.
Please enter an activation-key in the command line.
```

Example Using a Security Appliance Version 7.0

Use a PIX Security appliance Version 7.0 image with the downgrade:

```
PIX# downgrade tftp://17.13.2.25//scratch/views/test/target/f1/pix704.bin
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm] [Press Enter to confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Error: Need to use an image with version less than 7-0-0-0.
```

Example Using an Image with No Verified Actkey

Use an image for which we do not verify actkey:

```
PIX# downgrade tftp://17.13.2.25//tftpboot/mananthr/pix704.bin.4.4.1-rel
This command will reformat the flash and automatically reboot the system.
```

```
Do you wish to continue? [confirm] [Press Enter to confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image checksum has not been verified
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Warning: Activation key not verified.
Key 32c261f3 633fe24 c94ef2ea e299a3f might be incompatible with the image version
4-4-1-0.
Do you wish to continue? [confirm]
Downgrade process terminated.
Please enter an activation-key in the command line.
```

Example Using a Flash 4-Tuple Key without All the Features of the Current 5-Tuple Key

The Flash 4-tuple key does not have all features of the current 5-tuple key:

```
PIX# downgrade tftp://17.13.2.25//tftpboot/markananthr/pix704.bin.6.3.3
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm] [Press Enter to confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
The following features available in current activation key in flash
are NOT available in 4 tuple activation key in flash:
   VPN-3DES-AES
   GTP/GPRS
   5 Security Contexts
Failover is different:
   current activation key in flash: UR(estricted)
   4 tuple activation key in flash: R(estricted)
Some features might not work in the downgraded image if this key is used.
Do you wish to continue? [confirm]
Downgrade process terminated.
Please enter an activation-key in the command line.
```

Example Where the Entered Actkey Does Not Have the Features of the Current 5-Tuple Key

The entered actkey does not have all features of the current 5-tuple key:

```
PIX# downgrade tftp://17.13.2.25//tftpboot/mananthr/pix704.bin.6.3.3 activation-key
0x32c261f3 0x062afe24 0xc94ef2ea 0x0e299a3f
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm] [Press Enter to confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
The following features available in current activation key in flash
are NOT available in activation key entered:
   VPN-3DES-AES
```

```
   GTP/GPRS
   5 Security Contexts
Failover is different:
   current activation key in flash: UR(estricted)
   activation key entered: R(estricted)
Some features might not work in the downgraded image if this key is used.
Do you wish to continue? [confirm]
Downgrade process terminated.
Please enter an activation-key in the command line.
```

CHAPTER 6

Syslog Message Changes and Deletions

This chapter includes the following topics:

- Changed Syslog Messages, page 6-1
- Deleted Syslog Messages, page 6-2

See the security appliance *Cisco Security Appliance System Log Messages* for more information.

Changed Syslog Messages

- **112001**

  Old Syslog Message: %PIX-2-112001: (string:dec) PIX Clear complete

  New Syslog Message: %PIX-2-112001: Clear finished

  Change Reason: The filename and line number (string:dec) are undesirable in a syslog message. The PIX keyword is removed to make the syslog platform independent.

- **199002**

  Old Syslog Message: %PIX-6-199002: PIX startup completed. Beginning operation

  New Syslog Message: %PIX-6-199002: Startup completed. Beginning operation

  Change Reason: The PIX keyword is removed from the body of the syslog message to make the syslog platform independent.

- **199005**

  Old Syslog Message: %PIX-6-199005: PIX Startup begin

  New Syslog Message: %PIX-6-199005: Startup begin

  Change Reason: The PIX keyword is removed from the body of the syslog message to make the syslog platform independent.

- **201002**

  Old Syslog Message: %PIX-3-201002: Too many connections on {static|xlate} global_address! econns nconns

  New Syslog Message: %PIX-3-201002: Too many tcp connections on {static|xlate} global_address! econns nconns

  Change Reason: This syslog is only applicable to TCP connection, hence the change.

- **208005**

Old Syslog Message: %PIX-3-208005: (function:line_num) pix clear *command* return code

New Syslog Message: %PIX-3-208005: Clear *command* return

Change Reason: The filename and line number are undesirable in a syslog message. The PIX keyword is removed to make the syslog platform independent.

- **308001**

  Old Syslog Message: %PIX-6-308001: PIX console enable password incorrect for *number* tries (from IP_address)

  New Syslog Message: %PIX-6-308001: Console enable password incorrect for *number* tries (from_*IP address*)

  Change Reason: The PIX keyword is removed from the body of the syslog message to make the syslog platform independent.

- **315004**

  Old Syslog Message: %PIX-3-315004: Fail to establish SSH session because PIX RSA host key retrieval failed

  New Syslog Message: %PIX-3-315004: Fail to establish SSH session because RSA host key retrieval failed.

  Change Reason: The PIX keyword is removed from the body of the syslog message to make the syslog platform independent.

- **606001**

  Old Syslog Message: %PIX-6-606001: PDM session number number from IP_address started

  New Syslog Message: %PIX-6-606001: ASDM session number number from IP_address started

  Change Reason: The PDM keyword is changed to ASDM to update the syslog platform for ASDM.

- **606002**

  Old Syslog Message: %PIX-6-606002: PDM session number number from IP_address ended

  New Syslog Message: %PIX-6-606002: ASDM session number number from IP_address ended

  Change Reason: The PDM keyword is changed to ASDM to update the syslog platform for ASDM.

- **611314**

  Old Syslog Message: %PIX-6-611314: VPNClient: Load Balancing Cluster with Virtual IP: IP_address has redirected the PIX to server IP_address

  New Syslog Message: %PIX-6-611314: VPNClient: Load Balancing Cluster with Virtual IP:%I has redirected firewall to server

  Change Reason: The PIX keyword is removed to make the syslog platform independent.

Deleted Syslog Messages

- **103002**

  Old Syslog Message: %PIX-1-103002: (Primary) Other firewall network interface interface_number OK

  Deletion Reason: This syslog was not produced by PIX Version 6.3, nor will it be produced by PIX Security appliance Version 7.0.

- **105031**

Old Syslog Message: %PIX-1-105031: Failover LAN interface is up

Deletion Reason: Replaced by 105042.

- **105032**

  Old Syslog Message: %PIX-1-105032: LAN Failover interface is down

  Deletion Reason: Replaced by 105043.

- **105034**

  Old Syslog Message: %PIX-1-105032: LAN Failover interface is down

  Deletion Reason: Obsolete due to different implementation.

- **105035**

  Old Syslog Message: %PIX-1-105035: Receive a LAN failover interface down msg from peer.

  Deletion Reason: Obsolete due to different implementation.

- **105036**

  Old Syslog Message: %PIX-1-105036: PIX dropped a LAN Failover command message.

  Deletion Reason: Obsolete due to different implementation.

- **105037**

  Old Syslog Message: %PIX-1-105037: The primary and standby units are switching back and forth as the active unit.

  Deletion Reason: Obsolete due to different implementation.

- **109013**

  Old Syslog Message: %PIX-3-109013: User must authenticate before using this service

  Deletion Reason: This syslog not produced by PIX Version 6.3, nor will it be produced by PIX Security appliance Version 7.0.

- **109021**

  Old Syslog Message: %PIX-7-109021: Uauth null proxy error

  Deletion Reason: No longer relevant in this release.

- **111006**

  Old Syslog Message: %PIX-6-309002: Permitted manager connection from IP_address.

  Deletion Reason: Replaced by 605005 as per ICSA requirement.

- **210003**

  Old Syslog Message: %PIX-2-201003: Embryonic limit exceeded nconns/elimit for outside_address/outside_port (global_address) inside_address/inside_port on interface interface_name

  Deletion Reason: Obsolete due to different implementation.

- **210010**

  Old Syslog Message: %PIX-3-210010: LU make UDP connection for outside_address:outside_port inside_address:inside_port failed

  Deletion Reason: Obsolete due to different implementation.

- **210020**

  Old Syslog Message: %PIX-3-210020: LU PAT port port reserve failed

Deletion Reason: Obsolete due to different implementation.

- **210021**

  Old Syslog Message: %PIX-3-210021: LU create static xlate global_address ifc interface_name failed

  Deletion Reason: Obsolete due to different implementation.

- **211003**

  Old Syslog Message: %PIX-3-211003: CPU utilization for number seconds = percent

  Deletion Reason: This is an error condition in the code; it is no longer relevant.

- **215001**

  Old Syslog Message: %PIX-2-215001:Bad route_compress() call, sdb= number

  Deletion Reason: The syslog number has changed to 216001.

- **302302**

  Old Syslog Message: %PIX-3-302302: ACL = deny; no sa created

  Deletion Reason: The code containing this syslog changed dramatically; it is no longer relevant.

- **309002**

  Old Syslog Message: %PIX-6-309002: Permitted manager connection from IP_address

  Deletion Reason: This is for PIX Firewall Management, which is no longer supported.

- **316001**

  Old Syslog Message: %PIX-2-316001: Denied new tunnel to *IP_address*. VPN peer limit (platform_vpn_peer_limit) exceeded

  Deletion Reason: This is not applicable in the current release, as SOHO devices are not supported by this release.

- **320001**

  Old Syslog Message: %PIX-3-320001: The subject name of the peer certificate is not allowed for connection

  Deletion Reason: This has been replaced by more granular syslogs (from 713001 to 713224).

- **402101**

  Old Syslog Message: %PIX-4-402101: decaps: rec'd IPSEC packet has invalid spi for destaddr=dest_address, prot=protocol, spi=number

  Deletion Reason: The code containing this syslog changed dramatically; it is no longer relevant.

- **402102**

  Old Syslog Message: %PIX-4-402102: decapsulate: packet missing {AH|ESP}, destadr=dest_address, actual prot=protocol

  Deletion Reason: The code containing this syslog changed dramatically; it is no longer relevant.

- **402103**

  Old Syslog Message: %PIX-4-402103: identity doesn't match negotiated identity (ip) dest_address= dest_address, src_addr= source_address, prot= protocol, (ident) local=inside_address, remote=remote_address, local_proxy=IP_address/IP_address/port/port, remote_proxy=IP_address/IP_address/port/port

  Deletion Reason: The code containing this syslog changed dramatically; it is no longer relevant.

- **403500**

  Old Syslog Message: %PIX-6-403500: PPPoE - Service name 'any' not received in PADO. Intf:interface_name AC:ac_name

  Deletion Reason: PPPoE is not supported in the current release, customer would not see this syslog.

- **403501**

  Old Syslog Message: %PIX-3-403501: PPPoE - Bad host-unique in PADO - packet dropped Intf:interface_name AC:ac_name

  Deletion Reason: PPPoE is not supported in the current release, hence customers would not see this syslog.

- **403502**

  Old Syslog Message: %PIX-3-403502: PPPoE - Bad host-unique in PADS - dropping packet. Intf:interface_name AC:ac_name

  Deletion Reason: PPPoE is not supported in the current release, hence customers would not see this syslog.

- **404101**

  Old Syslog Message: %PIX-4-404101: ISAKMP: Failed to allocate address for client from pool string

  Deletion Reason: This has been replaced by 713132.

- **407001**

  Old Syslog Message: %PIX-4-407001: Deny traffic for local-host interface_name:inside_address, license limit of number exceeded

  Deletion Reason: This is not applicable in the current release.

- **501101**

  Old Syslog Message: %PIX-5-501101: User transitioning priv level

  Deletion Reason: The code containing this syslog changed dramatically; it is no longer relevant.

- **602102**

  Old Syslog Message: %PIX-6-602102: Adjusting IPSec tunnel mtu...

  Deletion Reason: The code containing this syslog changed dramatically; it is no longer relevant.

- **602201**

  Old Syslog Message: %PIX-6-602201: ISAKMP Phase 1 SA created (local <ip>/<port> (initiator|responder), remote <ip>/<port>, authentication=<auth_type>, encryption=<encr_alg>, hash=<hash_alg>, group=<DH_grp>, lifetime=<seconds>) Change Reason: Replaced by more granular syslog, look at 713xxx

  Deletion Reason: This has been replaced by more granular syslogs (from 713001 to 713224).

- **602203**

  Old Syslog Message: PIX-6-602203: ISAKMP session disconnected (local <ip> (initiator|responder), remote <ip>)

  Deletion Reason: This has been replaced by more granular syslogs (from 713001 to 713224).

- **602301**

  Old Syslog Message: %PIX-6-602301: sa created...

  Deletion Reason: This has been replaced by syslogs 713119 and 713120.

- **602302**

  Old Syslog Message: %PIX-6-602302: deleting sa

  Deletion Reason: This has been being replaced by 713113, 713169, 713170, 713194, 715009, 715052, 715067 and 715068.

- **603108**

  Old Syslog Message: %PIX-6-603108: Built PPTP Tunnel at interface_name, tunnel-id = number, remote-peer = IP_address, virtual-interface = number, client-dynamic-ip = IP_address, username = user, MPPE-key-strength = number

  Deletion Reason: PPPoE is not supported in the current release, hence customers would not see this syslog.

- **702201**

  Old Syslog Message: %PIX-7-702201: ISAKMP Phase 1 delete received (local <ip> (initiator|responder), remote <ip>)

  Deletion Reason: This has been replaced by more granular syslogs (from 713001 to 713224).

- **702202**

  Old Syslog Message: %PIX-7-702202: ISAKMP Phase 1 delete sent (local <ip> (initiator|responder), remote <ip>)

  Deletion Reason: This has been replaced by more granular syslogs (from 713001 to 713224).

- **702203**

  Old Syslog Message: %PIX-7-702203: ISAKMP DPD timed out (local <ip> (initiator|responder), remote <ip>)

  Deletion Reason: This has been replaced by more granular syslogs (from 713001 to 713224).

- **702204**

  Old Syslog Message: %PIX-7-702204: ISAKMP Phase 1 retransmission (local <ip> (initiator|responder), remote <ip>)

  Deletion Reason: This has been replaced by more granular syslogs (from 713001 to 713224).

- **702205**

  Old Syslog Message: %PIX-7-702205: ISAKMP Phase 2 retransmission (local <ip> (initiator|responder), remote <ip>)

  Deletion Reason: This has been replaced by more granular syslogs (from 713001 to 713224).

- **702206**

  Old Syslog Message: %PIX-7-702206: ISAKMP malformed payload received (local <ip> (initiator|responder), remote <ip>)

  Deletion Reason: This has been replaced by more granular syslogs (from 713001 to 713224).

- **702207**

  Old Syslog Message: %PIX-7-702207: ISAKMP duplicate packet detected (local <ip> (initiator|responder), remote <ip>)

  Deletion Reason: This has been replaced by more granular syslogs (from 713001 to 713224).

- **702208**

  Old Syslog Message: %PIX-7-702208: ISAKMP Phase 1 exchange started (local <ip> (initiator|responder), remote <ip>)

  Deletion Reason: This has been replaced by more granular syslogs (from 713001 to 713224).

- **702209**

  Old Syslog Message: %PIX-7-702209: ISAKMP Phase 2 exchange started (local <ip> (initiator|responder), remote <ip>)

  Deletion Reason: This has been replaced by more granular syslogs (from 713001 to 713224).

- **702210**

  Old Syslog Message: %PIX-7-702210: ISAKMP Phase 1 exchange completed(local <ip> (initiator|responder), remote <ip>)

  Deletion Reason: This has been replaced by more granular syslogs (from 713001 to 713224).

- **702211**

  Old Syslog Message: %PIX-7-702211: ISAKMP Phase 2 exchange completed(local <ip> (initiator|responder), remote <ip>)

  Deletion Reason: This has been replaced by more granular syslogs (from 713001 to 713224).

- **702212**

  Old Syslog Message: %PIX-7-702212: ISAKMP Phase 1 initiating rekey (local <ip> (initiator|responder), remote <ip>)

  Deletion Reason: This has been replaced by more granular syslogs (from 713001 to 713224).

- **702301**

  Old Syslog Message: %PIX-7-702301: lifetime expiring...

  Deletion Reason: Security associations do not expire in PIX Security appliance Version 7.0; this syslog is no longer relevant.

- **702302**

  Old Syslog Message: %PIX-3-702302: replay rollover detected...

  Deletion Reason: The code containing this syslog changed dramatically; it is no longer relevant.

- **702303**

  Old Syslog Message: %PIX-7-702303: sa_request...

  Deletion Reason: This syslog has been replaced by 713041, 713042, 713043 and 713176.

- **709002**

  Old Syslog Message: %PIX-7-709002: FO unreplicable: cmd=command

  Deletion Reason: This syslog was intended to catch programming errors and is no longer needed because of code changes.