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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- **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

- **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.