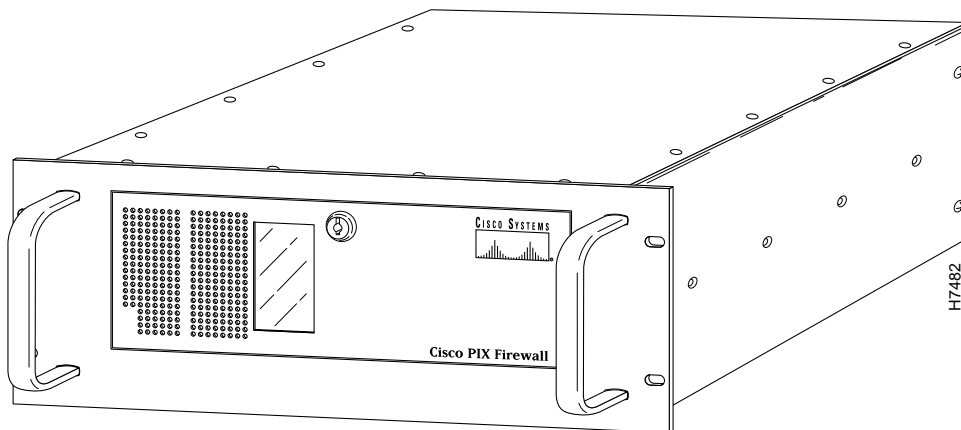# Introduction

Cisco Systems' PIX Firewall provides firewall and network translation services.

Figure 1-1 shows the Cisco PIX Firewall front view.

Figure 1-1   PIX Firewall Front View

PIX (Private Internet Exchange) Firewall provides full firewall protection that completely conceals the architecture of an internal network from the outside world. PIX Firewall allows secure access to the Internet from within existing private networks and the ability to expand and reconfigure TCP/IP networks without being concerned about a shortage of IP addresses. With PIX Firewall, users can take advantage of larger address classes than they may have been assigned by the Internet's Network Information Center (NIC). PIX Firewall provides this access through its Network Address Translation (NAT) facility as described by RFC 1631.

PIX Firewall Adaptive Security

The Adaptive Security (AS) feature applies to the dynamic translation slots and can be applied to static translation slots via the **static** command. The Adaptive Security algorithm is a very stateful approach to security. Every inbound packet is checked exhaustively against the Adaptive Security algorithm and against connection state information in memory. This stateful approach to security is regarded in the industry as being far more secure than a stateless packet screening approach.

Adaptive Security follows these rules:

- Allow any TCP connections that originate from the inside network.

- Ensure that if an FTP data connection is initiated to a translation slot, there is already an FTP control connection between that translation slot and the remote host. If not, drop and log the attempt to initiate an FTP data connection.

- Drop and log attempts to initiate TCP connections to a translation slot from the outside.

- Drop and log source routed IP packets sent to any translation slot on the PIX Firewall.

- Allow ICMP of types 0, 3, 4, 8, 11, 12, 17 and 18. By implication, deny ICMP redirects (type 5).

- Silently drop ping requests to dynamic translation slots.

- Answer (by the PIX Firewall) ping requests directed to static translation slots.

You can protect static translation slots with Adaptive Security, and you can have exceptions (called conduits) to the previously described rules, which you create with the **conduit** command. Multiple exceptions may be applied to a single static translation slot (via multiple **conduit** commands). This lets you permit access from an arbitrary machine, network, or any host on the Internet to the inside host defined by the static translation slot. PIX Firewall handles UDP data transfers in a manner similar to TCP. Special handling allows DNS service, archie, and RealAudio to work securely. PIX Firewall creates UDP connection state information when a UDP packet is sent from the inside network. Response packets resulting from this traffic are accepted if they match the connection state information. The connection state information is deleted after a short period of inactivity.

PIX Firewall Features

With the firewall feature, you can eliminate the overhead and risks associated with UNIX-based firewall systems and have complete accounting and logging of all transactions, including attempted break-ins. Both NCSA and SRI certify that the PIX Firewall secures your network from outside intrusion.

PIX Firewall has the following features:

- Firewall capability that keeps intruders out of your internal network while permitting regulated conduit access through the firewall for services such as electronic mail, Telnet, FTP, SNMP, and HTTP (World Wide Web) use.

- Network translation services that let a site share one or more NIC-registered IP addresses among many users.

- An Identity feature that lets NIC-registered IP addresses pass through the firewall without address translation, while still retaining Adaptive Security.

- The PIX Firewall offers performance dramatically better than competing firewalls. It gains speed through a patent pending process called Cut-Through proxies, which is the fastest way for a firewall to authenticate a user. Unlike a proxy server that must analyze every packet at layer seven of the OSI model, a time- and processing-intensive function, the PIX Firewall first queries a TACACS+ or RADIUS server for authentication. Once approved, the PIX Firewall then establishes a data flow and all traffic thereafter flows directly and quickly between the two parties. This Cut-Through capability allows the PIX Firewall to perform dramatically faster than proxy-based servers while maintaining session state.

- An IOS-like command set for simplified configuration and administration.

- Support for SNMP MIB-II gets and traps.

- Simplified configuration and system management with an HTML interface.

- Support for Telnet, FTP, and HTTP access using RADIUS (Remote Authentication Dial-In User Service) and TACACS+ security systems. PIX Firewall authenticates users in conjunction with the security systems that Cisco routers support. The security clients run on Cisco routers and send authentication requests to a central security server, which contains all user authentication and network service access information.

- For domestic sites, the Private Link encryption option that permits up to 64 PIX Firewall units to interact together across a WAN with completely secure data transfer. From the internal networks, the other networks connected through Private Link appear as one contiguous network. Private Link supports IETF IPSEC AH/ESP with DES.

- Failover capability that permits a secondary PIX Firewall unit to take over firewall communications if the primary unit fails.

- Support for 10BaseT and 100BaseTX networking.

- Support for Token-Ring network cards that can be operated singly so that Ethernet networking transforms into Token-Ring or in pairs for a standard Token-Ring network.

Note You can view information on the PIX Firewall and additional documentation over the World Wide Web at this URL: `http://www.cisco.com/pix`

Understanding PIX Firewall

The PIX Firewall contains two Ethernet interfaces, one for the inside, secure network and the other for the outside, unprotected network. Both the inside and outside Ethernet interfaces can listen to RIP routing updates, and the inside interface can broadcast a RIP default route.

When packets arrive at the inside Ethernet, the PIX Firewall checks to see if previous packets have come from the inside host. If not, the PIX Firewall creates a dynamic translation slot in its state table. The dynamic translation slot includes the inside IP address and the new globally unique IP address, which is drawn from the virtual network of up to 64K host addresses. PIX Firewall then changes the IP address, the checksums, and other aspects of the packet so they agree, and forwards the packet to the outside Ethernet interface on its way to the Internet.

When a packet arrives at the outside interface, it must first pass the PIX Firewall Adaptive Security criteria. If the packet passes the security tests, PIX Firewall removes the destination IP address, and the internal IP address is inserted in its place. The packet is forwarded to the inside interface.

Dynamic translation slots are useful for desktop machines that do not need constant addresses on the Internet. Inside network hosts with IP addresses not registered with the NIC (Network Information Center) can directly access the Internet with standard TCP/IP software on the desktop. No special client software is needed.

Another class of address translation on the PIX Firewall is static translation. Static translation effectively moves an internal unregistered host into the virtual network in the PIX Firewall. This is useful for internal machines that need to be addressed from the outside Internet gateways; for example, an SMTP server.

For more information on firewalls refer to *Firewalls and Internet Security* by William Cheswick and Steven Bellows, 1994, Addison-Wesley, ISBN 0-201-63357-4.

Access Modes

New to the version 3 release, the PIX Firewall command interpreter provides a new command set based on IOS technologies. This command set provides three administrator access modes:

- Unprivileged mode displays the ">" prompt and lets you view current running settings.

- Privileged mode displays the "#" prompt and lets you change current settings and write to flash memory. Any unprivileged command also works in privileged mode.

- Configuration mode displays the "(config)#" prompt and lets you change system configurations. Only configuration mode commands work in this mode.

By default, the console is in unprivileged mode. You can access privileged mode by entering the **enable** command. PIX Firewall then prompts you for a password. Enter the default password **cisco**. When you are done configuring PIX Firewall, change the password with the **enable password** command. Exit privileged mode by entering the **disable** command.

You can access configuration mode by entering the **config** command. You can then write your settings to flash memory, diskette, or to your console computer. Exit configuration mode by entering the **^z** command.

PIX Firewall Equipment

The PIX Firewall shipping carton contains the following:

- Rack-mountable PIX Firewall unit

- Keys for the front panel lock

- Power cord

- DB-9 to DB-25 null modem serial cable

- DB-25 gender adapter

- PIX Firewall system diskette

- This guide

- *Regulatory Compliance and Safety Information for the Cisco PIX Firewall*

- *Cisco PIX Firewall Release Notes*

- Cisco Connection Documentation CD

Before Installing PIX Firewall

Note   Read the *Regulatory Compliance and Safety Information for the Cisco PIX Firewall* before installing. Studying the safety material in this guide and the brief section that follows can help keep you safe and focused as you continue preparing your PIX Firewall for service.

Follow these guidelines to ensure general safety:

- Keep the chassis area clear and dust-free during and after installation.

- Put the removed chassis cover in a safe place.

- Keep tools away from walk areas where you and others could fall over them.

- Do not wear loose clothing that could get caught in the chassis. Fasten your tie or scarf and roll up your sleeves.

- Wear safety glasses if you are working under any conditions that might be hazardous to your eyes.

- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.

Warning Ultimate disposal of this product should be handled according to all national laws and regulations. Refer to the *Regulatory Compliance and Safety Information for the Cisco PIX Firewall* for more information.

Warning Do not work on the system or connect or disconnect cables during periods of lightning activity. Refer to the *Regulatory Compliance and Safety Information for the Cisco PIX Firewall* for more information.

Warning This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors). Refer to the *Regulatory Compliance and Safety Information for the Cisco PIX Firewall* for more information.

Warning The device is designed to work with TN power systems. Refer to the *Regulatory Compliance and Safety Information for the Cisco PIX Firewall* for more information.

Warning The ports labeled "Ethernet," "10BaseT," "Token Ring," "Console," and "AUX" are safety extra-low voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits. Because the BRI circuits are treated like telephone-network voltage, avoid connecting the SELV circuit to the telephone network voltage (TNV) circuits.

Warning Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or can weld the metal object to the terminals. Refer to the *Regulatory Compliance and Safety Information for the Cisco PIX Firewall* for more information.

Warning Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord. Refer to the *Regulatory Compliance and Safety Information for the Cisco PIX Firewall* for more information.

Warning Do not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is off and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected. Refer to the *Regulatory Compliance and Safety Information for the Cisco PIX Firewall* for more information.

Warning This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use. Refer to the *Regulatory Compliance and Safety Information for the Cisco PIX Firewall* for more information.

Warning Read the installation instructions before you connect the system to its power source. Refer to the *Regulatory Compliance and Safety Information for the Cisco PIX Firewall* for more information.

Command Changes In this Release

New commands have been added for the following features:

- Access modes — to mimic the IOS command set, access modes now group commands by security level. Unprivileged mode is the default, the **enable** command starts privileged mode, and **config term** starts configuration mode. Use **^z** to exit configuration and privileged mode, and **disable** to return to unprivileged mode. The command prompt changes for each mode.

- User authorization — users can now log into the protected network using security authentication systems supported by Cisco routers such as RADIUS and TACACS. The **auth**, **auth-user,** and **auth-server** commands enable authentication, define who can use it, and from which servers grant access. The **show auth**, **show auth-user**, and **show auth-server** verify status and let you monitor system access.

- Administration command syntax — the new **show** commands give you improved system monitoring capability in all areas of PIX Firewall access and use. Preface a command with **show** to list its status. In addition, if provided, preface the command with **no** to disable the action, or **clear** to erase information. You can list command information with the expanded help facility by entering a question mark after a command, such as **show ?**, **no ?**, or **clear ?** to list which commands accept each preface. The "Command Reference" section at the end of this guide lists each prefacing command individually for further information.

- Global lists — you can now have up to 16,384 separate groups of IP addresses available for outbound connections. The new **outbound** command replaces the V2 **access_list** command and the **global** command has changed to accomodate the address grouping feature.

- Address translation — the new **nat** commands let you restrict access to network IP addresses.

- HTTP configuration — you can now configure and monitor PIX Firewall status from your network browser. The **http** command, analogous to the **telnet** command, lets you define who has access to this configuration capability. The **who** command now displays both HTTP and Telnet access and the **show http** command lets you monitor progress. The **no http** and **clear http** commands let you disable access.

- SNMP access — you can use SNMP to monitor PIX Firewall events, such as SYSLOG messages. The **snmp-server** command lets you specify which servers have access to these events and **show snmp-server** lets you monitor access status.

- Failover connection (optional) — in the event of system failure, a second PIX Firewall can keep the protected network online. The **failover** and the **show failover** commands let you enable or disable this feature and monitor its status.

- Private Link — new features extend encryption with up to 7 keys that you can change on timed intervals. The **linkpath** command replaces the V2 **route link** command, **lnko** and **lnkopath** provide backward compatibility to V2 systems, and **age** specifies the duration a key is valid.

Command Changes Summary

Table 1-1 compares version 2 and version 3 commands.

Table 1-1   Command Changes Between PIX Firewall Versions 2 and 3

V2 Command	V3 Command	V2 Command	V3 Command
access_list	outbound	mem	show memory, show blocks, show xlate
apply	apply	passwd	passwd
arp	arp	reboot	reload
clear_config	write erase and reboot	restore	config memory and config floppy
conduit	conduit	rip	rip
exit	^z	route	route
global	global	route link	linkpath
help	help	save	write
ifconfig	ip address and interface ethernet	show	show
ifshow	show config	static	static
ifstat	show interface	tcpstat	show tcp
kill	kill	telnet	telnet
link	link	timeout	timeout
link_stat	show link	trace	--
list_rip	show rip	version	show version
loghost	syslog	who	who or show who
		xlate	show xlate

New Command Summary

Table 1-2 lists commands that are new to this release.

Table 1-2   New Commands for This Release

V3 Command	Description
age	Specify duration that a Private Link encryption key is active
auth	Enable user authentication
auth-user	Specify which users can login with authentication
auth-server	Specify which servers authenticate users
clear *cmd*	Clear or disable command functionality
configure	Enter configuration mode or download RAM from flash memory or floppy
disable	Exit privileged mode
enable	Start privileged mode
failover	Enable failover access

V3 Command	Description
hostname	Specify host name for PIX Firewall command prompt
http	Specify which users can use HTTP configuration
interface	Identify network interface type and speed
ip address	Indicate network interface IP address and subnet mask
linkpath	Identify Private Link remote system IP address and its network mask
lnko, lnkopath	Maintain compatibility with V2 PIX Firewall Private Link systems
nat	Restrict IP addresses from network access
no *cmd*	Disable command functionality
outbound	Define access lists for outbound connections
ping	Determine if IP address is available to PIX Firewall
show *cmd*	Provide status or additional information about command functionality
show blocks	View system buffer utilization
show hw	View hardware idenfication information
show memory	View memory utilization
show processes	View process status
show rif	View Token-Ring status
show xlate	View slot and translation information
snmp-server	Specfiy which servers have access to PIX Firewall events