Cisco PIX® Device Manager 3.0 Online Help

Cisco Systems

Contents

Find Help

- Index
- Glossary
- Help Topics
- Menus
- Tabs

- Cisco PIX Firewall Documentation
- FWSM Documentation
- Troubleshooting
- Obtaining Technical Assistance

Wizards

- Startup Wizard
- VPN Wizad

Menus

- File
- Options
- Search
- Tools

Cisco.com Resources

- Obtaining Technical Assistance
- Top Security Resources
- PIX Firewall Documentation
- PIX Firewall Product Literature
- PIX Command Reference
- PIX Software Updates
- PIX Bug Navigator II
- FWSM Documentation

Getting Started

- Getting Started
- About PDM - What's New
- Wizards
- General Topics
- Graphs
- Refresh
- PDM Icon Legend
- Status Bar
- CLI Commands Used by PDM Screens
- Unsupported Commands
- Obtaining Technical Assistance

Main Tabs

- Access Rules
- Translation Rules
- VPN
- Hosts/Networks
- System Properties
- Monitoring

More (Tutorials, Advanced Topics)

- More>Configuration Changes in PDM
- More>Internet Protocol (IP)
- More>NAT Dynamic
- More>NAT Static
- More>Password Policy
- More>Example Configurations
- More>TAC Resources for PIX Firewall
- More>VPN

TAC Resources

- More>TAC Resources for PIX Firewall
- Obtaining Technical Assistance>TAC
- Cisco Technical Assistance Center (TAC Public)
- PIX Firewall-TAC Home
- PIX Firewall Top Issues
- PIX Firewall Technical Tips
- TAC Security Tools
- IPSec VPN Support
- IPSec Technical Tips
- Security Product Field Notices (including PIX)

Copyright © 2001-2004, Cisco Systems, Inc.

Cisco PIX® Device Manager 3.0
Online Help

Cisco Systems

The following sections are included in this Help topic:

- Introduction
- About PDM Software
- System Requirements
  - Important Notes
  - Firewall Requirements
  - Browser Requirements
  - PC/Workstation Requirements
    - Windows
    - Sun Solaris
    - Linux
  - Configuration Recommendations
    - JVM, Browser, OS Combinations
- Obtaining Technical Assistance
- Earlier PDM Versions

Introduction

Cisco PIX Device Manager (PDM) Version 3.0(4) is the graphical user interface (GUI) software for configuring and monitoring your Cisco PIX Firewall. For information about earlier versions of PDM, see Earlier PDM Versions.

PDM Version 3.0 will run on all PIX 501, PIX 506/506E, PIX 515/515E, PIX 520, PIX 525, and PIX 535 platforms running Version 6.3. PDM Version 3.0 is a single image which supports only PIX Firewall Version 6.3.

PDM is designed to assist you in managing your network security. For example, PDM does the following:

- Runs on most popular operating systems and web browsers and does not require a separate plug-in. The PDM applet uploads to your workstation when you point your browser at the firewall.
- Helps you configure your firewall using visual tools such as task-oriented selections and drop-down menus, including a Startup Wizard to get up and running fast.
- Speeds up configuration by composing complex command-line interface (CLI) commands for you and then sending them to the firewall.
- Simplifies maintenance of existing configurations that were originally implemented using the firewall CLI or Cisco Secure Policy Manager (CSPM) or Management Center for PIX Firewalls.
- Monitors and configures one firewall unit at a time, but you can point your browser to more than one firewall unit and administer several from a single workstation.
- Simplifies remote access or site-to-site VPN setup with VPN Wizard.

- Allows both the active and standby firewalls to be configured for LAN-based failover.
- User security allows full administrative access or enforces read-only and monitor-only mode.
- Reduces troubleshooting time by warning of potential configuration errors before they are sent to the firewall.

About PDM Software

If your firewall unit is currently running Cisco PIX Firewall Version 6.3, the PDM 3.0 software is already loaded in the firewall Flash memory for you.

See About PDM for information about new features in PDM 3.0.

System Requirements

The following information is included in this section:

- Important Notes
- Firewall Requirements
- Browser Requirements
- PC/Workstation Requirements
    - Windows
    - Sun Solaris
    - Linux

Important Notes

- **CLI Command Support**—PDM Version 3.0 uses the PIX Firewall CLI command syntax which is very similar to Cisco IOS software, but not identical. Almost all PIX Firewall CLI commands are fully supported by PDM. If you are using PDM with an existing firewall configuration, refer to PDM Support for PIX Firewall CLI Commands for information on the few exceptions.
- **Multiple PDM Sessions**—PDM allows multiple PCs or workstations to each have one browser session open with the same firewall. A single firewall unit can support up to concurrent 5 PDM sessions. Only one session per browser per PC or workstation is supported for a particular firewall. See More Configuration Changes>Multiple CLI Sessions.
- **PIX OS Version**—PDM 3.0 requires PIX Firewall Version 6.3 and does not run with PIX Firewall versions earlier than Version 6.3. Refer to Earlier versions of PDM.
- **Java Plug-in Supported—**PDM Version 3.0 supports the Java plug-in 1.4.2 or higher for browsers.
- **Caveats**—Please use Bug Navigator II on CCO to view current caveat information. Bug Navigator II may be accessed at the following web site: http://www.cisco.com/support/bugtools
- **Changing OS Color Schemes**—If you change the color scheme of your operating system while PDM is

running, you should restart PDM or some PDM screens may not display correctly.
- **Installing New PDM Versions**—When you install a new version of PDM, close all browser sessions before launching PDM.

Firewall Requirements

If you are using a PIX Firewall already running PIX Firewall software Version 6.3, then you have already met all the requirements to run PDM 3.0 that are discussed in Firewall Requirements and can continue to the "Browser Requirements" section.

A firewall unit must meet the following requirements to successfully install and run PDM:

- **Encryption Licensing**—You must have an activation key that enables Data Encryption Standard (DES) or the more secure 3DES, which PDM requires for support of the Secure Sockets Layer (SSL) protocol. Cisco PIX Device Manager is included as part of Cisco PIX Firewall operating system Version 6.3. A separate license for PDM is not required.
  - Registered cisco.com users can request a DES (free), 3DES/AES activation key from the following URL:
    http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=324
  - New cisco.com users can complete the form at this URL before requesting a DES (free), 3DES/AES activation key:
    http://www.cisco.com/pcgi-bin/Software/FormManager/formgenerator.pl
    3DES/AES activation keys are available as part of a feature license upgrade and are not free.
- **Minimum Software Versions**—Verify that your firewall meets the requirements listed in the *Release Notes for the Cisco Secure PIX Firewall Version 6.3*. You must have Version 6.3 installed on the Cisco firewall unit before using PDM 3.0. For more information, see Important Notes and Earlier PDM Versions.
- **Upgrading Software**—For information on upgrading your Cisco PIX Firewall software, see the following web site:
  http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a0080094a5d.shtml

---

Browser Requirements

The following are required to access one or more firewall units through PDM:

- **Minimum Disk Space Requirement**—PDM requires the minimum amount of temporary disk space required by your browser to run on your operating system.
- **Java Plug-in—**A JavaScript and Java enabled browser running JDK 1.4.2 or higher. If Java is not enabled in the browser, PDM guides you on how to enable them. To check which version you have, launch PDM. When the PDM information window appears, the field "JDK Version" indicates your JDK version. If you have an older JDK version, you can get the latest JVM from Microsoft by downloading the product called "Virtual Machine" from Microsoft's JVM update web site.
  PDM Version 3.0 supports the Java Plug-in for browsers. When using the Java Plug-in, there is a significant

improvement in PDM load time if you access the firewall using the host name (not IP address). See Configuration Recommendations.

- **HTTP 1.1**—Settings for Internet Options>Advanced>HTTP 1.1 settings should use HTTP 1.1 for both proxy and non-proxy connections

---

PC/Workstation Requirements

PDM has different requirements depending on the platform from which it is accessed. It is supported on Microsoft Windows 2000, and Microsoft Windows XP.

PDM is not supported on Macintosh, Windows 3.1, Windows 95, Windows 98, Windows ME, or Windows NT operating systems.

This section includes the following topics:

- Windows Requirements
- SUN Solaris Requirements
- Linux Requirements

Windows Requirements

Operating Systems

- Microsoft Windows 2000 (Service Pack 4), or Microsoft Windows XP (English or Japanese version of Windows)

Browsers

- Internet Explorer 6.0 with native JVM (VM 3809 or higher) ***-or-***
- Internet Explorer 6.0 with Java Plug-in 1.4.2 or 1.5.0 ***-or-***
- Netscape 7.2 with Java Plug-in 1.4.2 or 1.5.0

Hardware

- Any Pentium III or Pentium-compatible processor running at 450 MHz or higher.
- At least 256 MB of random-access memory (RAM).
- A 1024 x 768 pixel display and at least High Color (16-bit) colors.

SUN Solaris Requirements

The following requirements apply to the use of PDM with Sun SPARC:

Operating Systems

- Sun SPARC Solaris 2.8 or 2.9

Browsers

- Mozilla 1.4 with Java Plug-in 1.4.2

Hardware

- SPARC microprocessor.
- At least 256 MB of random-access memory (RAM).
- An 1024 x 768 pixel display and at least High Color (16-bit) colors.

Linux Requirements

The following requirements apply to the use of PDM with Linux:

Operating Systems

- Red Hat Linux 9, Red Hat Enterprise Linux WS version 3

Browser

- Mozilla 1.4 with Java Plug-in 1.4.2

Hardware

- At least 256 MB of random-access memory (RAM).
- A 1024 x 768 pixel display with at least 256 colors. We recommend a 1024 x 768 pixel display and at least 16-bit colors.

Configuration Recommendations

JVM, Browser, OS Combinations

We recommend the following browser and JVM (Java Virtual Machine) combinations for these operating systems:

Operating System	Browser	JVM
Microsoft Windows 2000 (Service Pack 4), or Microsoft Windows XP	Internet Explorer 6.0	IE native (built-in) JVM (VM 3809)
Microsoft Windows 2000 (Service Pack 4), or Microsoft Windows XP	Internet Explorer 6.0	Java Plug-in 1.4.2
Microsoft Windows 2000 (Service Pack 4), or Microsoft Windows XP	Netscape 7.1	Java Plug-in 1.4.2
Sun Solaris 2.9	Mozilla 1.4	Java Plug-in 1.4.2
Red Hat Linux 9.0 running GNOME or KDE	Mozilla 1.4	Java Plug-in 1.4.2

Earlier PDM Versions

For documentation about earlier PDM versions, see the following web site:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/index.htm.

PDM and Firewall Version Dependencies

PDM	PIX Firewall	FWSM (Firewall Services Module)
1.0*	6.0, 6.1	
1.1	6.0, 6.1	
2.0*	6.2	
2.1	6.2	1.1
3.0	6.3	

*Obsolete version

Firewall Services Module

PDM Version 2.1 also supported the Firewall Services Module (FWSM) for the Catalyst 6000 switch. For more information about FWSM for Catalyst, see
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/index.htm.

Upgrading Earlier PDM Software

When you install a new version of PDM, close all browser sessions before launching PDM.

For information on upgrading your Cisco PIX Firewall software, see the following web site:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a0080094a5d.shtml

Copyright © 2001-2004, Cisco Systems, Inc.

A-D

AAA—Authentication, Authorization, and Accounting. *See also* TACACS+ and RADIUS.

ABR—Area Border Router. In OSPF, a router that has interfaces in multiple areas.

Access Control, Access Control Rule, ACE—Information entered into the configuration which lets you specify what type of traffic to permit or deny into an the interface. By default, traffic that is not explicitly permitted is denied.

ACL—Access Control List. A collection of Access Control Entries. An access list lets you specify what type of traffic to allow into an interface. By default, traffic that is not explicitly permitted is denied. *See also* Rule.

ActiveX—A set of object-oriented programming technologies and tools used to create mobile or portable programs. An ActiveX program is roughly equivalent to a Java applet.

Address Translation—The translation of a network address and/or port to another network address/or port. *See also* IP Address, NAT, PAT, Static PAT, and Interface PAT.

(PIX) Administrative Access Modes, Access Modes—PIX Firewall version 6.2 introduced support for up to 16 levels (0-15) of command authorization. This is similar to what is available with Cisco IOS software. With this feature, you can assign specific PIX Firewall commands to one of 16 levels. You can either assign separate passwords for each privilege level or perform authentication using a local or remote AAA database of user accounts.

For information about configuring this feature, refer to the *Cisco PIX Firewall and VPN Configuration Guide* in the chapter "Accessing and Monitoring PIX Firewall."

The PIX Firewall, and other firewall products using the PIX command set, provide five administrative access modes from the CLI:

- **Unprivileged** mode—Available without entering a password, when you first access the PIX Firewall. In this mode, the PIX Firewall displays the ">" prompt and lets you enter a small number of commands. In PIX Firewall version 6.2 and higher, by default, commands in this mode are mapped to privilege Level 0.
- **Privileged** mode—Displays the "#" prompt and lets you change configuration information. Any unprivileged command also works in privileged mode. Use the **enable** command to start privileged mode and the **disable**, **exit**, or **quit** commands to exit. In PIX Firewall version 6.2 and higher, by default, all privileged mode commands are mapped to privilege Level 15. You can assign enable passwords to other privilege levels and reassign specific commands to each level.

- **Configuration** mode—Displays the prompt **<***pix_name***>(config)#**, where *pix_name* is the host name assigned to the PIX Firewall. You use configuration mode to change system configuration. All privileged, unprivileged, and configuration commands work in this mode. Use the **configure terminal** command to start configuration mode and the **exit** or **quit** commands to exit.

- **Subcommand** mode—Displays the prompt **<***pix_name***>(config-<***main_cmd_name***>)#**,where *pixname* is the host name assigned to the PIX Firewall and *main_cmd_name* is the Object Grouping command used to enter subcommand mode. Object Grouping is a way to simplify access control by letting you apply access control statements to groups of network objects, such as protocols or hosts. For further information about enabling and using this mode, refer to the *Cisco PIX Firewall and VPN Configuration Guide,* "Simplifying Access Control with Object Grouping" section in "Controlling Network Access and Use."

- **Monitor** mode—This is a special mode that enables you to update the image over the network. While in the monitor mode, you can enter commands specifying the location of the TFTP server and the binary image to download. For information about using monitor mode to upgrade your PIX Firewall software, refer to *Cisco PIX Firewall and VPN Configuration Guide*, "Changing Feature Licenses and System Software."

AES—(Advanced Encryption Standard) is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits. *See also* DES and 3DES.

Authentication Header (AH)—Authentication Header. A security protocol that provides authentication and optional replay-detection services. AH is embedded in the data to be protected (a full IP datagram, for example). AH can be used either by itself or with Encryption Service Payload (ESP). This is an older IPSec protocol that is less important in most networks than ESP. AH provides authentication services but does not provide encryption services. It is provided to ensure compatibility with IPSec peers that do not support ESP, which provides both authentication and encryption. *See also* VPN and encryption. Refer to the RFC 2402.

AH Authentication—Authentication Header is an IP protocol (type 51) that can ensure data integrity, authentication, and replay detection. AH does not provide encryption and has been largely superseded by ESP. AH may be required when the remote peer does not support ESP.

A record address—"A" stands for address, and refers to name-to-address mapped records in DNS.

ARP—Address Resolution Protocol—A low-level TCP/IP protocol that maps a node's hardware address (called a "MAC" address) to its IP address. Defined in RFC 826. An example hardware address is 00:00:a6:00:01:ba. (The first three groups specify the manufacturer, the rest identify the host's motherboard.)

ASA—Adaptive Security Algorithm. Allows one-way (inside to outside) connections without an explicit configuration for each internal system and application.

Asymmetric Encryption—Also called Public key systems, this approach allows anyone to obtain access to anyone else's public key and therefore send an encrypted message to that person using the public key. *See also* VPN and encryption.

Authenticate, Authentication—Cryptographic protocols and services which verify the identity of users and the integrity of data. One of the functions of the IPSec framework. Authentication establishes the integrity of datastream

and ensures that it is not tampered with in transit. It also provides confirmation about datastream origin. *See also* AH, AH Authentication, AAA, encryption,VPN, and encryption.

Cache—A temporary repository of information accumulated from previous task executions that can be reused, decreasing the time required to perform the tasks.

CA—Certificate Authority, Certification Authority. A third-party entity that is responsible for issuing and revoking certificates. Each device that has its own certificate and public key of the CA can authenticate every other device within a given CA's domain. This term is also applied to server software that provides these services. A trusted source which issues Digital Certificates. *See also* ITU X.509 , and CA.

CBC—Cipher Block Chaining. A cryptographic technique which increases the encryption strength of an algorithm. CBC requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet.

Certificate—A signed cryptographic object that contains an identity and a public key associated with this identity. *See also* ITU X.509, Digital Certificate, and Certificate.

Cisco.com—Obtaining Technical Assistance, cisco.com.

CLI—Command Line Interface. The primary interface for entering configuration and monitoring commands to the PIX Firewall. To use the CLI from PDM, *see* CLI. Refer to the *Cisco PIX Firewall and VPN Configuration Guide* and the *Cisco PIX Firewall Command Reference* for more information. *See also* access modes.

Note: For more information about the CLI commands used by each PDM Screen, *see* CLI Commands Used by PDM Screens.

Caution: PIX and IOS CLI Syntax—The PIX Firewall CLI uses similar syntax and other conventions to the Cisco IOS CLI, but the PIX Firewall operating system is not a version of Cisco IOS software. Do not assume that a Cisco IOS CLI command works or has the same function with the PIX Firewall.

Cookie—A cookie is a web browser feature which stores or retrieves information, such as a user's preferences, to persistent storage. In Netscape and Internet Explorer, cookies are implemented by saving a small text file on your local hard drive. The file can be loaded the next time you run a Java applet or visit a website. In this way information unique to you as a user can be saved between sessions. The maximum size of a cookie is approximately 4KB.

Client/server computing—Term used to describe distributed computing (processing) network systems in which transaction responsibilities are divided into two parts: client (front end) and server (back end). Also called *distributed computing*. *See also* RPC.

Conduit—An exception to the PIX Firewall Adaptive Security Algorithm permitting connections from external to internal networks. Refer to the *Cisco PIX Firewall VPN and Configuration Guide* for information about conduits.

Configuration, Config, Config File—The PIX Firewall file which represents the equivalent of settings, preferences, and properties administered by PDM or the CLI. *See also* Configuration File Terminology. More

CRL, RA—Certificate Revocation List. A digitally signed message that lists all of the current but revoked certificates listed by a given CA. This is analogous to a book of stolen charge card numbers that allow stores to reject bad credit cards. When digital certificates are revoked, they are added to a certificate revocation list (CRL). When you implement authentication using certificates, you can choose to use CRLs or not. Using CRLs lets you easily revoke certificates before they expire, but the CRL is generally only maintained by the CA or its authorized Registration Authority (**RA**). If you are using CRLs and the connection to the CA or RA is not available when authentication is requested, the authentication request will fail . *See also* Digital Certificate, CA, and More>CA.

Cryptography, crypto, cryptographic services—Encryption, authentication, integrity, keys and other services used for secure communicating over networks. *See* VPN and IPSec.

Crypto map—A crypto map is applied to an interface. A data structure with a unique name and sequence number which is used for configuring VPNs on the PIX Firewall. A Crypto Map performs two primary functions:(1) it selects data flows that need security processing and (2) defines the policy for these flows and the crypto peer that traffic needs to go to.

The concept of a crypto map was introduced in Cisco's classic crypto for IOS but was expanded for IPSec.

Crypto maps contain the ACLs, encryption standards, peers, and other parameters necessary to specify security policies for VPNs using IKE and IPSEC. *See also* VPN.

CSPM—Cisco Secure Policy Manager (CSPM) is a multi-device management tool for Cisco security products including PIX Firewalls, Cisco IOS firewalls, VPN routers and Intrusion Detection System (IDS) Sensors. CSPM also provides other management services including monitoring, notification and reporting. For more information, *see* http://wwwin.cisco.com/cmc/cc/pd/sqsw/sqppmn/prodlit/csp22_rg.htm.

Caution: CSPM operates on the assumption that it is the only management interface for the PIX, and it will overwrite configuration changes made through other means, including PDM. *See* CSPM and PDM in Applying Configuration Changes for additional information.

CTIQBE—Computer Telephony Interface Quick Buffer Encoding. Used in IP telephony.

Cut-Through Proxies—User-based authentication of inbound or outbound connections. Allows security policies to be enforced on a per-user-ID basis, providing faster traffic flow after authentication.

Data confidentiality—Method where protected data is manipulated so that no attacker can read it. This is commonly provided by data encryption and keys that are only available to the parties involved in the communication.

Data integrity—Data integrity mechanisms, through the use of secret key based or public key based algorithms, that allow the recipient of a piece of protected data to verify that the data has not been modified in transit.

Data origin authentication—A security service where the receiver can verify that protected data could have originated only from the sender. This service requires a data integrity service plus a key distribution mechanism, where a secret key is shared only between the sender and receiver.

DES, 3DES, Triple DES—The DES was published in 1977 by the National Bureau of Standards and is a secret key encryption scheme based on the Lucifer algorithm from IBM. The contrast of DES is public-key. Cisco uses DES in classic crypto (40-bit and 56-bit key lengths), IPSec crypto (56-bit key), and on the PIX Firewall (56-bit key) and 3-DES (triple DES), which performs encryption three times using a 56-bit key. 3DES is more secure than DES but requires more processing for encryption and decryption. DES is generally considered secure enough for most business purposes. *See also* AES.

If your firewall is not enabled for DES, you can have a new activation key sent to you by completing the form at the following website: https://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=324 *See also* ESP.

DHCP—Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses to hosts dynamically, so that addresses can be reused when hosts no longer need them.

Diffie-Hellman—A Public key cryptography protocol that allows two parties to establish a shared secret over insecure communications channels. Diffie-Hellman is used within Internet Key Exchange (IKE) to establish session keys. Diffie-Hellman is a component of Oakley key exchange.

Diffie-Hellman Group 1, Group 2, and Group 5—Diffie-Hellman refers to a type of Public key cryptography using asymmetric encryption based on large prime numbers to establish both Phase 1 and Phase 2 SAs. Group 1 provides a smaller prime number than Group 2 but may be the only version supported by some IPSec peers. Diffe-Hellman Group 5 uses a 1536 bit prime number, is the most secure, and is recommended for use with AES.

See also VPN and encryption.

Digital Certificate, Certificate—Certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object. Digital Certificates are issued by trusted sources called certificate or certification authorities (CAs). Certificates have an expiration date and may also be placed on a certificate revocation list (CRL) if known to be compromised. *See also* ITU X.509.

Digital certificates also establish non-repudiation for IKE negotiation, which means that you can prove to a third party that IKE negotiation was completed with a specific peer.

Note: PIX Firewall time must be set to GMT in order to use Certificates.

See VPN>IKE>Certificate, VPN>Certificate>Configuration , VPN, and encryption.

DMZ—*See* Interface.

DNS, Domain Name—Domain Name System (or Service). An Internet service that translates domain names, which are alphabetic, into IP addresses, which are composed of numbers. Domain name registration information may be found at InterNIC.

DSS—A digital signature algorithm designed by The US National Institute of Standards and Technology (NIST) based on public key cryptography. DSS doesn't do user datagram encryption. DSS is a component in classic crypto, as well as the Redcreek IPSec card, but not in IPSec implemented in Cisco IOS software.

Dynamic PAT, NAT—*See also* NAT, PAT, and Address Translation.

E-H

ECHO—*See* Ping, ICMP. *See also* Fixup.

EMBLEM, Cisco EMBLEM Syslog Format—Enterprise Management BaseLine Embedded Manageability. EMBLEM syslog format is designed to be consistent with the Cisco IOS system log format and is more compatible with CiscoWorks management applications. See Configuration>System Properties>Logging>Syslog>Advanced.

Encryption, **Decryption** —Application of a specific algorithm or *cipher* to data, *cleartext*, so as to alter the appearance of the data making it incomprehensible, *ciphertext*, to those who are not authorized to see the information without a public key, pre-shared key, or other means of *deciphering* it.

The encryption algorithms supported by the PIX Firewall include DES, 3-DES (triple DES). *See* PIX Firewall Requirements.

Encryption Service Adapter (ESA)—A hardware based encryption accelerator that is used in:

- Cisco 7204 and 7206 routers
- Second-generation Versatile Interface Processor2-40s (VIP2-40s) in all Cisco 7500 series routers
- VIP2-40 in the Cisco 7000 series routers that have the Cisco 7000 series Route Switch Processor (RSP7000) and Cisco 7000 series Chassis Interface (RSP7000CI) cards installed.

IPSec does not use the ESA acceleration, but will work in a box that has an ESA card on a software-only basis.

ESP—Encapsulated Security Payload. This is the most important IPSec protocol, which provides authentication and encryption services for establishing a secure tunnel over an insecure network. *See* VPN, encryption. Refer to RFC 2406—IP Encapsulating Security Payload (ESP). and RFC 1827 for more information. The PIX Firewall implements the mandatory 56-bit DES-CBC with Explicit IV (RFC 2405); as the encryption algorithm, and MD5-HMAC (RFC 2403) or SHA-HMAC (RFC 2404) as the authentication. 3DES is also supported.

ESP Authentication—A hash algorithm is used to create a message digest, which is used for ensuring message integrity. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has been a successful (but extremely difficult) attack demonstrated against MD5.

ESP Encryption—Encapsulated Security Protocol (ESP) is the IPSec protocol used in the default transform sets provided with PIX Firewall. ESP is an IP protocol (type 50) that ensures message privacy through encryption, as well as data integrity, authentication, replay detection.

Failover, Failover mode—The PIX Firewall feature which links a primary unit and standby (or secondary) unit together, sharing the same configuration file, so that, if the primary fails, the standby unit can continue to provide network services. *See also* System Properties>Failover.

Fixup—A procedure the PIX Firewall employs to process certain application-level protocols. The specific processing performed by a fixup will vary by protocol, and can include tasks such as translating IP addresses embedded in the protocol payload and providing access through the PIX Firewall for dynamically-created data sessions.

Flash, Flash memory—A memory chip which retains data without power. A type of nonvolatile storage device. The Firewall configuration may written to its internal Flash by a menu item or . Note: Not related to Macromedia Flash, a web animation plug-in and file format standard.

FragGuard feature—a Cisco feature that provides IP fragment protection and performs full reassembly of all ICMP error messages and virtual reassembly of the remaining IP fragments that are routed through the PIX Firewall.

FTP—File Transfer Protocol. Part of the TCP/IP protocol stack, used for transferring files between hosts. *See also* Fixup.

Peer FQDN/IP—(Fully Qualified Domain Name/IP Address) IPSec parameter which identifies peers that are security gateways. *See also* VPN>Certificates>Peer FQDN/IP, DNS, and Certificates.

GMT—Greenwich Mean Time standard. Replaced by UTC (Coordinated Universal Time) in 1967 as the world time standard.

GRE—Generic Routing Encapsulation described in RFC1701, RFC1702. GRE is a tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single-protocol backbone environment.

See also PPTP and Multicasting Over GRE Tunnels.

H.225—A protocol used for TCP signalling in applications such as video conferencing. *See also* H.323 and Fixup.

H.225.0—An ITU standard that governs H.225.0 session establishment and packetization. H.225.0 actually describes several different protocols: RAS, use of Q.931, and use of RTP.

H.245—An ITU standard that governs H.245 endpoint control.

H.320—Suite of ITU-T standard specifications for videoconferencing over circuit-switched media, such as ISDN, fractional T-1, and switched-56 lines. Extension of ITU-T standard H.320 that enables videoconferencing over LANs and other packet-switched networks, as well as video over the Internet.

H.323—Allows dissimilar communication devices to communicate with each other by using a standardized communication protocol. H.323 defines a common set of CODECs, call setup and negotiating procedures, and basic data transport methods.

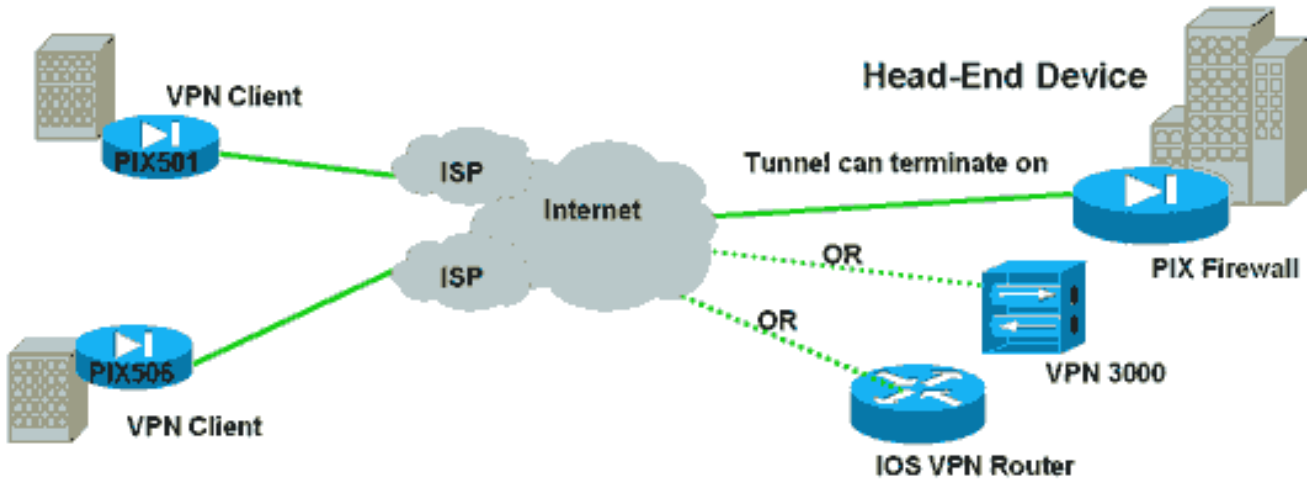
H.323 RAS—The registration, admission, and status (RAS) signaling protocol performs registration, admissions, bandwidth changes, and status and disengage procedures beteeen VoIP gateway and the gatekeeper.

H.450.2—Call transfer supplementary service for H.323.

H.450.3—Call diversion supplementary service for H.323.

Hash, Hash Algorithm— A hash algorithm a one way function which operates on a message of arbitrary length to to create a fixed length message digest used by cryptographic services to ensure its data integrity. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has been a successful (but extremely difficult) attack demonstrated against MD5. Cisco uses both Secure Hash Algorithm (SHA) and Message Digest 5 (MD5) hashes within our implementation of the IPSec framework. *See also* VPN, encryption, and HMAC.

Headend—A firewall, concentrator, or other host which serves as the entry point into a private network for VPN client connections over the public network. *See also* VPN and ISP.



HMAC—A mechanism for message authentication using cryptographic hashes such as SHA and MD5. For an exhaustive discussion of HMAC, *see* RFC 2104.

Host—A computer, such as a PC, or other computing device, such as a server, associated with an individual IP address and optionally a name. The name for any device on a TCP/IP network that has an IP address. In firewall configuration, a host is distinguished from a network. Also any network-addressable device on any network. The term "node" includes devices such as routers and printers which would not normally be called "hosts".

Host/Network—An IP address and mask (or netmask) used with other information to identify a single host or network subnet for Firewall configuration, such as an address translation (xlate) or access control rule (ACE).

HTTP, HTTPS—Hypertext Transfer Protocol, Hypertext Transfer Protocol, Secure. The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files. *See also* Fixup and System Properties>Administration>PDM HTTPS.

▲

I-L

IANA—Internet Assigned Number Authority. Assigns all port and protocol numbers for use on the Internet.

> **Port Numbers**—You can view port numbers at the following site:
> http://www.iana.org/assignments/port-numbers
>
> **Protocol Numbers**—You can view protocol numbers at the following site:
> http://www.iana.org/assignments/protocol-numbers

ICMP—Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. *See* System Properties>Administration>ICMP.

IDS—Intrusion Detection System. A method of detecting malicious network activity by signatures and then implementing a policy for that signature.

IETF—The Internet Engineering Task Force. A technical standards organization which develops RFC (request for comment) documents defining protocols for the internet.
http://www.ietf.org/home.html

IGMP—Internet Group Management Protocol. *See* Multicast Routing, IETF RFC 2236 IGMPv2, IETF draft-ietf-idmr-igmp-proxy-01.txt. *See* System Properties>Multicast>IGMP.

IKE—Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each router/firewall/host must verify the identity of its peer. This can be done by manually entering pre-shared keys into both hosts or by a CA service.

IKE is a hybrid protocol that uses part Oakley and part of another protocol suite called SKEME inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each router/firewall/host must be able to verify the identity of its peer. This can be done by manually entering pre-shared keys into both hosts, by a CA service, or the forthcoming secure DNS (DNSSec). This is the protocol formerly known as ISAKMP/Oakley, and is defined in RFC 2409—The Internet Key Exchange (IKE). A potential point of confusion is that the acronyms "ISAKMP" and "IKE" are both used in Cisco IOS software to refer to the same thing. These two items are somewhat different, as you will see in the next definition.

IKE Extended Authentication—(Xauth) is implemented per the IETF draft-ietf-ipsec-isakmp-xauth-04.txt ("extended authentication" draft). This provides this capability of authenticating a user within IKE using TACACS+ or RADIUS.

See VPN>IKE Policies. *See also* VPN and encryption.

IKE Mode Configuration, **Mode Config**—PIX IKE Mode Configuration is implemented per the IETF draft-ietf-ipsec-isakmp-mode-cfg-04.txt. IKE Mode Configuration provides a method for a security gateway to download an IP address (and other network level configuration) to the VPN client as part of an IKE negotiation.

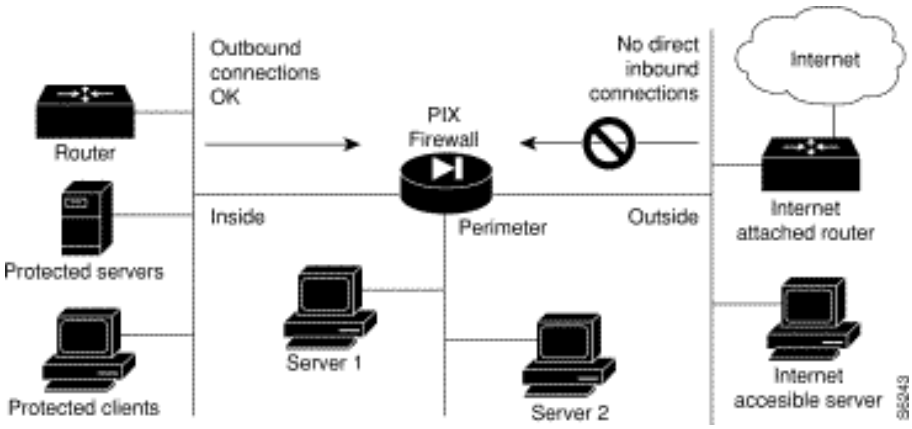
ILS—Internet Locator Service. The Internet Locator Service (ILS) is based on the Lightweight Directory Access Protocol (LDAP) and is ILSv2 compliant. ILS was developed by Microsoft for use with its NetMeeting, SiteServer, and Active Directory products.

Implicit Rule—An Access Rule automatically created by the PIX Firewall based on default rules or as a result of user-defined rules.

Inside—*See* Interface.

Interface, Interface Name—The physical connection between a particular network and a PIX Firewall. The inside interface default name is "**inside**" and the outside interface default name is "**outside**." Any perimeter interface default names are "intf*n*," such as "**intf2**" for the first perimeter interface, "**intf3**" for the second perimeter interface, and so on to the last interface. The numbers in the **intf** string corresponds to the interface card's position in the PIX Firewall. You can use the default names or, if you are an experienced user, give each interface a more meaningful name.

Interface Names—Human readable name assigned to a PIX Firewall network interface, a physical network connector. These names are customary and referenced by PIX Firewall documentation:



- **inside**—The first interface, usually port 1, which connects your internal, "trusted" network protected by your PIX Firewall.
- **outside**—The first interface, usually port 0, which connects to other "untrusted" networks outside your PIX Firewall; the Internet.
- **intf*n***—Any interface, usually beginning with port 2, which connects to a subset network of your design that you can custom name and configure, for example, **dmz** or **perimeter** to be an "inside" or "outside" type.
- **Interface PAT**—The use of Port Address Translation where the PAT IP address is also the IP address of the outside interface. *See* PAT.

Internet—The global network which uses IP, Internet protocols. Not a LAN. *See also* intranet.

Intranet—Intranetwork. A LAN which uses IP, Internet protocols. *See also* network and Internet.

IP—Internet Protocol. The Internet protocols are the world's most popular open-system (nonproprietary) protocol suite because they can be used to communicate across any set of interconnected networks and are equally well suited for LAN and WAN communications.

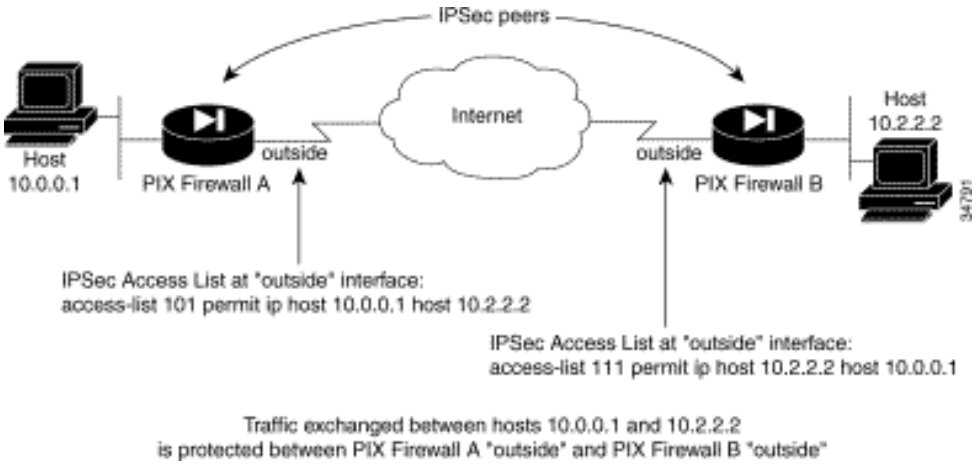
IP Address—IP version 4 addresses are 32-bits, or 4 bytes, in length. This address "space" is used to designate the following:

- network number
- optional subnetwork number
- a host number

The 32 bits are grouped into four octets (8 binary bits), represented by 4 decimal numbers separated by periods or "dots". The meaning of each of the four octets is determined by their use in a particular network.

IP Pool, IP Address Pool—*See* Pool.

IPSec—IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer.



IPSec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

IPSec operates in Phase 1 Phase 2.

IPSec provides a Tunnel Mode and a Transport Mode.

See also VPN, encryption, IKE, Site-to-Site VPN, SA, ESP, Split Tunneling, and VPN>IPSec Rules.

ISAKMP—The Internet Security Association and Key Management Protocol. A protocol framework that defines

payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association. *See* IKE.

ISP—Internet Service Provider. An organization which provides connection to the internet via their services, such as modem dial in over telephone voice lines or DSL.

Key, Cryptographic key—A data object used for encryption, decryption and/or authentication. Keys are only available to the parties involved in the communication. *See also* Secret key, and Pre-shared key, Public key, VPN>IKE>Pre-Shared Keys.

LAN—Local Area Network. A network residing in one location or belonging to one organization, typically, but not necessarily using the Internet protocols. Not the global Internet. *See also* intranet, network, and Internet.

Layer, Layers—*See* Protocol.

L2TP—Layer Two Tunneling Protocol. An Internet Engineering Task Force (IETF) standards track protocol defined in RFC 2661 that provides tunneling of PPP. The Layer Two Tunneling Protocol (L2TP) is an extension to the point-to-point protocol (PPP). L2TP merges Cisco's older Layer Two Forwarding (L2F) protocol with Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP can be used with IPSec encryption and is considered more secure against attack than PPTP. L2TP is available with Windows 2000 and Windows XP systems. *See* PPTP.

The Layer Two Tunneling Protocol (L2TP) is an extension to the point-to-point protocol (PPP). L2TP merges Cisco's older Layer Two Forwarding (L2F) protocol with Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP can be used with IPSec encryption and is considered more secure against attack than PPTP. L2TP is available with Windows 2000 and Windows XP systems.

LDAP—Lightweight Directory Access Protocol. Protocol that provides access for management and browser applications that provide read/write interactive access to the X.500 Directory. *See* ILS.

M-P

Mask, IP Subnet Mask, Netmask—A 32-bit bit mask which shows how an Internet address is to be divided into network, subnet and host parts. The netmask has ones in the bit positions in the 32-bit address which are to be used for the network and subnet parts, and zeros for the host part. The mask should contain at least the standard network portion (as determined by the address's class), and the subnet field should be contiguous with the network portion. *See also* IP Address, TCP/IP, host, host/network, and More>IP.

MC, MC Router—Multicast (MC) routers route multicast data transmissions to the hosts on each LAN in an internetwork that are registered to receive specific multimedia or other broadcasts.

MGCP—Media Gateway Control Protocol.

Message Digest—A message digest is created by a hash algorithm , such as MD5 or SHA-1, which is used for ensuring message integrity. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has

been a successful (but extremely difficult) attack demonstrated against MD5.

MD5—Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and are designed to strengthen the security of the MD4 hashing algorithm. SHA is more secure than MD4 and MD5. Cisco uses hashes for authentication within the IPSec framework. Cisco uses hashes for authentication within the IPSec framework. Also used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

See also VPN, encryption, and More>VPN.

Mode, Modes—*See* PIX Administrative access modes.

Mode Config, IKE Mode configuration—*See* IKE Mode Configuration.

MTU—Maximum transmission unit—The maximum number of bytes in a packet that can flow efficiently across the network with best response time. For Ethernet, the default MTU is 1500 bytes, but each network can have different values, with serial connections having the smallest values. The MTU is described in RFC 1191.

Multicast, Multicast Routing, MCR—Multicast refers to a network addressing method in which the source transmits a packet to multiple destinations, a multicast group, simultaneously.

Multicast Addressing

Multicast addresses range from **224.0.0.0** to **239.255.255.255**, however only the range **224.0.1.0** to **239.255.255.255** is available to us.

The first part of the multicast address range, **224.0.0.0** to **224.0.0.255**, is reserved and referred to as the **Reserved Local Link Addresses** (RLLA). These addresses are unavailable.

We can exclude the RLLA range by specifying
224.0.1.0 to **239.255.255.255**.

224.0.0.0 to **239.255.255.255** *excluding* **224.0.0.0** to **224.0.0.255**
is the same as
224.0.1.0 to **239.255.255.255**.

SMR (stub multicast routing) allows the PIX Firewall to function as a "stub router." A stub router is a device that acts as an Internet Group Management Protocol (IGMP) proxy agent. The IGMP is used to dynamically register specific hosts in a multicast group on a particular LAN with a multicast (MC) router. MC routers route multicast data transmissions to the hosts on each LAN in an internetwork that are registered to receive specific multimedia or other broadcasts. A stub router forwards IGMP messages between hosts and MC routers.

PIM (protocol independent multicast) protocol provides a scalable method for determining the best paths in a network for distributing a specific multicast transmission to each host that has registered using IGMP to receive the transmission. With PIM sparse mode (PIM SM), which is the default for Cisco routers, when the source of a multicast transmission begins broadcasting, the traffic is forwarded from one MC router to the next until the packets reach every registered host. If a more direct path to the traffic source exists, the last-hop router sends a join message toward the source that causes the traffic to be rerouted along the better path.

Allowing Hosts to Receive Multicast Transmissions

When hosts that need to receive a multicast transmission are separated from the MC router by a PIX Firewall, configure the PIX Firewall to forward IGMP reports from the downstream hosts and to forward multicast transmissions from the upstream router. The upstream router is the next-hop interface toward the transmission source from the outside interface of the PIX Firewall.

Note: PIX Firewall does not pass multicast packets. Many routing protocols use multicast packets to transmit their data. If you need to send routing protocols across the PIX Firewall, configure the routers with the Cisco IOS software **neighbor** command. We consider it inherently dangerous to send routing protocols across the PIX Firewall. If the routes on the unprotected interface are corrupted, the routes transmitted to the protected side of the firewall will pollute routers there as well.

Additional Information on Multicast

The following Cisco public websites provide background information about multicast routing:

- http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/ipimt_ov.htm
- http://www.cisco.com/warp/public/732/Tech/Multicast/
- Multicasting Over GRE Tunnels

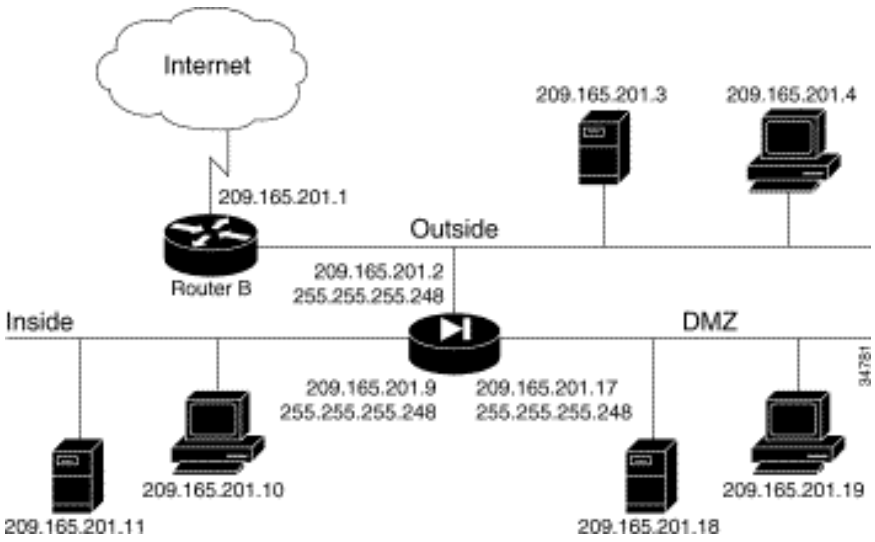
The following RFCs from the IETF provide technical details about the IGMP and multicast routing standards used for implementing the SMR feature:

- RFC 2236 IGMPv2
- RFC 2362 PIM-SM
- RFC 2588 IP Multicast and Firewalls
- RFC 2113 IP Router Alert Option
- IETF draft-ietf-idmr-igmp-proxy-01.txt

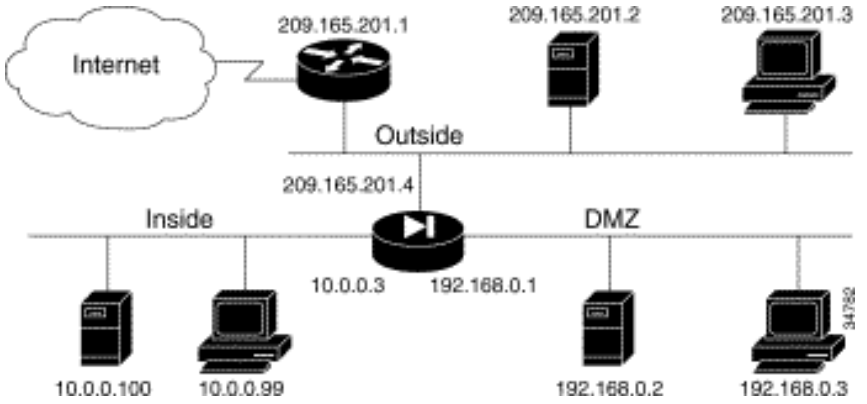
N2H2—A third party filtering application that works with the PIX Firewall to deny users access to selected web sites based on the company security policy. N2H2's URL filtering software, Filtering by N2H2, can filter HTTP requests based on destination host name, destination IP address, and username and password. Filtering by N2H2 relies on N2H2's sophisticated URL database, which includes more than 15 million sites organized into over 40 content categories. For more information about Filtering by N2H2, see N2H2's Web site at http://www.n2h2.com

NAT—Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. There are two types of NAT—static and dynamic.

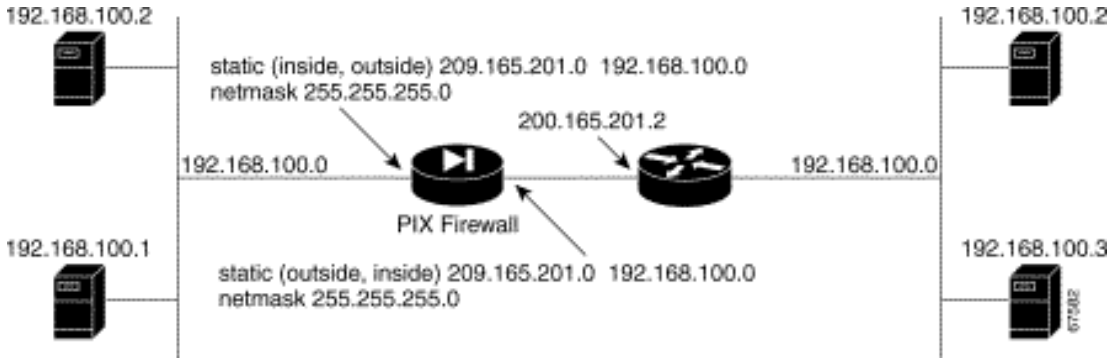
Without NAT



With NAT



Outside NAT with Overlap



See also NAT, More>Dynamic NAT, and More>Static NAT. See configuration examples in the *Cisco PIX Firewall and VPN Configuration Guide* in the chapter "Establishing Connectivity."

Netmask, Subnet Mask—*See also* Mask and More>IP.

Network—In the context of Firewall configuration, a network is a group of computing devices which share part of an IP address space and not a single host. A network consists of multiple "nodes" or devices with IP address, any of which may be referred to as "hosts." *See also* Internet, Intranet, IP, and LAN.

Node—*See also* host and network.

Nonvolatile storage, memory—Storage or memory which, unlike RAM (Random Access Memory) retains its contents without power. Data in a nonvolatile storage device survives a power-off, power-on cycle or reboot.

NTP—Network time protocol. *See also* NTP and Clock.

Oakley—A key exchange protocol that defines how to acquire authenticated keying material. The basic mechanism for Oakley is the Diffie-Hellman key exchange algorithm. You can find the standard in RFC 2412—The OAKLEY Key Determination Protocol.

Object Grouping—Object Grouping is a way to simplify access control by letting you apply access control statements to groups of network objects, such as protocol/services or hosts/networks. *See also* Manage Service Groups and Add/Edit Groups.

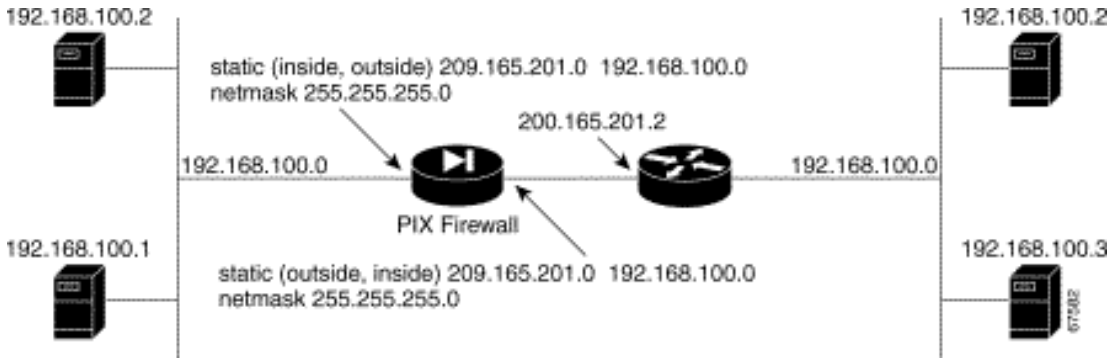
For further information about enabling and using this feature with the CLI, refer to the *Cisco PIX Firewall and VPN Configuration Guide,* "Simplifying Access Control with Object Grouping" section in "Controlling Network Access and Use."

OSPF—Open Shortest Path First. OSPF is a routing protocol widely deployed in large internetworks because of its efficient use of network bandwidth and its rapid convergence after changes in topology.

Outbound—Outbound CLI commands lets you specify whether inside users can create outbound connections. *See also* Static PAT, PAT, and NAT.

Outside—*See* Interface, NAT, Outside NAT, outbound, Static PAT, and PAT.

Outside NAT with Overlap



PAT, Dynamic—Port Address Translation. Dynamic PAT lets multiple outbound sessions appear to originate from

a single IP address. With PAT enabled, the PIX Firewall unit chooses a unique port number from the PAT IP address for each outbound translation slot (xlate). This feature is valuable when an Internet service provider cannot allocate enough unique IP addresses for your outbound connections. The global pool addresses always come first, before a PAT address is used. *See also*, Static PAT, more information about Dynamic NAT, and NAT.

Perfmon—PIX feature which gathers and reports a wide variety of feature statistics, such as connections/second, xlates/second, etc.

PFS—Identifies if Perfect Forwarding Secrecy (PFS) is included in a specific tunnel policy. PFS enhances security by using different security key for the IPSec Phase 1 and Phase 2 SAs. Without PFS, the same security key is used to establish SAs in both phases. PFS ensures that a given IPSec SA's key was not derived from any other secret (like some other keys). In other words, if someone were to breaks a key, PFS ensures that the attacker would not be able to derive any other key. If PFS were not enabled, someone could hypothetically break the IKE SA secret key, copy all the IPSec protected data, and then use knowledge of the IKE SA secret to compromise the IPSec SAs setup by this IKE SA. With PFS, breaking IKE would not give an attacker immediate access to IPSec. The attacker would have to break each IPSec SA individually.

Phase 1, IPSec Phase 1—The first phase of negotiating IPSec, which includes the key exchange, and the ISAKMP portions of IPSec.

Phase 2, IPSec Phase 2—The second phase of negotiating IPSec, where encryption occurs. Phase two determines:

1. What encryption rules will be used for payload
2. What source and destination will be used for encryption
3. What defines interesting traffic, according to access lists
4. The IPSec peer.

Phase two is where IPSec is applied to the interface.

PIM—Protocol Independent Multicast. The Protocol Independent Multicast (PIM) protocol provides a scalable method for determining the best paths in a network for distributing a specific multicast transmission to each host that has registered using IGMP to receive the transmission. With PIM sparse mode (PIM SM), which is the default for Cisco routers, when the source of a multicast transmission begins broadcasting, the traffic is forwarded from one MC router to the next until the packets reach every registered host. *See* IETF RFC 2362 PIM-SM.

Ping—An ICMP request sent between hosts to determine if a host is accessible on the network.

Pool, IP Address Pool, IP Pool—A range of local IP addresses specified by a name, and a range with a starting IP address and an ending address. IP Pools are used by DHCP and VPNs to dynamically assign local IP addresses to clients on the inside interface. *See also* Manage Global Address Pools.

Port, TCP, UDP Port—A field in the packet headers of TCP and UDP protocols which identifies the higher level service which is the source or destination of the packet. You can review "well known" port number assignments and protocol numbers at the following IANA websites:

http://www.iana.org/assignments/port-numbers

http://www.iana.org/assignments/protocol-numbers

Cisco TAC port numbers with RFCs:
http://www-tac.cisco.com/Support_Library/Hardware/PIX/portall.html

PPP—Point-to-Point Protocol. Developed for dial up ISP access using analog phone lines and modems.

PPTP—Point-to-Point Tunneling Protocol. PPTP was introduced by Microsoft to provide secure remote access to Windows networks, using Microsoft Point-to-Point Encryption (MPPE). Because of its vulnerability to attack, PPTP is generally only used where the greater security provided by IPSec authentication and encryption is not available or is not required. PPTP is available with Windows 95 and Windows 98 systems.

PPTP Ports: pptp 1723/tcp ,1723/udp pptp.

See also PAC, PPTP GRE, PPTP GRE Tunnel, PNS, PPTP Session, and PPPTP TCP.

PAC—PPTP Access Concentrator. A device attached to one or more PSTN or ISDN lines capable of PPP operation and of handling the PPTP protocol. The PAC need only implement TCP/IP to pass traffic to one or more PNSs. It may also tunnel non-IP protocols. *See* RFC 2637.

PPTP GRE—Version 1 of GRE (Generic Routing Encapsulation) for encapsulating PPP traffic.

PPTP GRE Tunnel—A tunnel is defined by a PNS-PAC pair. The tunnel protocol is defined by a modified version of GRE. The tunnel carries PPP datagrams between the PAC and the PNS. Many sessions are multiplexed on a single tunnel. A control connection operating over TCP controls the establishment, release, and maintenance of sessions and of the tunnel itself. *See* RFC 2637.

PNS—PPTP Network Server. A PNS is envisioned to operate on general-purpose computing/server platforms. The PNS handles the server side of the PPTP protocol. Since PPTP relies completely on TCP/IP and is independent of the interface hardware, the PNS may use any combination of IP interface hardware including LAN and WAN devices.

PPTP Session—PPTP is connection-oriented. The PNS and PAC maintain state for each user that is attached to a PAC. A session is created when end-to-end PPP connection is attempted between a dial user and the PNS. The datagrams related to a session are sent over the tunnel between the PAC and PNS. *See* RFC 2637.

PPTP TCP—Standard TCP session over which PPTP call control and management information is passed. The control session is logically associated with, but separate from, the sessions being tunneled through a PPTP tunnel. *See* RFC 2637.

PPPoE—Point-to-Point Protocol over Ethernet. An IP protocol which encapsulates PPP packets and sends them over a local network or the internet to establish a connection to a host, usually between a client and an ISP.

Pre-shared key—A pre-shared key provides a method of IKE authentication that is suitable for networks with a limited, static number of IPSec peers. This method is limited in scalability because the key must be configured for each pair of IPSec peers. When a new IPSec peer is added to the network, the pre-shared key must be configured for every IPSec peer with which it communicates. Digital certificates and certificate authorities (CAs) provide a more

scalable method of IKE authentication. *See* Secret key, Public key, and Pre-Shared Keys.

Primary, primary unit—The firewall unit normally operating when two units, a Primary and Secondary, are operating in Failover mode.

Protocol, Protocol Literals—A standard which defines the exchange of packets between network nodes for communication. Protocols work together in layers. Protocols are specified in a Firewall configuration as part of defining a security policy by their literal values or port numbers.

Possible PIX protocol literal values are **`ahp, eigrp, esp, gre, icmp, igmp, igrp, ip,ipinip, ipsec, nos, ospf, pcp, snp, tcp, and udp.`**

Proxy-ARP—This feature enables the PIX Firewall to reply to an ARP request for IP addresses in the global pool. *See also* ARP.

Public key—A public key is one of a pair of keys, called RSA keys, which are generated by each IPSec peer. A public key has the characteristic that data encrypted with it can only be decrypted using the associated private key. This characteristic of public/private key pairs provides a secure method of authentication over an insecure media, such as the public Internet. When a private key is used in a digital signature, the receiver can use the sender's public key to verify that the message was encrypted by the sender's private key. Digital certificates are used to distribute public keys and to provide a secure method of associating a public key with a specific entity.

Q-T

RADIUS—Remote Authentication Dial-In User Service. *See also* AAA and TACACS+.

Refresh—

Replay-detection—A security service where the receiver can reject old or duplicate packets in order to defeat replay attacks (replay attacks rely on the attacker sending out older or duplicate packets to the receiver and the receiver thinking that the bogus traffic is legitimate). Replay-detection is done by using sequence numbers combined with authentication, and is a standard feature of IPSec.

RFC—Request for comment. RFC documents define Protocols and standards for communications over the internet. RFCs are developed and published by The Internet Engineering Task Force (IETF).

Route—The path through an internetwork.

RLLA—Reserved Local Link Addresses. *See also* Multicast.

RPC—remote procedure call. RPCs are procedure calls that are built or specified by clients and executed on servers, with the results returned over the network to the clients. *See also* client/server computing.

Caution: RPC is not a very secure protocol and should be used with caution.

RPF—Reverse Path Forwarding.

RSA—A public key cryptographic algorithm (named after its inventors, Rivest, Shamir and Adelman) with a variable key length. RSA's main weakness is that it is significantly slow to compute compared to popular secret-key algorithms, such as DES. Cisco's IKE implementation uses a Diffie-Hellman exchange to get the secret keys. This exchange can be authenticated with RSA (or pre-shared keys). With the Diffie-Hellman exchange, the DES key never crosses the network (not even in encrypted form), which is not the case with the RSA encrypt and sign technique. RSA is not public domain, and must be licensed from RSA Data Security. *See also* public key and encryptionVPN>IKE.

RSH—Remote Shell Protocol. A protocol that allows a user to execute commands on a remote system without having to log in to the system. For example, **RSH** can be used to remotely examine the status of a number of access servers without connecting to each communication server, executing the command, and then disconnecting from the communication server.

RTSP—Real Time Streaming Protocol. Enables the controlled delivery of real-time data, such as audio and video. RTSP is designed to work with established protocols, such as Routing Table Protocol (**RTP**) and HTTP.

Rule—Information added to the configuration to define your security policy in the form of conditional statements that instruct the firewall how to react to a particular situation. *See also*, address translation and access control rules.

Running Configuration—The configuration currently running in RAM on the firewall unit which determines its operational characteristics.

SA—An instance of security policy and keying material applied to a data flow. Security associations (SAs) are established in pairs by IPSec peers during both phases of IPSec. SAs specify the encryption algorithms and other security parameters used to create a secure tunnel. Phase 1 SAs (IKE SAs) establish a secure tunnel for negotiating Phase 2 SAs. Phase 2 SAs (IPSec SAs) establish the secure tunnel used for sending user data.

Both IKE and IPSec use SAs, although SAs are independent of one another. IPSec SAs are *unidirectional* and they are unique in each security protocol. A set of SAs are needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports ESP between peers, one ESP SA is required for each direction. SAs are uniquely identified by destination (IPSec endpoint) address, security protocol (AH or ESP), and security parameter index (SPI).

IKE negotiates and establishes SAs on behalf of IPSec. A user can also establish IPSec SAs manually.

An IKE SA is used by IKE only, and unlike the IPSec SA, it is *bi-directional*.

See also IPSec, IKE, Site-to-Site VPN, and ESP.

Secret key— A secret key is shared only between the sender and receiver. *See* Public key and Pre-shared key.

Security Services—*See* cryptographic services.

Serial transmission—A method of data transmission in which the bits of a data character are transmitted sequentially over a single channel.

SHA-1— SHA is closely modeled after MD4 and produces a 160-bit digest. Because SHA produces a 160-bit digest, it is more resistant to brute-force attacks than 128-bit hashes (such as MD5), but it is slower. Secure Hash Algorithm 1 is a joint creation of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). This algorithm, like other hash algorithms, is used to generate a hash value, also known as a message digest, which acts like the cyclic redundancy check (CRC) used in lower-Layer Protocols to ensure that message contents are not changed during transmission. SHA-1 is generally considered more secure than MD5. It produces a 160-bit message digest for which no known attacks or partial attacks have yet been demonstrated. *See also* encryption and VPN.

SIP—Session Initiation Protocol. Enables call handling sessions, particularly two-party audio conferences, or "calls." SIP works with Session Description Protocol (SDP) for call signaling. SDP specifies the ports for the media stream. Using SIP, the PIX Firewall can support any SIP Voice over IP (VoIP) gateways and VoIP proxy servers. *See also* Fixup.

Site-to-site VPN—A site-to-site VPN is established between two IPSec peers that connect remove networks into a single virtual private network. In this type of VPN, neither IPSec peer is the destination or source of user traffic. Instead, each IPSec peer provides encryption and authentication services for hosts on the local area networks (LANs) connected to each IPSec peer. The hosts on each LAN send and receive data through the secure tunnel established by the pair of IPSec peers. *See also* VPN, IPSec, IKE, and ESP.

Skeme—A key exchange protocol that defines how to derive authenticated keying material, with rapid key refreshment.

SMR—Stub Multicast Routing.

SMTP—Simple Mail Transfer Protocol. Internet protocol providing e-mail services. *See also* Fixup.

SNMP—Simple Network Management Protocol. A standard method for managing network devices using data structures called management information bases (MIBs). *See also* SNMP.

Split Tunneling, VPN Split Tunnel—Split tunneling allows a remote VPN client simultaneous encrypted access to a private network and clear unencrypted access to the Internet. If you do not enable split tunneling, all traffic between the VPN client and the PIX Firewall is sent through an IPSec tunnel. All traffic originating from the VPN client is sent to the PIX Firewall's outside interface through a tunnel, and the client's access to the Internet from its remote site is denied. *See also* VPN, Tunneling, Encryption, IKE, Site-to-Site VPN, SA, and ESP.

Spoofing—The act of a packet illegally claiming to be from an address from which it was not actually sent. Spoofing is designed to foil network security mechanisms such as filters and access lists.

SQL*Net—Structured Query Language Protocol. An Oracle protocol used to communicate between client and server processes. *See also* Fixup.

SSH—Secure Shell) is an application running on top of a reliable transport layer, such as TCP/IP, that provides strong authentication and encryption capabilities. Up to five SSH clients are allowed simultaneous access to the PIX Firewall console. *See also* Fixup.

Note: You must generate an RSA key-pair for the PIX Firewall before clients can connect to the PIX Firewall console. To use SSH, your firewall must have a Data Encryption Standard (DES) or 3DES (Triple DES) activation key.

SSL—Secure Sockets Layer. A protocol which resides between the application layer and TCP/IP to provide transparent encryption of data traffic.

Standby, standby unit, secondary unit—The backup firewall unit when two are operating in Failover mode.

State, Stateful, Stateful Inspection—Network protocols maintain certain data, called state information, at each end of a network connection between two hosts. State information is necessary to implement the features of a protocol, such as guaranteed packet delivery, data sequencing, flow control, and transaction or session IDs. Some of the protocol state information is sent in each packet while each protocol is being used. For example, a web browser connected to a web server uses HTTP and supporting TCP/IP protocols. Each protocol layer maintains state information in the packets it sends and receives. PIX and some other firewalls inspect the state information in each packet to verify that it is current and valid for every protocol it contains. This is called stateful inspection and is designed to create a powerful barrier to certain types of computer security threats.

Static PAT—Static Port Address Translation. A static address maps a local IP address to a global IP address. Static PAT is a static address that also maps a local port to a global port. *See also* dynamic PAT.

Telnet—A terminal emulation protocol for TCP/IP networks such as the Internet. Telnet is a common way to control web servers remotely.

Subnetmask, Netmask—*See* Mask.

TACACS+—Terminal Access Controller Access Control System Plus. Provides remote access authentication and related services, such as event logging. User passwords are administered in a central database rather than in individual network devices, providing an easily scalable network security solution. *See also* AAA and RADIUS.

TCP,TCP/IP—Transmission Control Protocol, Internet Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. *See also* IP and IP address.

TCP Intercept—With the TCP intercept feature, once the optional embryonic connection limit is reached, and until the embryonic connection count falls below this threshold, every SYN bound for the affected server is intercepted.

For each SYN, PIX Firewall responds on behalf of the server with an empty SYN/ACK segment. PIX Firewall retains pertinent state information, drops the packet, and waits for the client's acknowledgment. If the ACK is received, then a copy of the client's SYN segment is sent to the server and the TCP three-way handshake is performed between PIX Firewall and the server. If and only if, this three-way handshake completes, may the connection resume as normal. If the client does not respond during any part of the connection phase, then PIX Firewall retransmits the necessary segment using exponential back-offs.

TFTP—Trivial File Transfer Protocol. TFTP is a simple protocol used to transfer files. It runs on UDP and is explained in depth in Request For Comments (RFC) 1350. See also Fixup.

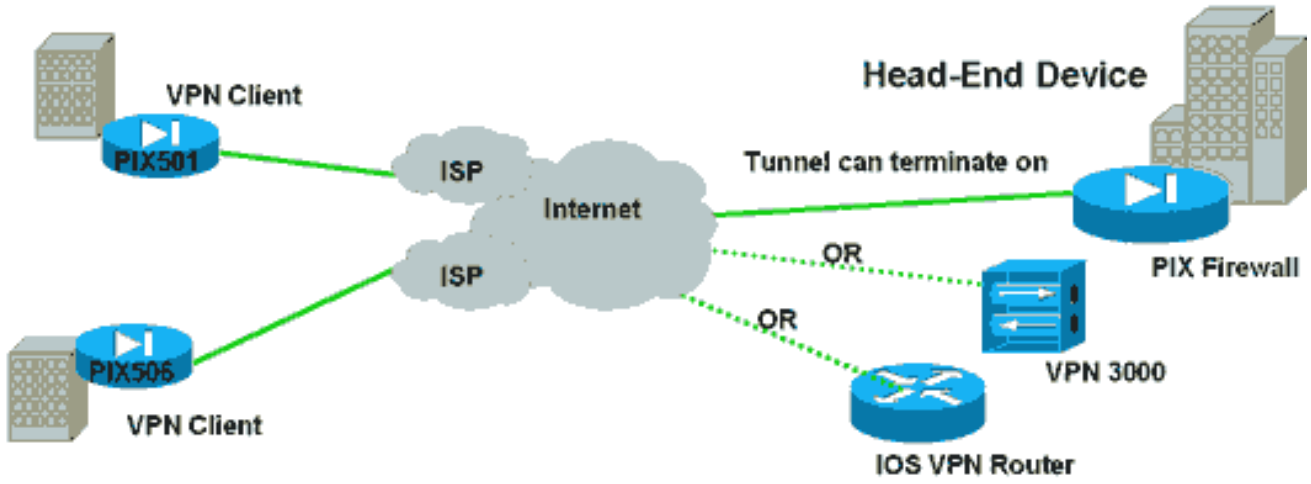
Transform, IPSec Transform Set—A transform set specifies the IPSec protocol, encryption algorithm, and hash algorithm to use on traffic matching the IPSec policy. A transform describes a security protocol (AH or ESP) with its corresponding algorithms. The IPSec protocol used in almost all transform sets is the Encapsulated Security Protocol (ESP) with the DES cipher algorithm and HMAC-SHA for authentication.

Translate, Translation, Address Translation—*See* Xlate.

Transport Mode—An encapsulation mode for AH/ESP. Transport Mode encapsulates the upper layer payload (such as Transmission Control Protocol (TCP) or User Datagram Protocol (UDP)) of the original IP datagram. This mode can only be used when the peers are the endpoints of the communication. The contrast of Transport Mode is Tunnel Mode.

Tunnel Mode—Encapsulation of the complete IP Datagram for IPSec. Tunnel Mode is used to protect datagrams sourced from or destined to non-IPSec systems (such as in a Virtual Private Network (VPN) scenario).

Tunnel, Tunneling—A tunnel is a method of transporting data in one protocol by encapsulating it in another protocol, usually for compatibility, implementation simplification, or security reasons. Tunneling allows a remote VPN client encrypted access to a private network through the Internet. *See also* Transform Set, Tunnel Mode, Split Tunneling, and Tunnel Policy.



U-Z

UDP—User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol that belongs to the Internet protocol family.

URL—Universal Resource Locator. A standardized addressing scheme for accessing hypertext documents and other services using a browser, for example, http://www.cisco.com/go/pix.

UTC—UTC (Coordinated Universal Time) replaced **GMT** (Greenwich Mean Time) in 1967 as the world time standard. It is based on an atomic time scale rather than an astronomical time scale. However, if the PIX CLI command **`clock timezone`** and **`clock summer-time`** commands have been used to set the correct local time zone, then the clock can be set to the local time, rather than UTC.

VPN—Virtual Private Network. A network connection between two **peers** over the public network which is made private by strict authentication of users and the encryption of all data traffic. VPNs can be established between clients, such as PCs, and a headend, such as PIX Firewall. *See also* IPSec, IKE, VPN>IKE Policies, Tunnel, Site-to-Site VPN, SA, ESP, PPP, L2TP, and PPTP. *See also* VPN Topics, VPN Wizard Topics, VPN Terms, VPN, and VPN Example Configurations.

Websense—A third party filtering application that works with the PIX Firewall to deny users access to web sites based on the company security policy. Websense enables group and username authentication between a host and a PIX Firewall. The PIX Firewall performs a username lookup, and then the Websense server handles URL filtering and username logging.

WINS—Windows Internet Naming Service. A Windows system that determines the IP address associated with a particular network computer.

X.509, **ITU X.509**—Digital certificate standard by the (ITU). *See* ITU X.509

Xauth—*See* IKE Extended Authentication**.**

Xlate—An xlate, also referred to as a translation entry, represents a mapping of one IP address to another, or a mapping of one IP address/port pair to another. *See also* NAT, PAT, Address Translation, and IP Address.

Acronyms and Abbreviations

For more information on acronyms used in PDM Help and PIX Firewall documentation, *see Internetworking Terms and Acronyms*.

ACRONYM	DESCRIPTION

AAA	authentication, authorization, and accounting.
ACE	Access Control Entry
ACL	access control list
AH	Authentication Header.
ARP	Address Resolution Protocol—A low-level TCP/IP protocol that maps a node's hardware address (called a "MAC" address) to its IP address. Defined in RFC 826. An example hardware address is 00:00:a6:00:01:ba. (The first three groups specify the manufacturer, the rest identify the host's motherboard.)
BGP	Border Gateway Protocol—While PIX Firewall does not support use of this protocol, you can set the routers on either side of the PIX Firewall to use RIP between them and then run BGP on the rest of the network before the routers.
BOOTP	Bootstrap Protocol—Lets diskless workstations boot over the network and is described in RFC 951 and RFC 1542.
CA	certification authority.
CHAP	Challenge Handshake Authentication Protocol. Security feature supported on lines using PPP encapsulation that prevents unauthorized access.
CPP	Combinet Proprietary Protocol.
chargen	Character Generation—Via TCP, a service that sends a continual stream of characters until stopped by the client. Via UDP, the server sends a random number of characters each time the client sends a datagram. Defined in RFC 864.
conn	Connection slot in PIX Firewall—Refer to the **xlate** command page for more information.
CPU	Central Processing Unit.
CRL	certificate revocation list.
DES	Data Encryption Standard.
DHCP	Dynamic Host Configuration Protocol.

DNS	Domain Name System—Operates over UDP unless zone file access over TCP is required.
DoS	Denial of Service.
EEPROM	Electrically Erasable Programmable Read-Only Memory.
EGP	Exterior Gateway Protocol—While PIX Firewall does not support use of this protocol, you can set the routers on either side of the PIX Firewall to use RIP between them and then run EGP on the rest of the network before the routers.
EIGRP	Enhanced Interior Gateway Routing Protocol—While PIX Firewall does not support use of this protocol, you can set the routers on either side of the PIX Firewall to use RIP between them and then run EIGRP on the rest of the network before the routers.
ESP	Encapsulating Security Protocol. Refer to RFC 1827 for more information.
FDDI	Fiber Distributed Data Interface—Fiber optic interface.
FTP	File Transfer Protocol.
gaddr	Global address—An address set with the **global** and **static** commands.
GRE	Generic Routing Encapsulation protocol—Commonly used with Microsoft's implementation of PPTP.
HSRP	Hot-Standby Routing Protocol.
HTTP	Hypertext Transfer Protocol—The service that handles access to the World Wide Web.
https	Secure Hypertext Transfer Protocol.
IANA	Internet Assigned Number Authority—Assigns all port and protocol numbers for use on the Internet. You can view port numbers at the following site: http://www.iana.org/assignments/port-numbers You can view protocol numbers at the following site: http://www.iana.org/assignments/protocol-numbers

ICMP	Internet Control Message Protocol—This protocol is commonly used with the **ping** command. You can view ICMP traces through the PIX Firewall with the **debug trace on** command. Refer to RFC 792 for more information.
IFP	Internet Filtering Protocol.
IGMP	Internet Group Management Protocol.
IGRP	Interior Gateway Routing Protocol.
IKE	Internet Key Exchange.
IKMP	Internet Key Management Protocol.
ISAKMP	Internet Security Association and Key Management Protocol.
IP	Internet Protocol.
IPCP	IP Control Protocol. Protocol that establishes and configures IP over PPP.
IPinIP	IP-in-IP encapsulation protocol.
IPSec	IP Security Protocol efforts in the IETF (Internet Engineering Task Force).
IRC	Internet Relay Chat protocol—The protocol that lets users access chat rooms.
KDC	Key Distribution Center.
L2TP	Layer Two Tunneling Protocol
laddr	Local address—The address of a host on a protected interface.
MD5	Message Digest 5—An encryption standard for encrypting VPN packets. This same encryption is used with the **aaa authentication console** command to encrypt Telnet sessions to the console.
MIB	Management Information Base—Used with SNMP.
MPPE	Microsoft Point-To-Point Encryption.

MS-CHAP	Microsoft CHAP (Challenge Handshake Authentication Protocol). *See* "CHAP" for more information.
MSRPC	Microsoft Remote Procedure Call.
MTU	maximum transmission unit—The maximum number of bytes in a packet that can flow efficiently across the network with best response time. For Ethernet, the default MTU is 1500 bytes, but each network can have different values, with serial connections having the smallest values. The MTU is described in RFC 1191.
NAT	Network Address Translation.
NetBIOS	Network Basic Input Output System—An application programming interface (API) that provides special functions for PCs in local-area networks (LANs).
NIC	Network Information Center.
NNTP	Network News Transfer Protocol—News reader service.
NOS	Network Operating System.
NTP	Network Time Protocol—Set system clocks via the network.
NVT	Network virtual terminal.
OSPF	Open Shortest Path First protocol.
PAP	Password Authentication Protocol. Authentication protocol that lets PPP peers authenticate one another.
PAT	Port Address Translation.
PDM	PIX Device Manager.
PFS	perfect forward secrecy.
PFSS	PIX Firewall Syslog Server.
PIX	Private Internet Exchange.
PKI	Public Key Infrastructure.

POP	Post Office Protocol.
PPPoE	Point-to-Point Protocol over Ethernet.
PPP	Point-to-Point Protocol. Provides PIX Firewall-to-router and host-to-network connections over synchronous and asynchronous circuits.
PPTP	Point-to-Point Tunneling Protocol. RFC 2637 describes the PPTP protocol.
RA	registration authority.
RADIUS	Remote Authentication Dial-In User Service—User authentication server specified with the **aaa-server** command.
RAS	The registration, admission, and status protocol. Provided with H.323 support.
RC4	RC4 is stream cipher designed by Rivest for RSA Data Security, Inc. It is a variable key-size stream cipher with byte-oriented operations. The algorithm is based on the use of a random permutation.
RFC	Request For Comment—RFCs are the de facto standards of networking protocols.
RIP	Routing Information Protocol.
RPC	Remote Procedure Call.
RSA	Rivest, Shamir, and Adelman. RSA is the trade name for RSA Data Security, Inc.
RTP	Real-Time Transport Protocol.
RTCP	RTP Control Protocol.
RTSP	Real Time Streaming Protocol.
SA	security association.
SCCP	Simple (Skinny) Client Control Protocol
SDP	Session Description Protocol.

SIP	Session Initiation Protocol.
SSH	Secure Shell.
SMR	Stub Multicast Routing.
SMTP	Simple Mail Transfer Protocol—Mail service. The **fixup protocol smtp** command enables the Mail Guard feature. The PIX Firewall Mail Guard feature is compliant with both the RFC 1651 EHLO and RFC 821 section 4.5.1 commands.
SNMP	Simple Network Management Protocol—Set attributes with the **snmp-server** command.
SPC	Shared Profile Component.
SPI	Security Parameter Index—A number which, together with a destination IP address and security protocol, uniquely identifies a particular security association.
SQL*Net	SQL*Net is a protocol Oracle uses to communicate between client and server processes. (SQL stands for Structured Query Language.) The protocol consists of different packet types that firewall handles to make the data stream appear consistent to the Oracle applications on either side of the firewall. SQL*Net is enabled with the **fixup protocol sqlnet** command, which is provided in the default configuration.
SYN	Synchronize sequence numbers flag in the TCP header.
TACACS+	Terminal Access Controller Access Control System Plus.
TCP	Transmission Control Protocol. Refer to RFC 793 for more information.
TurboACL	Turbo Access Control List—A feature introduced with PIX Firewall version 6.2 that improves the performance of large ACLs.
TFTP	Trivial File Transfer Protocol.
Triple DES	Triple Data Encryption Standard. Also known as 3DES.
uauth	User authentication.
UDP	User Datagram Protocol.
URL	Universal Resource Locator.

UUIE	user-user information element.
VPDN	virtual private dial-up network.
VPN	Virtual Private Network . More
WWW	World Wide Web.
Xauth	extended authentication.
XDMCP	X Display Manager Control Protocol.
xlate	Translation slot in PIX Firewall.

Copyright © 2001-2004, Cisco Systems, Inc.

A-D

AAA
Auth, XAUTH
AAA Authentication, RADIUS, TACACS+
AAA Rules
AAA Server Groups
AAA Servers
About PDM
Access Rules
ACL
Address, IP
Administration
Admin Modes
Antispoof
Applications supported by PIX Firewall.
Apply, Applying Config Changes
Authentication, See also Password
Authorization
Auto Update

Banner
Best Practices, Network Security PolicyWhite Paper
Bookmarks, Graph

CLI Tool
CLI Commands Used by PDM Screens
Clock, NTP, Status Bar
Command Reference
Configuration Changes in PDM
Console Sessions, Secure Shell Sessions, Telnet Console Sessions, PDM Users
Contents

Default Route, Wizard, See also Route
DHCP Admin, Monitor DHCP Clients
DHCP Options 156 and 66

M-P

Mail, SMTP Fixup
Mask, Netmask
Menu
Miscellaneous Help, General Topics
Monitor, **Monitoring**, Monitoring Graphs

More (Advanced Topics, Reference)

- More>Configuration Changes in PDM
- More>Internet Protocol (IP)
- More>NAT Dynamic
- More>NAT Static
- More>Password Policy
- More>Sample Configurations
- More>TAC Resources for PIX Firewall
- More>VPN

MRoute, IGMP MRoute
Multicast

NAT, dynamic NAT , static NAT
Navigation Contents, Getting Started, Glossary, About
Netmask, Mask
NTP, Clock

Options, Preferences, Unparsed Commands

Password Admin
PDM, About PDM
PDM Icon Legend
PDM Logging, View PDM Log, Monitor PDM Users
Ping Tool
Policy, IDS
Policy, Security
Ports
PPPoE, Monitoring PPPoE Client

DHCP Relay
DES, 3DES
DNS fixup

E-H

Encryption, VPN Terms, IPSec, IKE, DES,

Failover, primary unit, standby unit, LAN-based
File Menu
Filter Rules
Fixups, Fixups List
Fragment
FTP Fixup

Glossary
GMT
Graphs
Group, Service Group, Network Group

H323 Fixup
History Metrics
Home
Hosts/Networks
HTTP Fixup
HTTPS, PDM,
HTTPS, Monitoring>Connection Graphs>HTTPS

I-L

ICMP Admin
IDS Policy, IDS Signatures, IDS Monitor
IGMP
IKE
Interfaces Admin
IPSec, VPN>IPSec Rules
IPSec Tunnel Mode
Preferences, Options
Pre-shared key
primary unit, Failover, standby unit
Print
Privileges, Status Bar
Protocol
Protocols supported by PIX Firewall.
ProxyARPs Admin
Public key

Q-T

RADIUS, TACACS+
Refresh
RFCs, Requests for Comments
RIP Admin
Route, Routing, Static Route, RIP, Proxy ARPs, Hosts/Networks NAT, Routing
RSH Fixup
RTSP Fixup
Rule

Search Field (Access Rules or Translation Rules),
Search Hosts/Networks
Service Groups, Manage Service Groups
Signatures, IDS
SIP Fixup
Site-to-Site VPN
SKINNY Fixup
SMTP Fixup
SNMP Administration, SNMP Fixup
Split Tunneling
Spoof, Antispoof
SQL*Net FixUP
SSH (Secure Shell) Administration, Monitor Secure Shell Sessions
Start (Getting Started)
Startup Wizard
Static Routes, Wizard
Status Bar
Syslog Logging
System Properties

IPSec Transport Mode.
ILS
IP
IP Address
Icon Legend

LAN-based Failover
Licenses, User Licenses
Location of Help Topics
Log, Logging, Admin, Setup, PDM, Syslog, Other,
Log, Logging, Monitor PDM Log, View PDM Log

Tabs
TACACS+, RADIUS
TCP
Technical Assistance
Telnet Admin, Telnet Console Sessions
TFTP Server Admin, Write TFTP Server, TFTP fixup
Time, Status Bar
Timeout, System Properties
Topics, Help Topics, Topics by Location
Translation Rules
Translation Rules, Edit Translation Rules
Troubleshooting, Tools>Ping,
Tunnel, Split Tunneling, IPSec Tunnel Mode
Tutorial, TAC Examples, PIX Configuration Examples
More... Tutorials, Reference

U-Z

UDP
Unparsed Configuration Commands
Unsupported Configuration Commands
URL Filtering, System Properties
User Accounts, Status Bar
User Licenses
UTC

VPN, Site-to-Site VPN
VPN Tab
VPN Terms
VPN Wizard
VPN, More VPN

Web Server
Wizard, Startup, VPN
Write TFTP Server

XAUTH Auth, AAA

Copyright © 2001-2004, Cisco Systems, Inc.

Cisco PIX® Device Manager 3.0
Online Help

GETTING STARTED

About PDM

Contents

Getting Started

Glossary

Home

Index

Obtaining Technical Assistance

PIX Documentation

Catalyst 6000 Documentation

GENERAL TOPICS

Applying Configuration Changes

Applications Support

Certificates

CLI Commands Used by PDM Screens

Configuration - Access Rules | Translation Rules | Hosts/Networks | VPN | Systems Properties

Graphs

Icon Legend

IP Protocols

IPSec

Main Tool Bar - Home | Configuration | Monitoring | Refresh | Save | Help

Manage Global Address Pools

Monitoring - Introduction

More (Tutorials, Advanced Topics, Reference)

Printing

Refresh

Save

Status Bar

Technical Assistance

Unparsed Commands

Unsupported Commands

VPN - VPN Tab | VPN Wizard | VPN Monitoring | VPN Terms | VPN (Glossary) | More>VPN

Wizards - Startup Wizard | VPN Wizard

MENUS

FILE

File Menu

File>Reset Firewall to Factory Default Configuration

File>Save Running Configuration to TFTP Server

File>Print

OPTIONS

Options>Preferences

SEARCH

Search>Search by Field

Search>Search by Host/Network

TOOLS

Tools>CLI (Command Line Interface)

Tools>Ping

Tools>Manage Service Groups

More (Tutorials, Advanced Topics, Reference)

- More>Configuration Changes in PDM
- More>Internet Protocol (IP)
- More>NAT Dynamic
- More>NAT Static
- More>Password Policy
- More>Sample Configurations
- More>TAC Resources for PIX Firewall
- More>VPN

MAIN TABS

ACCESS RULES

Access Rules

Access Rules>Add, Edit, Insert or Paste Rule

AAA Rules

AAA Rules>Advanced

AAA Rules>Add, Edit, Insert or Paste Rule

Filter Rules

Filter Rules>Add, Edit, Insert or Paste Rule

Log Options

HOSTS/NETWORKS

Hosts/Networks (Main)

Host/Networks>Edit>NAT

Host/Network>NAT (Network Address Translation)

Hosts/Networks>Add>Basic Information

Hosts/Networks>Add>Manage Global Address Pools

Hosts/Networks>Add>Static NAT Options

Hosts/Networks>Add>Static Route

Hosts/Networks>Edit>Basic Information

Hosts/Networks>Edit>Static Route

Hosts/Networks>Groups>Add

MONITORING

Monitoring>Build Graph Window (Intro)

Monitoring>Connection Graphs

Monitoring>DHCP Client Lease Information

Monitoring>Graph Window

Monitoring>Interface Graphs

Monitoring>Miscellaneous>Intrusion Detection System

PDM

Monitoring>PDM Log Viewer

Monitoring>PDM Log

Monitoring>PDM Users

Monitoring>PPPoE Client Information

Monitoring>Secure Shell Sessions

Monitoring>System Graphs

Monitoring>Telnet Sessions

Monitoring>User Licenses

VPN

Monitoring>VPN Connection Graphs>IPSec Tunnels or L2TP/PPTP>New Graph

Monitoring>VPN Connection Graphs>IPSec Tunnels

Monitoring>VPN Connection Graphs>L2TP/PPTP

Monitoring>VPN Statistics>IKE SAs

Monitoring>VPN Statistics>IPSec VPNs

Monitoring>VPN Statistics>L2TP

Monitoring>VPN Statistics>PPTP

STARTUP WIZARD

Startup Wizard>Welcome

Startup Wizard>Auto Update Configuration

Startup Wizard>Basic Configuration

Startup Wizard>DHCP Server Configuration

Startup Wizard>NAT and PAT Configuration

Startup Wizard>Other Interfaces Configuration

Startup Wizard>Outside Interface Configuration

Startup Wizard>PPPoE Configuration

Startup Wizard>Starting Configuration

Startup Wizard>Startup Wizard Completed

Startup Wizard>Easy VPN Remote Configuration

SYSTEM PROPERTIES	AAA | Admin | Advanced | DHCP | Fixup | IDS | Interfaces | Logging
	Multicast | Routing

System Properties>Auto Update

System Properties>Failover

System Properties>History Metrics

System Properties>URL Filtering

AAA

System Properties>AAA>AAA Server Groups

System Properties>AAA>AAA Servers

System Properties>AAA>Authentication Prompt

Administration

System Properties>Administration>Authentication/Authorization

System Properties>Administration>Banner

System Properties>Administration>Clock

System Properties>Administration>Console

System Properties>Administration>Device

System Properties>Administration>ICMP

System Properties>Administration>Mgmt. Access

System Properties>Administration>NTP

System Properties>Administration>Password

System Properties>Administration>PDM/HTTPS

System Properties>Administration>Secure Shell

System Properties>Administration>SNMP

System Properties>Administration>Telnet

System Properties>Administration>TFTP Server

System Properties>Administration>User Accounts

Advanced

System Properties>Advanced>Anti-Spoofing

System Properties>Advanced>Fragment

System Properties>Advanced>TCP Options

System Properties>Advanced>Timeout

System Properties>Advanced>Turbo Access Rules

Advanced>Fixup

System Properties>Advanced>Fixup

System Properties>Advanced>Fixup>CTIQBE

System Properties>Advanced>Fixup>ESP-IKE

System Properties>Advanced>Fixup>FTP

System Properties>Advanced>Fixup>H.323

System Properties>Advanced>Fixup>H.323 RAS

System Properties>Advanced>Fixup>HTTP

System Properties>Advanced>Fixup>ICMP Error

System Properties>Advanced>Fixup>ILS

System Properties>Advanced>Fixup>MGCP

System Properties>Advanced>Fixup>Configure MGCP

System Properties>Advanced>Fixup>MGCP>Configure MGCP>Add MCGP Group

System Properties>Advanced>Fixup>MGCP>Configure MGCP>Edit MCGP Group

System Properties>Advanced>Fixup>PPTP

System Properties>Advanced>Fixup>RSH

System Properties>Advanced>Fixup>RTSP

System Properties>Advanced>Fixup>SIP

System Properties>Advanced>Fixup>Skinny

System Properties>Advanced>Fixup>SMTP

System Properties>Advanced>Fixup>SNMP

System Properties>Advanced>Fixup>SQL*Net

System Properties>Advanced>Fixup>TFTP

DHCP Services

System Properties>DHCP Relay

System Properties>DHCP Server

IDS

System Properties>IDS>IDS Policy

System Properties>IDS>IDS Signatures

Interfaces

System Properties>Interfaces

Logging

System Properties>Logging>Logging Setup

System Properties>Logging>Logging Setup Edit

System Properties>Logging>Other

System Properties>Logging>PDM Logging

System Properties>Logging>Rate Limit

System Properties>Logging>Rate Limit>Add/Edit

System Properties>Logging>Syslog

System Properties>Logging>Syslog>Advanced

Multicast

System Properties>Multicast

System Properties>Multicast>IGMP>Access Group

System Properties>Multicast>IGMP>Access Group>Edit

System Properties>Multicast>IGMP>Join Group

System Properties>Multicast>IGMP>Join Group>Add

System Properties>Multicast>IGMP>MRoute

System Properties>Multicast>IGMP>MRoute>Add/Edit

System Properties>Multicast>IGMP>Protocol

System Properties>Multicast>IGMP>Protocol>Edit

System Properties>Multicast>Stub Multicast Routing

System Properties>Multicast>Stub Multicast Routing>Edit

Routing

System Properties>Routing>RIP

System Properties>Routing>Static Route

System Properties>Routing>Proxy ARPs

System Properties>Routing>OSPF>Filtering

System Properties>Routing>OSPF>Filtering>Add or Edit OSPF Filtering Entry

System Properties>Routing>OSPF>Interface

System Properties>Routing>OSPF>Interface>Edit OSPF Interface Authentication

System Properties>Routing>OSPF>Setup>Edit OSPF Interface Advanced Properties

System Properties>Routing>OSPF>Interface>Edit OSPF Interface Properties

System Properties>Routing>OSPF>Redistribution

System Properties>Routing>OSPF>Redistribution>Add or Edit Redistribution Entry

System Properties>Routing>OSPF>Setup

System Properties>Routing>OSPF>Setup>Area/Networks>Add an Area

System Properties>Routing>OSPF>Setup>Process Instances>Edit OSPF Process Advanced Properties

System Properties>Routing>OSPF>Setup>Route Summarization>Add a Route Summarization Entry

System Properties>Routing>OSPF>Summary Address

System Properties>Routing>OSPF>Summary Address>Add or Edit OSPF Summary Address Entry

System Properties>Routing>OSPF>Virtual Links

System Properties>Routing>OSPF>Virtual Links>Add or Edit a Virtual Link

System Properties>Routing>OSPF>Virtual Links>Add or Edit a Virtual Link>
Edit Virtual Link Advanced Properties

TRANSLATION RULES

Translation Rules

Translation Rules>Add/Edit Address Translation Rules

Translation Rules>Translation Exemption Rule

VPN WIZARD

VPN Wizard>Add AAA Server

VPN Wizard>Attributes Pushed to Client (Optional)

VPN Wizard>Extended Client Authentication

VPN Wizard>IPSec Traffic Selector (continued)

VPN Wizard>IPSec Traffic Selector

VPN Wizard>L2TP and IPSec

VPN Wizard>Local Username Password Database

VPN Wizard>MPPE Encryption

VPN Wizard>PPTP Authentication

VPN Wizard>Remote Access Client

VPN Wizard>Remote Access Client>Address Pool

VPN Wizard>Remote Access Client>VPN Client Group

VPN Wizard>Remote Access Client>Address Translation Exemption (Optional)

VPN Wizard>Site to Site VPN>IKE Policy

VPN Wizard>Site to Site VPN>Remote Site Peer

VPN Wizard>Transform Set

VPN Wizard>VPN Wizard Start

VPN **More**

Certificates

VPN>Certificate>Authorization

VPN>Certificate>Configuration

VPN>Certificate>Configuration>Advanced

VPN>Certificate>Configuration>Advanced>Peer Certificate

VPN>Certificate>Configuration>Advanced>Peer FQDN/IP

VPN>Certificate>Enrollment

VPN>Certificate>Enrollment>X500

IKE

VPN>IKE>Policies

VPN>IKE>Policies>Add/Edit IKE Rule

VPN>IKE>Pre-Shared Keys

VPN>IKE>PRE-Shared Keys>Add ISAKMP Key

VPN>IKE>XAuth/Mode Config>Edit

VPN>IKE>XAuth/Mode Configuration

IPSec

VPN>IPSec>IPSec Rules

VPN>IPSec>IPSec Rules>Add Rule

VPN>IPSec>IPSec Rules>Add Rule>Manage Service Groups

VPN>IPSec>IPSec Rules>Add Rule>Manage Service Groups>Add Service

VPN>IPSec>Transform Sets

VPN>IPSec>Transform Sets>Add Transform Set

VPN>IPSec>Tunnel Policy

VPN>IPSec>Tunnel Policy>Add

VPN>IPSec>Tunnel Policy>Add>Advanced

VPN >IPSec>Tunnel Policy>Advanced>Select Transform Set

Remote Access

VPN>Remote Access>IP Pools

VPN>Remote Access>VPN Client

VPN>Remote Access>VPN Client>Add or Edit Client Group

VPN>Remote Access>Add Cisco VPN Client Settings>Advanced Options

VPN>Remote Access>L2PT/PPTP Client

VPN>Remote Access>Add/Edit Windows Client Settings

VPN>VPN Hardware Client

VPN>VPN System Options

Copyright © 2001-2004, Cisco Systems, Inc.

Cisco PIX® Device Manager 3.0
Online Help

Cisco PIX Device Manager (PDM) is a browser-based configuration tool that enables you to graphically set up, configure, and monitor your Cisco PIX Firewall running Version 6.3(4). PDM Version 3.0(4) is a single image. PDM is implemented as a signed Java applet which uploads to your PC or workstation when you point your browser at the firewall without requiring a plug-in or other software to be installed beforehand.

PDM simplifies administration by letting you configure all of your Cisco firewall units using visual tools, such as tables, drop-down menus, and task-oriented selections, directly from your standard desktop web browser. However, PDM also maintains compatibility with the PIX Firewall command-line interface (CLI) and includes a tool for using the standard CLI commands with the convenience of a browser connection. In addition, PDM enables you to monitor connections, traffic and other activity over time with graphs which can also be printed.

For more information about PDM, see the PDM Data Sheet.

For a list of applications and protocols supported by firewalls managed by PDM, see More ▸ IP and More ▸ VPN.

For more information about Cisco PIX Firewall products, see
http://www.cisco.com/go/pix and
http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod_technical_documentation.html

---

What's New in Cisco PIX Device Manager version 3.0

New Features in PDM version 3.0

The following items are features new to PDM Version 3.0(4), since PDM Version 3.0(1) was released. Many of these features were introduced to support changes with PIX Firewall Version 6.3(4).

- **AAA Fallback**—By default, a AAA server failure would prevent you from authenticating and/or authorizing. This feature lets you optionally choose to use the LOCAL database on the Cisco PIX Firewall for authentication and/or authorization in the event of a AAA server failure. You can optionally use the LOCAL Cisco PIX Firewall database for:
  - Authentication and/or authorization to the firewall
  - IKE extended authentication (XAuth)

  This feature was introduced with PIX Firewall version 6.3(4).
- **Virtual LAN (VLAN) support for PIX 506/506E**—PDM supports VLANs on the Cisco PIX Firewall 506/506E. A maximum of two logical interfaces can be configured on these two interface platforms because there is a four interface limit.
- **Filter except for HTTPS, FTP, Java, and ActiveX**—PDM 3.0 allows additional filter actions, namely "do not filter ActiveX," "do not filter Java Applet," "do not filter HTTPS," and "do not filter FTP." These filters allow you specify hosts or networks that should not be filtered. For example, if the host or network you

specify is included in a Filter ActiveX rule, then you can create a Do Not Filter ActiveX rule to create an exception.

- **SIP IP Address Privacy**—If any two SIP endpoints participating in an IP phone call or instant messaging session use the same internal firewall interface to contact their SIP proxy server on an external firewall interface, enabling SIP IP Address Privacy ensures that all SIP signaling messages go through the SIP proxy server.
  This feature is in effect when SIP over TCP Fixup or SIP over UDP Fixup is enabled. By default, this feature is disabled.
  If SIP IP Address Privacy is enabled, the firewall will not translate internal and external host IP addresses embedded in the TCP or UDP payload of inbound SIP traffic, ignoring translation rules for those IP addresses.
- **ISAKMP (IKE) Event Tracing**—ISAKMP Event Tracing includes a simple event tracing buffer for troubleshooting. It is helpful for detailed troubleshooting when a syslog server is unavailable, such as in a PIX 501 Easy VPN Remote deployment. You can configure the number of events to log. By default, event tracing is disabled.
- **Support Netmask in Local Pool**—This feature allows you to optionally configure a netmask for the IP local pool. This information is sent to the VPN client when it sends a mode configuration request for the netmask. Without this feature, a VPN client such as the Windows VPN 4.x Client will simply use the classful netmask since none is provided.
- **SNMP Fixup**—This feature allows you to inspect SNMP traffic passing through the firewall. By default, SNMP inspection is disabled.
  In addition, you can filter out traffic based on the SNMP protocol version. The SNMP versions are version 1, 2, 2c, and 3.
- **Extended DNS (EDNS0) Fixup**—The Extended DNS (EDNS0) feature adds support for the DNS fixup and support for a UDP DNS packet greater than 512 bytes. Support for greater than 512 bytes is defined in RFC 2671. Prior to this feature, the firewall simply dropped UDP DNS packets greater than 512 bytes.
- **TFTP Fixup**—The TFTP fixup solves the problem of an inside SIP phone trying to get configuration files through TFTP from an outside proxy server. The fixup is enabled by default and uses port 69. This feature was introduced in PIX 6.3(2).
- **Display VAC Information**—The PDM Home Page now indicates whether a VPN accelerator card (VAC) or VAC+ is present or not.

The following features were introduced in PDM Version 3.0(1)

- **VLAN**—802.1Q VLAN support comes to the PIX Firewall, providing added flexibility in managing and provisioning the firewall. This feature enables the decoupling of IP interfaces from physical interfaces (hence making it possible to configure logical IP interfaces independent of the number of interface cards installed), and supplies appropriate handling for IEEE 802.1Q tags.
- **OSPF**—Route propagation and greatly reduced route convergence times are two of the many benefits that arrive with OSPF. The PIX Firewall implementation will support intra-area, inter-area and external routes. The distribution of static routes to OSPF processes and route redistribution between OSPF processes are also included.
- **PAT for ESP Tunnels**—Provides the ability to PAT IP protocol 50 to support a single IPSec user outbound access.
- **NAT Traversal**—This feature addresses most of the known incompatibilities between NAT and IPSec that have become a major barrier to the deployment of IPSec. The design is based on the IETF NAT wrapper draft to ensure maximum interoperability with Cisco NAT products as well as non-Cisco NAT platforms.
- **DHCP Relay**—Acting as a DHCP Relay Agent, the PIX Firewall can assist in dynamic configuration of IP hosts on any of its interfaces. It receives requests from hosts on a given interface and forwards them to a user-configured DHCP server on another interface.
- **Comments in ACLs**—This feature allows users to include comments in access lists to make the ACL

easier to understand and scan.

- **Syslog by ACL**—This feature allows users to configure a specific ACL entry with a logging option. When such an option is configured, statistics for each flow that matches the permit or deny conditions of the ACL entry are logged.
- **AES**—This feature adds support for AES on PIX Firewall. It is anticipated that the IETF will mandate AES as required privacy transforms for both IPSec and IKE in the near future. AES supports 128-bit, 192-bit, and 256-bit encryption.
- **Diffie-Hellman Group 5**—This feature adds support for 1536-bit MODP Group that has been given the group 5 identifier.
- **Specify Interface as Address in ACLs**—Users running the DHCP client on the PIX Firewall outside interface will no longer have to adjust their access-lists every time the outside DHCP address gets changed by their ISP.
- Java Plug-in 1.4—PDM 3.0 adds support for the Java Plug-in versions 1.4.2. The plug-in can be downloaded at http://java.sun.com.
- **New Fixups**—TAPI/JTAPI, MGCP, PAT for PPTP, PAT for ESP Tunnels, ICMP Error.
- **CA Enrollment using X.500**—Aggressive Mode is used for pre-shared keys and Main Mode (MM) can now be used for RSA-IG based key exchange. This is in conformance with 3002 behavior, where MM is performed whenever possible.
- **HTTPS Authentication Proxy**—This new feature provides a secure method of exchanging information between an HTTP client and PIX Firewall by using HTTPS for the transaction.
- **Verify Certificate Domain Name**—You can now verify and filter out valid but unexpected peer certificates during IKE negotiation.
- **VPN Interoperability**—In PDM you can specify a key-id or a string for interoperability with other headend VPN devices.
- **Change level for Syslog Messages**—This feature allows users to change the default logging level for a specific ACL entry with a logging option. When such an option is configured, statistics for each flow that matches the permit or deny conditions of the ACL entry are logged.
- **AAA Proxy Limit**—You can limit the number of concurrent proxy connections allowed.
- **HTTPS/FTP using Websense**—This feature extends the existing Websense-based URL filtering to HTTPS and FTP.
- **SIP**—You can configure the ports on which the firewall listens for SIP over TCP traffic.
- **Ability to disable SIP UDP fixup**—This adds support for valid non-SIP packets being dropped by the PIX Firewall when they use a SIP UDP port.
- **DHCP server on any interface**—Any interface can now be configured as a DHCP server.
- **Management Feature Access**—You can now perform PIX management functions, such as running PDM, on an internal interface with a fixed IP address over an IPSec VPN tunnel.
- **Console Timeout**—The new **Console** panel lets you set the time a console connection remains open when idle.
- **Banner**—The new **Banner** panel lets you configure message of the day, login, and session banners.
- **Improved Printing**—Printing has been improved so access lists can be printed and viewed more easily.
- **RME Syslog Compatibility**— This new feature provides the ability to log messages in Cisco EMBLEM format to a syslog server. This feature allows the RME (Resource Manager Essentials) syslog analyzer to parse PIX messages sent to a syslog host.
- **PDM Home Page**—The new PDM home page lets you view at a glance important information about your PIX Firewall such as the status of your interfaces, the version you are running, licensing information, and performance.
- **Batch mode when sending CLIs**—PDM is faster in the method it uses to send a series of CLI commands to the firewall. It allows all CLIs to be sent and configured, even if you end up losing the connection because of the changes you make.

Additional new features supported by the PIX Firewall can be found in the Cisco PIX Firewall Release Notes Version 6.3.

Administrative Session Security

Several safeguards are available to ensure that access to a firewall via PDM is secure:

- **Administrator Authentication**—When you access PDM, the firewall prompts you for login credentials. You can restrict access via a password, which is encrypted and stored locally on the PIX Firewall. You can also use an external authentication server to store username and password information.
- **Allowed Hosts**—You can configure the PIX Firewall to allow only certain hosts to run PDM.
- **Signed Applets**—Java features include digital signatures for applets, so that you can ascertain the origin of an applet, and limit entry into your system to applets that have been signed by trusted entities. For more information about Java security features, refer to http://www.sun.com/960901/feature3/javasecure.html.
- **SSL**—All communication between PDM and the firewall is secured via Secure Sockets Layer (SSL). SSL is supported in most browsers and enables information to be encrypted through the 56-bit Data Encryption Standard (DES) or the more secure 168-bit Triple DES (3DES).

System Requirements

PIX Firewall Platforms

PDM is available on all Cisco PIX Firewall 501, PIX Firewall 506/506E, PIX Firewall 515/515E, PIX Firewall 520, PIX Firewall 525, and PIX Firewall 535 platforms running Version 6.3. PDM Version 3.0 is a single image which supports only PIX Firewall Version 6.3.

For more detailed requirements, see Getting Started.

Copyright © 2001-2004, Cisco Systems, Inc.

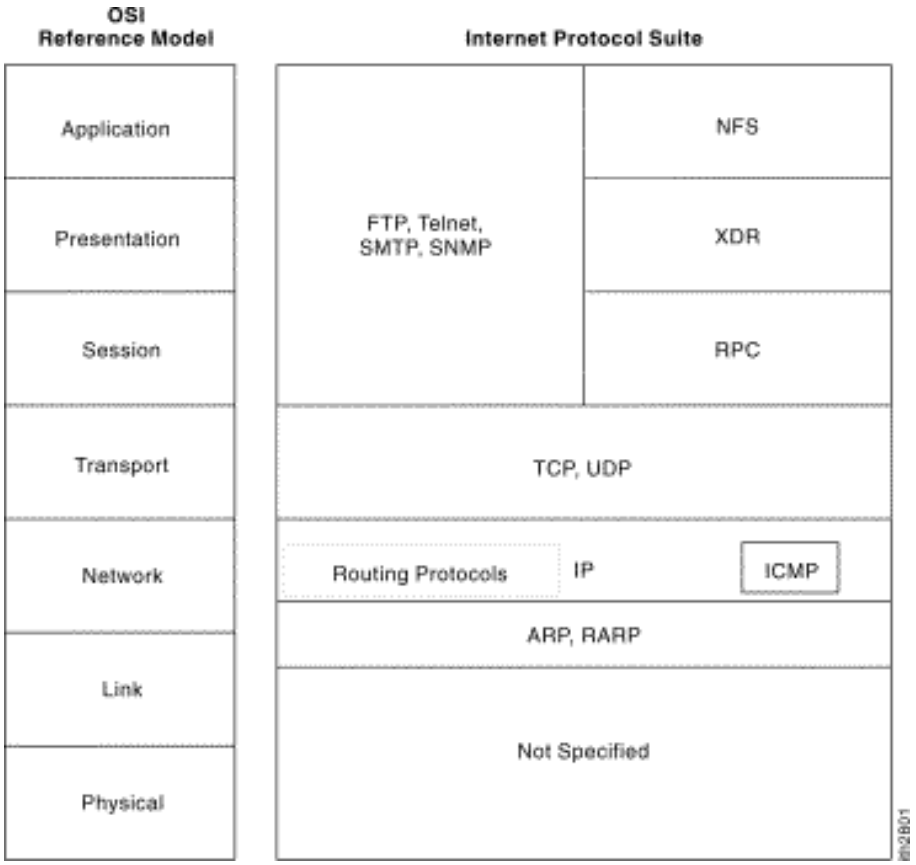
IP (Internet Protocols)

This topic provides reference information on IP and related subjects in the context of configuring and using firewalls managed by PDM. See also, **System Properties>Advanced>**TCP Options and Fixups.

The Internet protocols consist of a suite of communication protocols, of which the two best known are the Transmission Control Protocol (TCP) and the Internet Protocol (IP). The Internet protocol suite not only includes lower-layer protocols (such as TCP and IP), but it also specifies common applications such as electronic mail, terminal emulation, and file transfer.

Layers

Internet protocols span the complete range of OSI model layers which describe the function of network protocols.

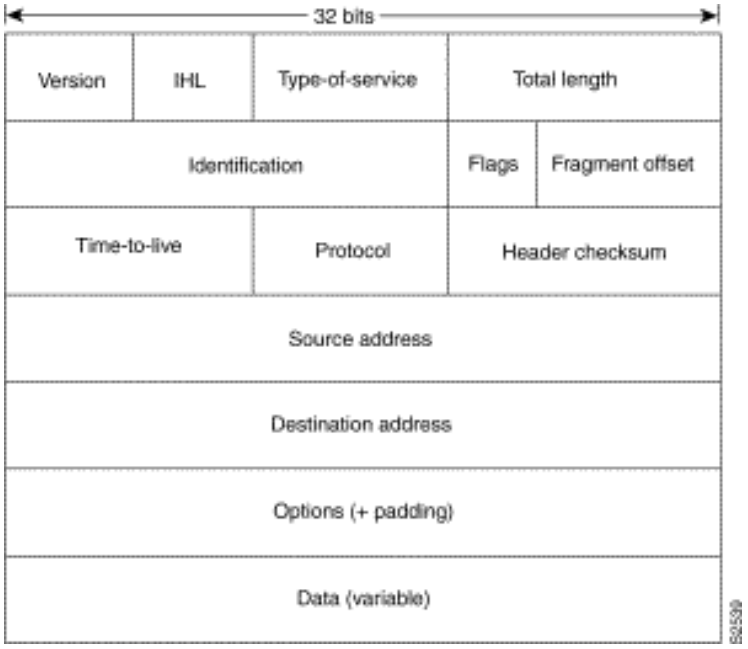


Application-Layer Protocols

The Internet protocol suite includes many application-layer protocols that represent a wide variety of applications, including the following:

- **File Transfer Protocol (FTP)**—Moves files between devices
- **Simple Network-Management Protocol (SNMP**)—Primarily reports anomalous network conditions and sets network threshold values
- **Telnet**—Serves as a terminal emulation protocol
- **X Windows**—Serves as a distributed windowing and graphics system used for communication between X terminals and UNIX workstations
- **Network File System (NFS**)—External Data Representation (XDR), and Remote Procedure Call (RPC)—Work together to enable transparent access to remote network resources
- **Simple Mail Transfer Protocol (SMTP)**—Provides electronic mail services
- **Domain Name System (DNS)**—Translates the names of network nodes into network addresses

IP Packet



Fourteen fields comprise an IP packet.

1. **Version**—Indicates the version of IP currently used.
2. **IP Header Length** (IHL)—Indicates the datagram header length in 32-bit words.
3. **Type-of-Service**—Specifies how an upper-layer protocol would like a current datagram to be handled, and assigns datagrams various levels of importance.
4. **Total Length**—Specifies the length, in bytes, of the entire IP packet, including the data and header.
5. **Identification**—Contains an integer that identifies the current datagram. This field is used to help piece together datagram fragments.
6. **Flags**—Consists of a 3-bit field of which the two low-order (least-significant) bits control fragmentation. The low-order bit specifies whether the packet can be fragmented. The middle bit specifies whether the packet is the last fragment in a series of fragmented packets. The third or high-order bit is not used.
7. **Fragment Offset**—Indicates the position of the fragment's data relative to the beginning of the data in the original datagram, which allows the destination IP process to properly reconstruct the original datagram.
8. **Time-to-Live**—Maintains a counter that gradually decrements down to zero, at which point the datagram is discarded. This keeps packets from looping endlessly.

9. **Protocol**—Indicates which upper-layer protocol receives incoming packets after IP processing is complete.
10. **Header Checksum**—Helps ensure IP header integrity.
11. **Source Address**—Specifies the sending node.
12. **Destination Address**—Specifies the receiving node.
13. **Options**—Allows IP to support various options, such as security.
14. **Data**—Contains upper-layer information.

IP Address

[Introduction] [Classes] [PIX IP Address Values] [Multicast]

Introduction

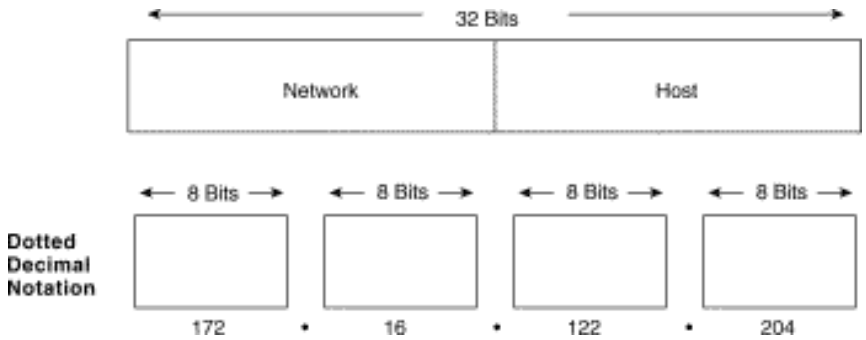
IP version 4 addresses are 32-bits, or 4 bytes, in length. This address "space" is used to designate the following:

- network number
- optional subnetwork number
- a host number

The 32 bits are grouped into four octets which are represented by 4 decimal numbers separate by periods or "dots". The meaning of each of the four octets is determined by their use in a particular network.

Addresses used on the public internet must be completely unique for the period of time they are being used. On private networks, addresses may be unique only to the private network or subnetwork. This is called the "reuse" of addresses.

Addresses may also be translated using schemes, such NAT and PAT, as well as temporarily assigned using DHCP.

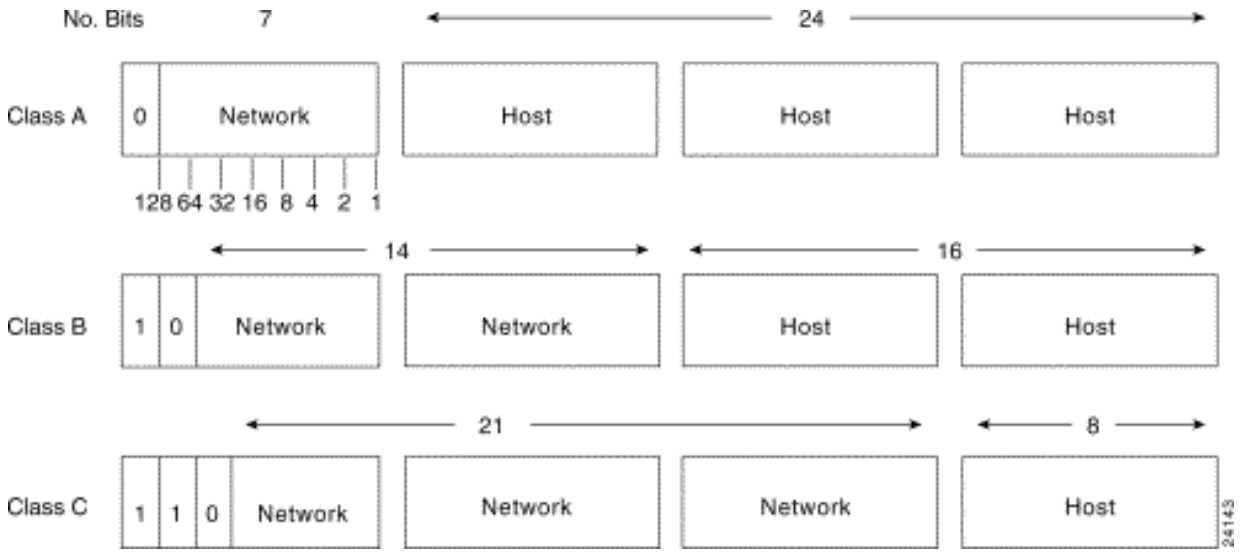


IP Address Classes

IP addressing supports five different address classes: A, B,C, D, and E. Only classes A, B, and C are available for commercial use. The leftmost (high-order) bits indicate the network class. The following illustration provides

reference information about the five IP address classes.

IP Classes



IP address classes are defined as follows:

- **Class A**— If the first octet is between 1 and 127 (inclusive), the address is a Class A address. In a Class A address, the first octet is the one-byte net address and the last three octets are the host address. The network mask for Class A addresses is 255.0.0.0.
- **Class B**— If the first octet is between 128 and 191 (inclusive), the address is a Class B address. In a Class B address, the first two octets are the net address and the last two octets are the host address. The network mask for Class B addresses is 255.255.0.0.
- **Class C**— If the first octet is 192 or higher, the address is a Class C address. In a Class C address, the first three octets are the net address and the last octet is the host address. The network mask for Class C addresses is 255.255.255.0.
- **Class D**—These addresses are used for multicast transmissions and within the range from 224.0.0.0 to 239.255.255.255. Some of these addresses are assigned to multicasts used by specific TCP/IP protocols. Other Class D addresses are assigned to applications, such as streaming video, that send data to many recipients simultaneously. For information about enabling the PIX Firewall to transmit multicast traffic, refer to the firewall *Configuration Guide*, *Enabling Stub Multicast Routing.*

PIX IP Address Values

We recommend that you use RFC 1918 IP addresses for inside and perimeter addresses. These addresses follow:

- **Class A**: 10.0.0.0 to 10.255.255.255
- **Class B**: 172.16.0.0 to 172.31.255.255
- **Class C**: 192.168.0.0 to 192.168.255.255
- **Class D**: 224.0.0.0 to 239.255.255.255

PIX Firewall requires that IP addresses in the `ip address`, `static`, `global`, `failover`, and `virtual` commands be unique. These IP addresses cannot be the same as your router IP addresses.

In PDM Online Help and Firewall Configuration Guide, the use of "address" and "IP address" are synonymous.

IP addresses are primarily one of these values for PIX Firewall CLI:

- *local_ip*—An untranslated IP address on the internal, protected network. In an outbound connection originated from *local_ip*, the *local_ip* is translated to the *global_ip*. On the return path, the *global_ip* is translated to the *local_ip*. The *local_ip* to *global_ip* translation can be disabled with the `nat 0 0 0` command. In syslog messages, this address is referenced as laddr.
- *global_ip*—A translated global IP address in the pool or those addresses declared with the **global** or **static** commands. In syslog messages, this address is referenced as gaddr.
- *foreign_ip*—An untranslated IP address on an external network. foreign_ip is an address for hosts on the external network. If the `alias` command is in use, an inbound message originating for the *foreign_ip* source address is translated to *dnat_ip* by PIX Firewall.
- *dnat_ip*—(dual NAT) A translated (by the `alias` command) IP address on an external network. In an outbound connection destined to *dnat_ip*, it will be untranslated to *foreign_ip*. In syslog messages, this address is referenced as *faddr*.
- *virtual_ip*—(used with the `virtual` command) A fictitious public or private IP address that is not the address of a real web server on the interface you are accessing. We recommend that you use an RFC 1918 address or one you make up.

Multicast Addresses

Multicast addressing allows a source to transmit packets to multiple destinations, a multicast group, simultaneously.

Multicast addresses range from **`224.0.0.0`** to **`239.255.255.255`**, however only the range **`224.0.1.0`** to **`239.255.255.255`** is available to us.

The first part of the multicast address range, **`224.0.0.0`** to **`224.0.0.255`**, is reserved and referred to as the **Reserved Local Link Addresses** (RLLA). These addresses are unavailable.

We can exclude the RLLA range by specifying **`224.0.1.0`** to **`239.255.255.255`**.

`224.0.0.0` to **`239.255.255.255`** *excluding* **`224.0.0.0`** to **`224.0.0.255`**
is the same as
`224.0.1.0` to **`239.255.255.255`**.

Note: PIX Firewall does not pass multicast packets. Many routing protocols use multicast packets to transmit their data. If you need to send routing protocols across the PIX Firewall, configure the routers with the Cisco IOS software **neighbor** command. We consider it inherently dangerous to send routing protocols across the PIX Firewall. If the routes on the unprotected interface are corrupted, the routes transmitted to the protected side of the firewall will pollute routers there as well.

The following RFCs from the IETF provide technical details about the IGMP and multicast routing standards used for implementing the SMR feature:

RFC 2236 IGMPv2

- RFC 2362 PIM-SM
- RFC 2588 IP Multicast and Firewalls
- RFC 2113 IP Router Alert Option
- IETF draft-ietf-idmr-igmp-proxy-01.txt

For a primer on multicast on other Cisco equipment, please see PDM **Glossary>Multicast** and the following Cisco public websites which provide background information about multicast routing:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/ipimt_ov.htm
http://www.cisco.com/warp/public/732/Tech/Multicast/

Mask, Netmask, IP Subnet Mask

Using Subnet Masks

This section lists information by subnet mask and identifies which masks are for networks, hosts, and broadcast addresses.

Note In some networks, broadcasts are also sent on the network address.

This section includes the following topics:

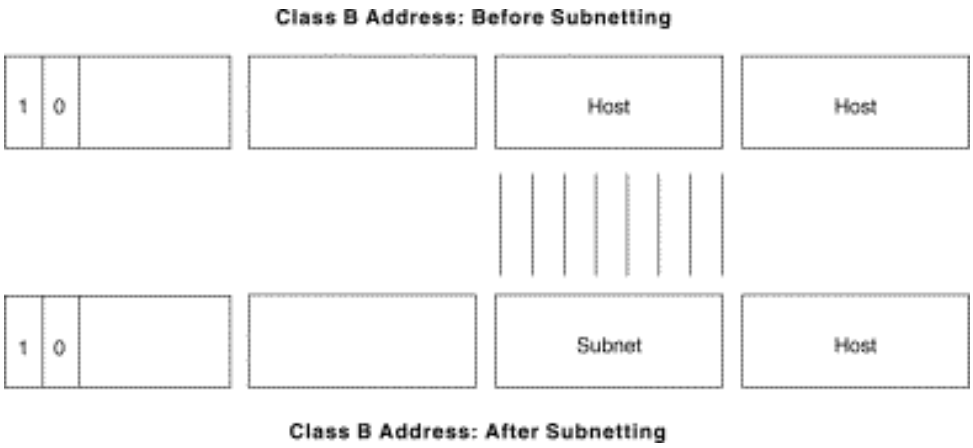
- Introduction to IP Subnetwork Masks
- Uses for Subnet Information
- With Limited IP Addresses
- Addresses in the .128 Mask
- Addresses in the .192 Mask
- Addresses in the .224 Mask
- Addresses in the .240 Mask
- Addresses in the .248 Mask
- Addresses in the .252 Mask

Introduction to IP Subnet Masks

IP Subnet Addressing. IP networks can be divided into smaller networks called subnetworks (or subnets). Subnetting provides the network administrator with several benefits, including extra flexibility, more efficient use of network addresses, and the capability to contain broadcast traffic (a broadcast will not cross a router). Subnets are under local administration. As such, the outside world sees an organization as a single network and has no detailed knowledge of the organization's internal structure. A given network address can be broken up into many subnetworks. For example, 172.16.1.0, 172.16.2.0, 172.16.3.0, and 172.16.4.0 are all subnets within network 171.16.0.0. (All 0s in the host portion of an address specifies the entire network.)

IP Subnet Mask A subnet address is created by "borrowing" bits from the host field and designating them as the subnet field. The number of borrowed bits varies and is specified by the subnet mask. The following illustration shows how bits are borrowed from the host address field to create the subnet address field.

IP Subnet Mask



Netmask Basics

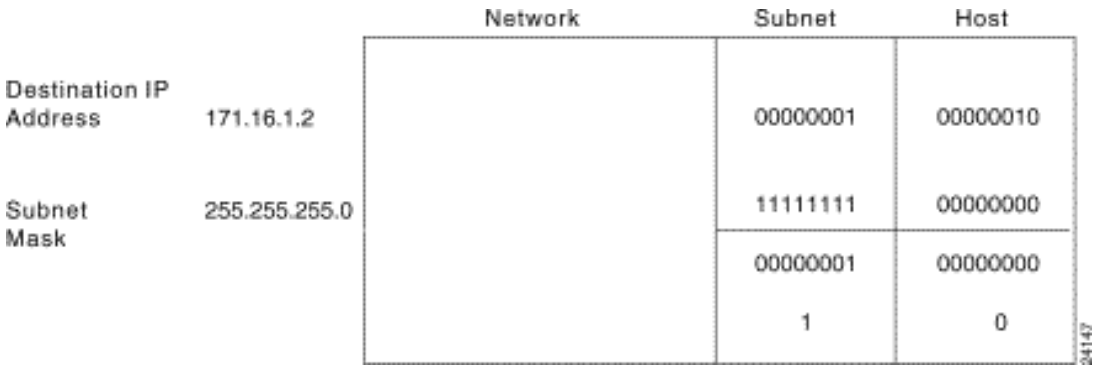
A mask is a 32-bit field which shows how an Internet address is to be divided into network, subnet and host parts. The netmask has ones in the bit positions in the 32-bit address which are to be used for the network and subnet parts, and zeros for the host part. The mask should contain at least the standard network portion (as determined by the address's class), and the subnet field should be contiguous with the network portion.

How Subnet Masks are Used to Determine the Network Number

Logical AND Operation. Three basic rules govern logically "ANDing" two binary numbers. First, 1 "ANDed" with 1 yields 1. Second, 1 "ANDed" with 0 yields 0. Finally, 0 "ANDed" with 0 yields 0. Two simple guidelines exist for remembering logical AND operations: Logically "ANDing" a 1 with a 1 yields the original value, and logically "ANDing" a 0 with any number yields 0.

The following figure illustrates that when a logical AND of the destination IP address and the subnet mask is performed, the subnetwork number remains, which the router uses to forward the packet. Applying a logical AND the destination IP address and the subnet mask produces the subnetwork number.

Netmask Logical AND



firewall and Masks

For the Cisco Firewall commands that accept network masks, specify the correct mask for a network address. For hosts, use 255.255.255.255. However, for the **ip address** command, use a network mask, and for the **global** command, use a network address for both Port Address Translation (PAT) addresses and when specifying a pool of global addresses.

For the **conduit** and **access-list** commands, precede host addresses with the **host** parameter and without specifying a mask.

The following are examples of commands in which a mask can be specified:

```
ip address inside 10.1.1.1 255.255.255.0
ip address outside 209.165.201.1 255.255.255.224
nat (inside) 1 10.1.1.0 255.255.255.0
global (outside) 1 209.165.201.2 netmask 255.255.255.224
static (inside,outside) 209.165.201.3 10.1.1.3 netmask 255.255.255.255
access-list acl_out permit tcp any host 209.165.201.3 eq www
aaa authentication include http outside 209.165.201.3 255.255.255.255 0 0 TACACS+
route outside 0 0 209.165.201.4 1
telnet 10.1.1.2 255.255.255.255
```

In these examples, the **ip address** commands specify addresses for the inside and outside network interfaces. The **ip address** command only uses network masks. The inside interface is a Class A address, but only the last octet is used in the example network and therefore has a Class C mask. The outside interface is part of a subnet so the mask reflects the .224 subnet value.

The **nat** command lets users start connections from the inside network. Because a network address is specified, the class mask specified by the **ip address inside** command is used.

The **global** command provides a PAT address to handle the translated connections from the inside. The global address is also part of the subnet and contains the same mask specified in the **ip address outside** command.

The **static** command maps an inside host to a global address for access by outside users. Host masks are always specified as 255.255.255.255.

The **access-list** command permits any outside host to access the global address specified by the **static** command. The **host** parameter is the same as if you specified 209.165.201.3 255.255.255.255.

The **aaa** command indicates that any users wishing to access the global address must be authenticated. Because authentication only occurs when users access the specified global which is mapped to a host, the mask is for a host. The "0 0" entry indicates any host and its respective mask.

The **route** statement specifies the address of the default router. The "0 0" entry indicates any host and its respective mask.

The **telnet** command specifies a host that can access the PIX Firewall unit's console using Telnet. Because it is a single host, a host mask is used.

If you are using subnet masks, refer to "Uses for Subnet Masks," to be sure that each IP address you choose for global or static addresses is in the correct subnet.

The subnet masks are also identified by the number of bits in the mask. The following table list subnet masks by the number of bits in the network ID.

Subnet Masks by Network ID

Network ID Bits	Host ID Bits	Subnet	Example Notation	# of Subnets	# of Hosts on Each Subnet
24	8	.0	192.168.1.1/24	1	254
25	7	.128	192.168.1.1/25	2	126
26	6	.192	192.168.1.1/26	4	62
27	5	.224	192.168.1.1/27	8	30
28	4	.240	192.168.1.1/28	16	14

29	3	.248	192.168.1.1/29	32	6
30	2	.252	192.168.1.1/30	64	2

The .255 mask indicates a single host in a network.

Uses for Subnet Information

Use subnet information to ensure that your host addresses are in the same subnet and that you are not accidentally using a network or broadcast address for a host.

The network address provides a way to reference all the addresses in a subnet, which you can use in the `global`, `outbound`, and `static` commands. For example, you can use the following net `static` command statement to map global addresses 192.168.1.65 through 192.168.1.126 to local addresses 192.168.2.65 through 192.168.2.126: **static (dmz1,dmz2) 192.168.1.64 192.168.2.64 netmask 255.255.255.192.**

Subnet mask information is especially valuable when you have disabled Network Address Translation (NAT) using the `nat 0` command. PIX Firewall requires that IP addresses on each interface be in different subnets.

However all the hosts on a PIX Firewall interface between the PIX Firewall and the router must be in the same subnet as well. For example, if you have an address such as 192.168.17.0 and you are not using NAT, you could use the 255.255.255.192 subnet mask for all three interfaces and use addresses 192.168.17.1 through 192.168.17.62 for the outside interface, 192.168.17.65 through 192.168.17.126 for the perimeter interface, and 192.168.17.129 through 192.168.17.190 for the inside interface.

With Limited IP Addresses

Another use for subnet mask information is for network planning when an Internet service provider (ISP) gives you a limited number of IP addresses and requires you to use a specific subnet mask. Use the information in this appendix to ensure that the outside addresses you choose are in the subnet for the appropriate subnet mask.

For example, if your ISP assigns you 192.168.17.176 with a subnet mask of .240, you can see in the Table for 240, Subnet Number 12 for the .240 mask, that hosts can have IP addresses of 192.168.17.177 through 192.168.17.190. Because this only yields 14 hosts, you will probably use one for your router, another for the outside interface of the PIX Firewall, one for a static for a web server, if you have it, one for a static for your mail server, and the remaining 10 for global addresses. One of these addresses should be a PAT address so that you do not run out of global addresses.

Addresses in the .128 Mask

Valid addresses for the .128 subnet mask. This mask permits up to 2 subnets with enough host addresses for 126 hosts per subnet.

.128 Network Mask Addresses

Subnet Number	Network Address	Starting Host Address	Ending Host Address	Broadcast Address
1	.0	.1	.126	.127
2	.128	.129	.254	.255

Addresses in the .192 Mask

Valid addresses for the .192 subnet mask. This mask permits up to 4 subnets with enough host addresses for 62 hosts per subnet.

<

Subnet Number	Network Address	Starting Host Address	Ending Host Address	Broadcast Address
1	.0	.1	.62	.63
2	.64	.65	.126	.127
3	.128	.129	.190	.191

4	.192	.193	.254	.255

Addresses in the .224 Mask

Valid addresses for the .224 subnet mask. This mask permits up to 8 subnets with enough host addresses for 30 hosts per subnet.

Subnet Number	Network Address	Starting Host Address	Ending Host Address	Broadcast Address
1	.0	.1	.30	.31
2	.32	.33	.62	.63
3	.64	.65	.94	.95
4	.96	.97	.126	.127
5	.128	.129	.158	.159
6	.160	.161	.190	.191
7	.192	.193	.222	.223
8	.224	.225	.254	.255

Addresses in the .240 Mask

Valid addresses for the .240 subnet mask. This mask permits up to 16 subnets with enough host addresses for 14 hosts per subnet.

Subnet Number	Network Address	Starting Host Address	Ending Host Address	Broadcast Address
1	.0	.1	.14	.15
2	.16	.17	.30	.31
3	.32	.33	.46	.47
4	.48	.49	.62	.63
5	.64	.65	.78	.79
6	.80	.81	.94	.95
7	.96	.97	.110	.111
8	.112	.113	.126	.127
9	.128	.129	.142	.143

10	.144	.145	.158	.159
11	.160	.161	.174	.175
12	.176	.177	.190	.191
13	.192	.193	.206	.207
14	.208	.209	.222	.223
15	.224	.225	.238	.239
16	.240	.241	.254	.255

Addresses in the .248 Mask

Valid addresses for the .248 subnet mask. This mask permits up to 32 subnets with enough host addresses for 6 hosts per subnet.

Subnet Number	Network Address	Starting Host Address	Ending Host Address	Broadcast Address
1	.0	.1	.6	.7
2	.8	.9	.14	.15

3	.16	.17	.22	.23
4	.24	.25	.30	.31
5	.32	.33	.38	.39
6	.40	.41	.46	.47
7	.48	.49	.54	.55
8	.56	.57	.62	.63
9	.64	.65	.70	.71
10	.72	.73	.78	.79
11	.80	.81	.86	.87
12	.88	.89	.94	.95
13	.96	.97	.102	.103
14	.104	.105	.110	.111
15	.112	.113	.118	.119

16	.120	.121	.126	.127
17	.128	.129	.134	.135
18	.136	.137	.142	.143
19	.144	.145	.150	.151
20	.152	.153	.158	.159
21	.160	.161	.166	.167
22	.168	.169	.174	.175
23	.176	.177	.182	.183
24	.184	.185	.190	.191
25	.192	.193	.198	.199
26	.200	.201	.206	.207
27	.208	.209	.214	.215
28	.216	.217	.222	.223

29	.224	.225	.230	.231
30	.232	.233	.238	.239
31	.240	.241	.246	.247
32	.248	.249	.254	.255

Valid Addresses in the .252 Mask

Valid addresses for the .252 subnet mask. This mask permits up to 64 subnets with enough host addresses for 2 hosts per subnet.

Subnet Number	Network Address	Starting Host Address	Ending Host Address	Broadcast Address
1	.0	.1	.2	.3
2	.4	.5	.6	.7
3	.8	.9	.10	.11
4	.12	.13	.14	.15
5	.16	.17	.18	.19

6	.20	.21	.22	.23
7	.24	.25	.26	.27
8	.28	.29	.30	.31
9	.32	.33	.34	.35
10	.36	.37	.38	.39
11	.40	.41	.42	.43
12	.44	.45	.46	.47
13	.48	.49	.50	.51
14	.52	.53	.54	.55
15	.56	.57	.58	.59
16	.60	.61	.62	.63
17	.64	.65	.66	.67
18	.68	.69	.70	.71

19	.72	.73	.74	.75
20	.76	.77	.78	.79
21	.80	.81	.82	.83
22	.84	.85	.86	.87
23	.88	.89	.90	.91
24	.92	.93	.94	.95
25	.96	.97	.98	.99
26	.100	.101	.102	.103
27	.104	.105	.106	.107
28	.108	.109	.110	.111
29	.112	.113	.114	.115
30	.116	.117	.118	.119
31	.120	.121	.122	.123

32	.124	.125	.126	.127
33	.128	.129	.130	.131
34	.132	.133	.134	.135
35	.136	.137	.138	.139
36	.140	.141	.142	.143
37	.144	.145	.146	.147
38	.148	.149	.150	.151
39	.152	.153	.154	.155
40	.156	.157	.158	.159
41	.160	.161	.162	.163
42	.164	.165	.166	.167
43	.168	.169	.170	.171
44	.172	.173	.174	.175

45	.176	.177	.178	.179
46	.180	.181	.182	.183
47	.184	.185	.186	.187
48	.188	.189	.190	.191
49	.192	.193	.194	.195
50	.196	.197	.198	.199
51	.200	.201	.202	.203
52	.204	.205	.206	.207
53	.208	.209	.210	.211
54	.212	.213	.214	.215
55	.216	.217	.218	.219
56	.220	.221	.222	.223
57	.224	.225	.226	.227

58	.228	.229	.230	.231
59	.232	.233	.234	.235
60	.236	.237	.238	.239
61	.240	.241	.242	.243
62	.244	.245	.246	.247
63	.248	.249	.250	.251
64	.252	.253	.254	.255

TCP/IP

TCP/IP (Transmission Control Protocol) is a connection-oriented transport layer protocol that provides reliable full-duplex data transmission in an IP environment. TCP corresponds to the transport layer (Layer 4) of the OSI reference model. Among the services TCP provides are stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing.

With stream data transfer, TCP delivers an unstructured stream of bytes identified by sequence numbers. This service benefits applications because they do not have to chop data into blocks before handing it off to TCP. Instead, TCP groups bytes into segments and passes them to IP for delivery.

TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an internetwork. It does this by sequencing bytes with a forwarding acknowledgment number that indicates to the destination the next byte the source expects to receive. Bytes not acknowledged within a specified time period are retransmitted. The reliability mechanism of TCP allows devices to deal with lost, delayed, duplicate, or misread packets. A time-out mechanism allows devices to detect lost packets and request retransmission.

TCP offers efficient flow control, which means that, when sending acknowledgments back to the source, the

receiving TCP process indicates the highest sequence number it can receive without overflowing its internal buffers. Full-duplex operation means that TCP processes can both send and receive at the same time.

Finally, TCP's multiplexing means that numerous simultaneous upper-layer conversations can be multiplexed over a single connection.

TCP Connection Establishment

To use reliable transport services, TCP hosts must establish a connection-oriented session with one another. Connection establishment is performed by using a "three-way handshake" mechanism.

A three-way handshake synchronizes both ends of a connection by allowing both sides to agree upon initial sequence numbers. This mechanism also guarantees that both sides are ready to transmit data and know that the other side is ready to transmit as well. This is necessary so that packets are not transmitted or retransmitted during session establishment or after session termination.

Each host randomly chooses a sequence number used to track bytes within the stream it is sending and receiving. Then, the three-way handshake proceeds in the following manner:

The first host (Host A) initiates a connection by sending a packet with the initial sequence number (X) and SYN bit set to indicate a connection request. The second host (Host B) receives the SYN, records the sequence number X, and replies by acknowledging the SYN (with an ACK = X + 1). Host B includes its own initial sequence number (SEQ = Y). An ACK = 20 means the host has received bytes 0 through 19 and expects byte 20 next. This technique is called forward acknowledgment. Host A then acknowledges all bytes Host B sent with a forward acknowledgment indicating the next byte Host A expects to receive (ACK = Y + 1). Data transfer then can begin.

Positive Acknowledgment and Retransmission (PAR)

A simple transport protocol might implement a reliability-and-flow-control technique where the source sends one packet, starts a timer, and waits for an acknowledgment before sending a new packet. If the acknowledgment is not received before the timer expires, the source retransmits the packet. Such a technique is called positive acknowledgment and retransmission (PAR).

By assigning each packet a sequence number, PAR enables hosts to track lost or duplicate packets caused by network delays that result in premature retransmission. The sequence numbers are sent back in the acknowledgments so that the acknowledgments can be tracked.

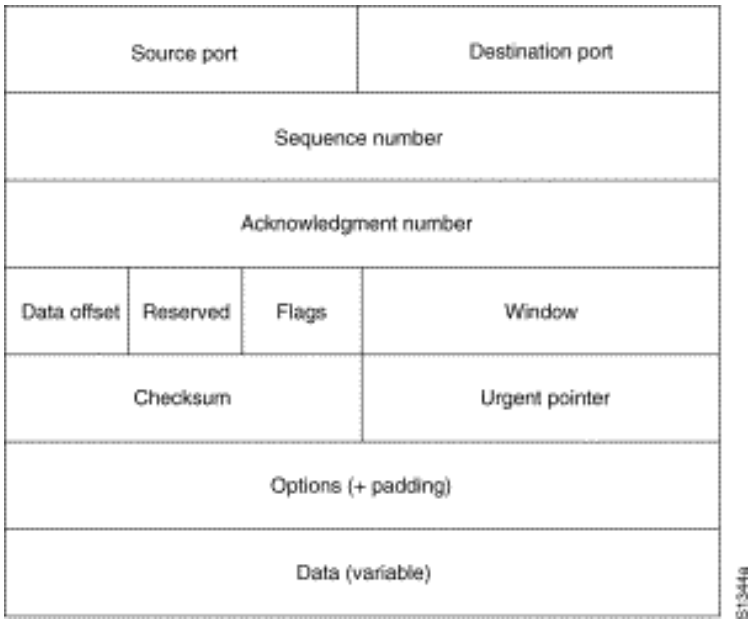
PAR is an inefficient use of bandwidth, however, because a host must wait for an acknowledgment before sending a new packet, and only one packet can be sent at a time.

TCP Sliding Window

A TCP sliding window provides more efficient use of network bandwidth than PAR because it enables hosts to send multiple bytes or packets before waiting for an acknowledgment. In TCP, the receiver specifies the current window size in every packet. Because TCP provides a byte-stream connection, window sizes are expressed in bytes. This means that a window is the number of data bytes that the sender is allowed to send before waiting for an acknowledgment. Initial window sizes are indicated at connection setup, but might vary throughout the data transfer to provide flow control. A window size of zero, for instance, means "Send no data." In a TCP sliding-window operation, for example, the sender might have a sequence of bytes to send (numbered 1 to 10) to a receiver who

has a window size of five. The sender then would place a window around the first five bytes and transmit them together. It would then wait for an acknowledgment. The receiver would respond with an ACK = 6, indicating that it has received bytes 1 to 5 and is expecting byte 6 next. In the same packet, the receiver would indicate that its window size is 5. The sender then would move the sliding window five bytes to the right and transmit bytes 6 to 10. The receiver would respond with an ACK = 11, indicating that it is expecting sequenced byte 11 next. In this packet, the receiver might indicate that its window size is 0 (because, for example, its internal buffers are full). At this point, the sender cannot send any more bytes until the receiver sends another packet with a window size greater than 0.

TCP Packet Format



Twelve fields comprise a TCP packet:

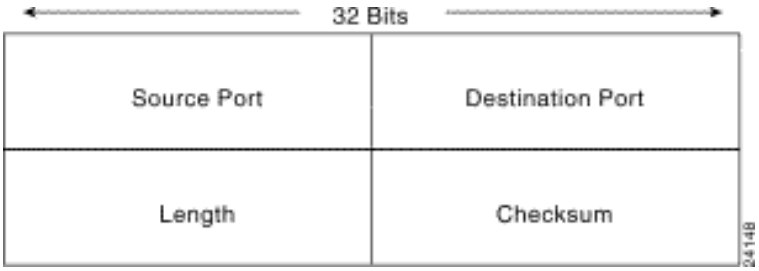
1. **Source Por**t—Identifies points at which upper-layer source and destination processes receive TCP services.
2. **Destination Port**—Identifies points at which upper-layer source and destination processes receive TCP services.
3. **Sequence Numbe**r—Usually specifies the number assigned to the first byte of data in the current message. In the connection-establishment phase, this field also can be used to identify an initial sequence number to be used in an upcoming transmission.
4. **Acknowledgment Number**—Contains the sequence number of the next byte of data the sender of the packet expects to receive.
5. **Data Offset**—Indicates the number of 32-bit words in the TCP header.
6. **Reserved**—Remains reserved for future use.
7. **Flags**—Carries a variety of control information, including the SYN and ACK bits used for connection establishment, and the FIN bit used for connection termination.
8. **Window**—Specifies the size of the sender's receive window (that is, the buffer space available for incoming data).
9. **Checksum**—Indicates whether the header was damaged in transit.
10. **Urgent Pointer**—Points to the first urgent data byte in the packet.
11. **Options**—Specifies various TCP options.
12. **Data**—Contains upper-layer information.

UDP

The User Datagram Protocol (UDP) is a connectionless transport-layer protocol (Layer 4) that belongs to the Internet protocol family. UDP is basically an interface between IP and upper-layer processes. UDP protocol ports distinguish multiple applications running on a single device from one another.

Unlike the TCP, UDP adds no reliability, flow-control, or error-recovery functions to IP. Because of UDP's simplicity, UDP headers contain fewer bytes and consume less network overhead than TCP. UDP is useful in situations where the reliability mechanisms of TCP are not necessary, such as in cases where a higher-layer protocol might provide error and flow control. UDP is the transport protocol for several well-known application-layer protocols, including Network File System (NFS), Simple Network Management Protocol (SNMP), Domain Name System (DNS), and Trivial File Transfer Protocol (TFTP).

UDP Packet Format



The UDP packet format contains four fields: source and destination ports, length, and checksum.

Ports

[Names] [Values] [RFCs]

Port Literal Names

The following literal names can be used instead of a numerical port value in command lines:

PIX Firewall permits the following TCP literal names: `bgp`, `chargen`, `cmd`, `daytime`, `discard`, **domain**, `echo`, `exec`, `finger`, **ftp**, `ftp-data`, `gopher`, `h323`, `hostname`, `http`, `ident`, `irc`, `klogin`, `kshell`, `lpd`, **nntp**, **pop2**, **pop3**, `pptp`, `rpc`, **smtp**, `sqlnet`, **sunrpc, tacacs, talk, telnet, time, uucp, whois,** and **www**.

PIX Firewall uses port 1521 for SQL*Net. This is the default port used by Oracle for SQL*Net. This value, however, does not agree with IANA port assignments.

PIX Firewall listens for RADIUS on ports 1645 and 1646. If your RADIUS server uses ports 1812 and 1813, you will need to reconfigure it to listen on ports 1645 and 1646.

Permitted UDP literal names are `biff`, `bootpc`, `bootps`, `discard`, `dnsix`, `echo`, `mobile-ip`, `nameserver`,

`netbios-dgm`, `netbios-ns`, `ntp`, `rip`, `snmp`, `snmptrap`, `sunrpc`, `syslog`, `tacacs`, `talk`, `tftp`, `time`, `who`, and `xdmcp`.

Note: To assign a port for DNS access, use `domain`, not `dns`. The `dns` keyword translates into the port value for `dnsix`.

Port Numbers, Names and RFCs

Port numbers and their RFCs can be viewed online at this URL

http://www-tac.cisco.com/Support_Library/Hardware/PIX/portall.html

or at the IANA website:

http://www.iana.org/assignments/port-numbers

Port Literal Values

Literal	Value	Description
bgp	179	Border Gateway Protocol, RFC 1163
biff	512	Used by mail system to notify users that new mail is received
bootpc	68	Bootstrap Protocol Client
bootps	67	Bootstrap Protocol Server
chargen	19	Character Generator

cmd	514	Similar to `exec` except that `cmd` has automatic authentication
daytime	13	Day time, RFC 867
discard	9	Discard
domain	53	DNS (Domain Name System)
dnsix	195	DNSIX Session Management Module Audit Redirection
echo	7	Echo
exec	512	Remote process execution
finger	79	Finger
ftp	21	File Transfer Protocol (control port)
ftp-data	20	File Transfer Protocol (data port)
gopher	70	Gopher
hostname	101	NIC Host Name Server
nameserver	42	Host Name Server

ident	113	Ident authentication service
irc	194	Internet Relay Chat protocol
isakmp	500	ISAKMP
klogin	543	KLOGIN
kshell	544	Korn Shell
lpd	515	Line Printer Daemon - printer spooler
login	513	Remote login
mobile-ip	434	MobileIP-Agent
netbios-ns	137	NetBIOS Name Service
netbios-dgm	138	NetBIOS Datagram Service
nntp	119	Network News Transfer Protocol
ntp	123	Network Time Protocol
pim-auto-rp	496	Protocol Independent Multicast, reverse path flooding, dense mode

pop2	109	Post Office Protocol - Version 2
pop3	110	Post Office Protocol - Version 3
pptp	1723	Point to Point Tunnelling Protocol pptp 1723/tcp pptp, pptp 1723/udp pptp
radius	1645, 1646	Remote Authentication Dial-In User Service
rip	520	Routing Information Protocol
smtp	25	Simple Mail Transport Protocol
snmp	161	Simple Network Management Protocol
snmptrap	162	Simple Network Management Protocol - Trap
sqlnet	1521	Structured Query Language Network
sunrpc	111	Sun RPC (Remote Procedure Call)
syslog	514	System Log
tacacs	49	TACACS+ (Terminal Access Controller Access Control System Plus)
talk	517	Talk

telnet	23	RFC 854 Telnet
tftp	69	Trivial File Transfer Protocol
time	37	Time
uucp	540	UNIX-to-UNIX Copy Program
who	513	Who
whois	43	Who Is
www	80	World Wide Web
xdmcp	177	X Display Manager Control Protocol, used to communicate between X terminals and workstations running UNIX

Protocols and Applications

This section provides information about the protocols and applications with which you may need to work when configuring PIX Firewall. It includes the following topics:

- Supported Multimedia Applications
- Supported Protocols and Applications
- Literal Values for Protocols
- VPN Standards Supported by firewall

Possible literal values are `ahp`, `eigrp`, `esp`, `gre`, `icmp`, `igmp`, `igrp`, `ip`, `ipinip`, `ipsec`, `nos`, `ospf`, `pcp`, `snp`, `tcp`, and `udp`. You can also specify any protocol by number. The `esp` and `ah` protocols only work in conjunction with Private Link.

Note: firewall does not pass multicast packets. Many routing protocols use multicast packets to transmit their

data. If you need to send routing protocols across the PIX Firewall, configure the routers with the Cisco IOS software `neighbor` command. We consider it inherently dangerous to send routing protocols across the PIX Firewall. If the routes on the unprotected interface are corrupted, the routes transmitted to the protected side of the firewall will pollute routers there as well.

Numeric Values for the Protocol Literals

Literal	Value	Description
ah	51	Authentication Header for IPv6, RFC 1826
eigrp	88	Enhanced Interior Gateway Routing Protocol
esp	50	Encapsulated Security Payload for IPv6, RFC 1827
gre	47	General Routing Encapsulation
icmp	1	Internet Control Message Protocol, RFC 792
igmp	2	Internet Group Management Protocol, RFC 1112
igrp	9	Interior Gateway Routing Protocol
ip	0	Internet Protocol
ipinip	4	IP-in-IP encapsulation

nos	94	Network Operating System (Novell's NetWare)
ospf	89	Open Shortest Path First routing protocol, RFC 1247
pcp	108	Payload Compression Protocol
snp	109	Sitara Networks Protocol
tcp	6	Transmission Control Protocol, RFC 793
udp	17	User Datagram Protocol, RFC 768

Protocol numbers can be viewed online at the IANA website:
http://www.iana.org/assignments/protocol-numbers
http://www.iana.org/assignments/port-numbers.

Supported Applications

Supported Multimedia Applications

PIX Firewall supports the following multimedia and video conferencing applications:

- CUseeMe Networks CU-SeeMe
- CUseeMe Networks CU-SeeMe Pro
- CUseeMe Networks MeetingPoint
- Intel Internet Video Phone
- Microsoft NetMeeting
- Microsoft NetShow

- NetMeeting
- RealNetworks RealAudio and RealVideo
- Point-to-Point Protocol over Ethernet (PPPoE)
- VDOnet VDOLive
- VocalTec Internet Phone
- VXtreme WebTheater
- Xing StreamWorks

Supported Protocols and Applications

PIX Firewall supports the following TCP/IP protocols and applications:

- Address Resolution Protocol (ARP)
- Archie
- Berkeley Standard Distribution (BSD)-rcmds
- Bootstrap Protocol (BOOTP)
- Domain Name System (DNS)
- File Transfer Protocol (FTP)
- Generic Route Encapsulation (GRE)
- Gopher
- HyperText Transport Protocol (HTTP)
- Internet Control Message Protocol (ICMP)
- Internet Protocol (IP)
- NetBIOS over IP (Microsoft Networking)
- Point-to-Point Tunneling Protocol (PPTP)
- Simple Network Management Protocol (SNMP)

- Sitara Networks Protocol (SNP)
- SQL*Net (Oracle client/server protocol)
- Sun Remote Procedure Call (RPC) services, including Network File System (NFS)
- Telnet
- Transmission Control Protocol (TCP)
- Trivial File Transfer Protocol (TFTP)
- User Datagram Protocol (UDP)

Copyright © 2001-2004, Cisco Systems, Inc.

TCP Options

Configuration>System Properties>Advanced>TCP Options

The **TCP Options** panel lets you set various parameters for TCP connections.

The following sections are included in this Help topic:

- Field Descriptions

For more information on the TCP protocols, see **IP**.

Field Descriptions

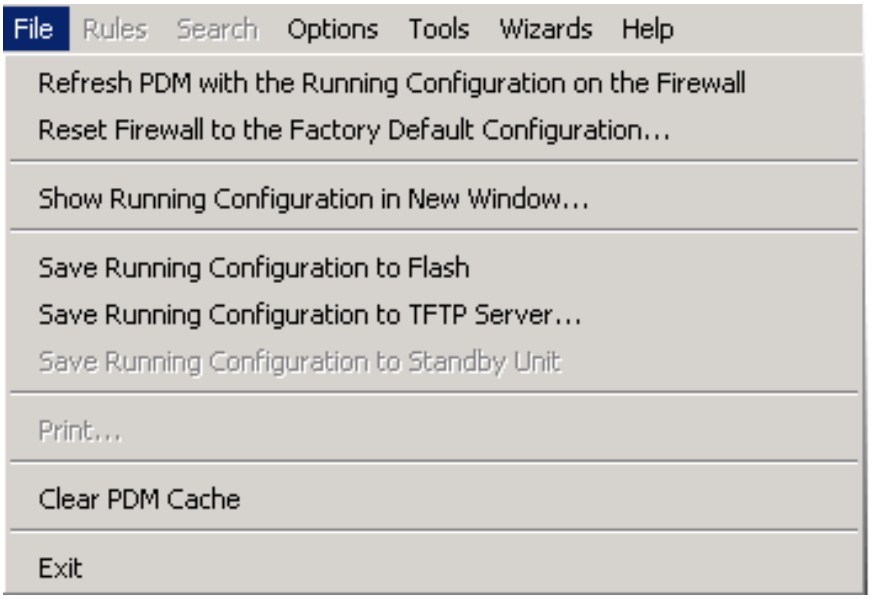
TCP Options panel displays the following fields:

- **Force maximum segment size**—Selecting this check box causes the firewall to enforce a maximum segment size (MSS) for all TCP sessions transiting the firewall. This feature is used primarily to ensure that the TCP session does not experience fragmentation. Should the MSS used for a TCP session exceed the maximum specified, the firewall will rewrite the MSS within the TCP packet to the maximum specified.
- **Force minimum segment size**—Selecting this check box causes the firewall to enforce a minimum segment size (MSS) for all TCP sessions transiting the firewall. This feature is used primarily to avoid attacks based on illegitimately small MSS sizes. Should the MSS used for a TCP session fall below the minimum specified, the firewall will rewrite the MSS within the TCP packet to the minimum specified. The absolute smallest allowed segment size is 48 bytes.
- **Force TCP connection to linger in TIME_WAIT state**—Selecting this check box will force the firewall to retain its TCP connection information/state for at least 15 seconds after the normal TCP **close-down** sequence is seen. This option helps to ensure that both sides of the TCP session receive the close-down packets.
- **Reset inbound**—Selecting this check box causes the firewall to send TCP resets for all TCP sessions that arrive at the outside interface, are attempting to transit the firewall, and are denied by the firewall based on Access Rules. When this option is not selected, the firewall silently discards the packets of all such sessions.
- **Reset outside**—Selecting this check box causes the firewall to send TCP resets for all TCP sessions that arrive at the outside interface, terminate at the outside interface, and are denied by the firewall based on Access Rules. When this option is not selected, the firewall silently discards the packets of all such sessions.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last

time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

File Menu



Refresh

Select **File>Refresh PDM with the Running Configuration on the Firewall** or click **Refresh** to load a copy of the running configuration to PDM. Use refresh to make sure PDM has a current copy of the running configuration.

Reset Firewall to the Factory Default Configuration

The PIX 501 and PIX 506/506E ship with a factory default configuration that provides plug-and-play operation for most standard applications. A copy of the factory default configuration is kept in the firewall, even if other configuration changes are made. You can select **File>Reset Firewall to the Factory Default Configuration** to restore the known good factory default configuration, which is particularly useful for troubleshooting purposes. After the default configuration is restored, you can then quickly test basic connectivity by selecting Tools>Ping. For more information, see Ping and Command Line Interface.

Show Running Configuration in New Window

Select **File>Show Running Configuration in New Window** to display the current running configuration in a new window. This menu item functions similarly to the **show config** command. For more information, see Command Line Interface.

Save Running Configuration to Flash

Select **File>Save Running Configuration to Flash** or click **Save** to write a copy of the running configuration to the Flash memory inside the firewall chassis.

Save Running Configuration to TFTP Server

Select **File>Save Running Configuration to TFTP Server** to store a copy of the current running configuration file on a TFTP server. For more information, see TFTP Server.

Save Running Configuration to Standby Unit

Select **File>Save Running Configuration to Standby Unit** to send a copy of the running configuration file on the primary unit to the running configuration of a failover standby unit. For more information, see Failover.

Note: This menu item is available only when the firewall is configured for failover.

Clear PDM Cache

Select **File>Clear PDM Cache** to clear the copy of PDM that resides in the cache of the local PC hard drive that accessed PDM through a web browser. By default, the firewall keeps a secure copy of PDM in cache for reduced load time. The second time you access PDM, the cached copy loads, instead of loading a new copy.

Exit

Select **File>Exit** to exit PDM.

Copyright © 2001-2004, Cisco Systems, Inc.

Refresh PDM with the Running Configuration on the Firewall

File>Refresh PDM with the Running Configuration on the Firewall

Refresh PDM with the current running configuration by by selecting **File>Refresh PDM with Current Configuration on the Firewall** or by clicking **Refresh** on the button bar.

Copyright © 2001-2004, Cisco Systems, Inc.

Print

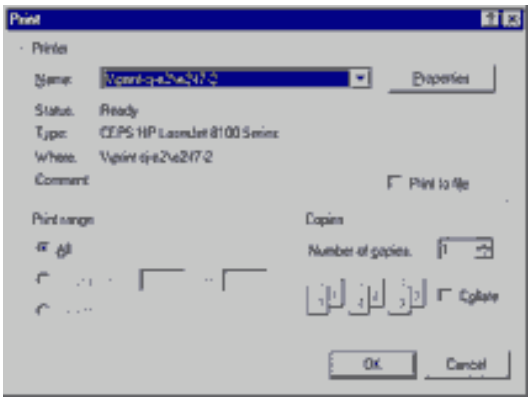
File>Print

1. To begin printing, select **File>Print** or click **Print** on the button bar.

Note: Java Print Permissions
If PDM is running in Netscape Communicator and the user has not yet granted print privileges to the Java applet, a security dialog appears requesting Print privileges. Click **Grant** to grant the applet printing privileges. When using Internet Explorer, permission to print is already granted when you originally accepted the signed applet.

---

2. The **Print** dialog box then appears, which varies depending on your operating



system.

3. In the **Print** dialog box, select the appropriate settings, including:

- Destination printer
- Quality, layout, or other printer-specific settings
- Page orientation

Note: We recommend landscape page orientation when printing rules.

Then click **OK** to print.

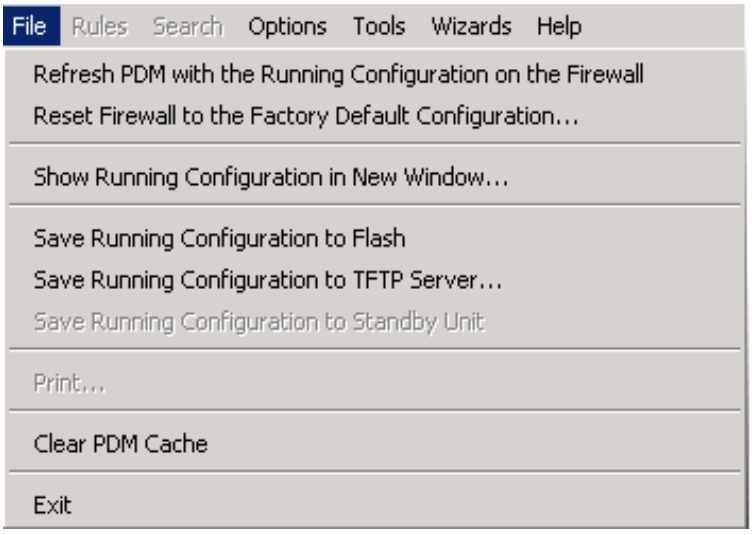
Copyright © 2001-2004, Cisco Systems, Inc.

Reset Firewall to Factory Default Configuration

File>Reset Firewall to Factory Default Configuration

Beginning with Version 6.2, the PIX 501 and PIX 506/506E ship with a factory default configuration, which provides plug-and-play operation for most applications. A copy of the factory default configuration is kept within the firewall, even if other configuration changes are made. You can select **File>Reset Firewall to the Factory Default Configuration** to restore the "known good" factory default configuration, which is particularly useful for troubleshooting purposes. After the default configuration is restored, you can quickly test basic connectivity by selecting **Tools>Ping**.

For more information, see Tools>Ping and Tools>Command Line Interface.



To see the current configuration, select **File>Refresh PDM with the Running Configuration on the Firewall** or **File>Show Running Configuration in New Window**.

To save the current running configuration so that it is used when the firewall is restarted, select **File>Save Running Configuration to Flash**.

Field Descriptions

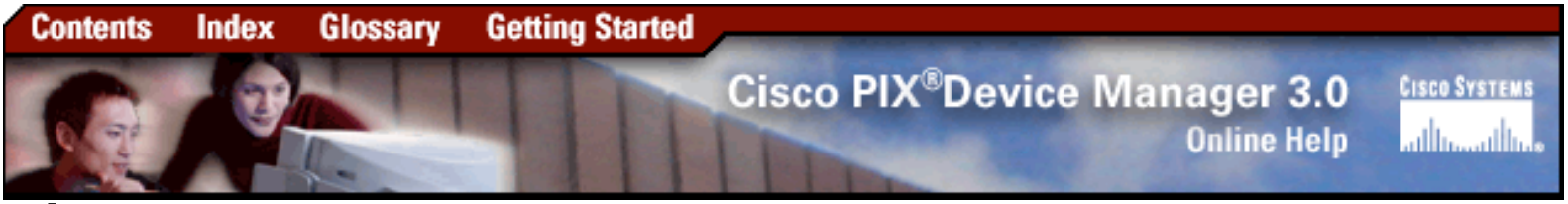
The **Reset Firewall to Factory Default Configuration** panel displays the following fields:

- **Use this address for the inside interface**—Check to enable the IP Address and Subnet Mask fields to be

applied to the inside interface.

- **Inside IP Address**—The IP Address of the inside interface.
- **Inside Subnet Mask**—The mask for the IP address of the inside interface. The default value is 255.255.255.0.
- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.



Ping

Tools>Ping

The **Ping** panel provides a useful tool for verifying the configuration and operation of the firewall and surrounding communications links, as well as basic testing of other network devices.

The following sections are included in this Help topic:

- Field Descriptions
- Using the PDM Ping tool
- Troubleshooting operation of the PDM Ping tool

A ping is the network equivalent of sonar for submarines. A ping is sent to an IP address and it returns an echo, or reply. This simple process enables network devices to discover, identify, and test each other.

The **Ping** tool uses the Internet Control Message Protocol (ICMP) protocol described in RFC-777 and RFC-792. ICMP defines an *echo* and *echo reply* transaction between two network devices, which has become known as a ping. The *echo* (request) packet is sent to the IP address of a network device. The receiving device reverses the source and destination address and sends the packet back as the *echo reply*.

Field Descriptions

The **Ping** panel includes the following fields:

- **IP Address**—The destination IP address for the ICMP echo request packets. Note: If a host name has been assigned in the **Configuration>Hosts/Networks>Basic Information>Host Name** panel, you can use the host name in place of the IP address.
- **Interface**—(Optional). The firewall interface that transmits the *echo* request packets is specified. If it is not specified, the firewall checks the routing table to find the destination address and uses the required interface.
- **Ping Output**—The result of the ping. When you click **Ping**, three attempts are made to ping the IP address and three results display the following fields:
  - **Reply IP address/Device name**—The IP address of the device pinged or a device name, if available. The name of the device, if assigned Hosts/Networks, may be displayed, even if **NO response** is the result.
  - **Response received/NO response received**—
    - **Response received**—the result if an *echo reply* was returned from the destination IP address specified.
    - **NO response received**—the result if no *echo reply* was returned before the specified timeout.
  - **Response time/timeout (ms)**—When the ping is transmitted, a millisecond timer starts with a specified maximum, or timeout value. This is useful for testing the relative response times of different

routes or activity levels, for example.

- **Response received**—When an *echo reply* is received, the timer stops and its value is displayed.
- **NO response received**—If an *echo reply* is not received before the timeout value is reached, the timeout value is displayed.

- **Example Ping Output**

```
10.1.1.2 NO response received -- 1000ms
10.1.1.2 NO response received -- 1000ms
10.1.1.2 NO response received -- 1000ms

If a name is assigned in Hosts/Networks>Host Name:

Router_1600 response received -- 0ms
Router_1600 response received -- 0ms
Router_1600 response received -- 30ms
```

- **Ping**—Sends an ICMP *echo* request packet from the specified or default interface to the specified IP address and starts the response timer.
- **Close**—Closes the Ping tool.
- **Help**—Provides more information about the Ping tool

Using the Ping Tool

The Ping tool uses the Internet Control Message Protocol (ICMP) protocol described in RFCs 777 and 792. Sending an ICMP *echo* request packet to an IP address is a "ping". An "echo" is an ICMP *echo reply* packet returned from the receiving device.

PIX Firewall administrators can use the PDM Ping tool as an interactive diagnostic aid in several ways, for example:

Loopback testing of two interfaces—A ping may be initiated from one interface to another on the same Cisco firewall unit, as an external loopback test to verify basic "up" status and operation of each interface.

Pinging *to* a firewall interface—An interface on another Cisco firewall may be pinged by the Ping tool or another source to verify that it is up and responding.

Pinging *through* a PIX Firewall—Ping packets originating from the Ping tool may pass *through* an intermediate PIX Firewall unit on their way to a device. The echo packets will also pass through two of its interfaces as they return. This procedure can be used to perform a basic test of the interfaces, operation, and response time of the intermediate unit.

Pinging to test questionable operation of a network device—A ping may be initiated from a firewall interface to a network device which is suspected to be functioning improperly. If the interface is configured properly and an echo is not received, there may be problems with the device.

Pinging to test intermediate communications—A ping may be initiated from a firewall interface to a network device which is known to be functioning properly and returning echo requests. If the echo is received, the proper operation of any intermediate devices and physical connectivity is confirmed.

Troubleshooting Operation of the Ping Tool

When pings fail to receive an echo, it may be the result of a configuration or operational error in a Cisco firewall unit, and not always due to "NO response" from the IP address being pinged. Before using the **Ping** tool to ping *from*, *to* or *through* a firewall interface, verify the following:

Basic interface checks

Verify that interfaces are configured properly in Configuration>System Properties>Interfaces and/or using the CLI **show interfaces** command from Tools>CLI.

Check each interface physically for good mechanical and electrical connectivity —cables are connected, link indicators are green, and any passive devices, such as hubs are operational.

Verify that devices in the intermediate communications path, such as switches or routers, are properly delivering other types of network traffic.

Make sure that traffic of other types from "known good" sources is being passed. Use the **show interface** command from Tools>CLI tool or **Monitoring>Interface Graphs**.

On certain PIX Firewall models with a factory default configuration, you may find it useful to backup the current running configuration and then use **File>Reset to Factory Default Configuration** to restore a "known good" configuration to test connectivity and perform troubleshooting.

Pinging *from* a firewall interface—For basic testing of an interface, a ping may be initiated from a firewall interface to a network device which, by other means, is known to be functioning properly and returning echoes via the intermediate communications path.

Verify receipt of the ping from the firewall interface by the "known good" device. If it is not received, there may be a problem with the transmit hardware or configuration of the interface.

If the firewall interface is configured properly and it does not receive an echo from the "known good" device, there may be problems with the interface hardware receive function. If a different interface with "known good" receive capability can receive an echo after pinging the same "known good" device, the hardware receive problem of the first interface is confirmed.

Pinging *to* a firewall interface—When attempting to ping *to* a firewall interface, verify that pinging response (ICMP *echo reply)*, is enabled for that interface in the Configuration>System Properties>Administration>ICMP panel. When pinging is disabled, the firewall cannot be detected by other devices or software applications, and will not respond to the PDM Ping tool.

Pinging *through* the firewall

First, verify that other types of network traffic from "known good" sources is being passed through through the firewall unit. Use **Monitoring>Interface Graphs**, or an SNMP management station.

To enable internal hosts to ping external hosts, ICMP access must be configured correctly for both the inside and outside interfaces in **Configuration>Access Rules**.

Copyright © 2001-2004, Cisco Systems, Inc.

Interfaces

Configuration>System Properties>Interfaces

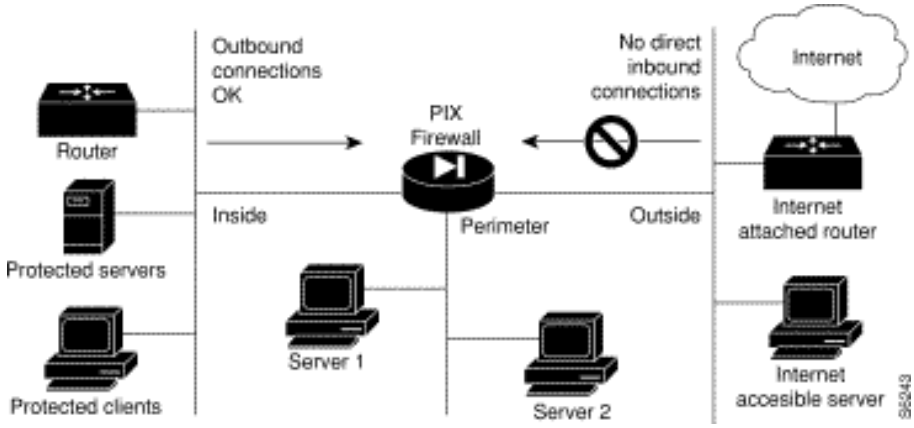
The **Interfaces** panel lets you enable, disable, and/or edit the configuration of network interfaces.

The following sections are included in this Help topic:

- Firewall Interfaces
- Important Notes
- Monitoring Interfaces
- VLANs
- Field Descriptions
- Add/Edit Interface
- Add/Edit Interface>Properties
- Add/Edit Interface>PPPoE>Advanced
- Adding an Interface
- Enabling, Disabling, and Editing Interfaces
- Deleting an Interface
- Inside Interface (ethernet1)>Add/Edit
- Outside Interface (ethernet0)>Edit
- Outside Interface (ethernet0)>Edit>Properties
- Outside Interface (ethernet0)>Edit>PPPoE>Advanced
- Setting Up LANs
- Applying Changes

Firewall Interfaces

The firewall requires that you configure and then enable each interface which will be active. Inactive interfaces can be disabled. When disabled, the interface will not transmit or receive data, but the configuration information is retained.



The physical location of each interface and corresponding connector or virtual connector on the firewall unit can be identified by their **Interface Name** and **Hardware ID** name, such as ethernet0 or ethernet, or their **VLAN ID**, if VLAN interfaces are supported.

The **Interface Name** is a logical name that relates to how it is used in your network configuration. For example, **inside** (connects to your internal network) or **outside** (connects to an external network or the public Internet).

In addition to their names, this panel displays and lets you **edit** additional configuration information required for each interface. Your configuration edits are captured by PDM but not sent to the firewall unit until you click **Apply**.

Note: The Cisco PIX Firewall 506 and Cisco PIX Firewall 506E support VLANs.

▲

Important Notes

1. **Failover—Configuration>Systems Properties>Failover** and **Configuration>Systems Properties>Interfaces** must be configured together to support Stateful Failover and/or LAN-based Failover**.** For more information, see **Configuration>Systems Properties>Interfaces and Failover**.
2. **Speed—**Speed settings for interfaces may not be changed for any interface if Failover is enabled. Do not use the **Auto** (automatic speed selection) setting for any interface when using failover.
3. **Mask—**To avoid routing problems, the firewall defaults to 255.255.255.255 for the network mask. IP addresses and masks are usually provided together by your ISP or network administrator. Please set the correct mask for the number of static IP addresses assigned to you by your ISP or network administrator. For more information see, **More IP>Mask**.

▲

Monitoring Interfaces

You can monitor interfaces using **Monitoring>Interface Graphs**. Using **Tools>CLI**, the **show interface** command provides additional useful information about interface configurations.

The following is sample output from the **show interface** command:

```
show interface

interface ethernet0 "outside" is up, line protocol is up
Hardware is i82559 ethernet, address is 0050.54ff.3772
IP address 172.23.59.230, subnet mask 255.255.255.224
MTU 1500 bytes, BW 10000 Kbit half duplex
1370126 packets input, 138813980 bytes, 0 no buffer
Received 40491 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
2482258 packets output, 1682123205 bytes, 0 underruns
0 output errors, 8259 collisions, 0 interface resets
0 babbles, 0 late collisions, 1179 deferred
0 lost carrier, 0 no carrier
input queue (curr/max blocks): hardware (128/128) software (0/6)
output queue (curr/max blocks): hardware (2/6) software (0/4)


interface ethernet1 "inside" is up, line protocol is up
Hardware is i82559 ethernet, address is 0050.54ff.3773
IP address 10.1.1.1, subnet mask 255.255.255.0
MTU 1500 bytes, BW 10000 Kbit full duplex
279855 packets input, 26155384 bytes, 0 no buffer
Received 274299 broadcasts, 0 runts, 0 giants
1 input errors, 0 CRC, 1 frame, 0 overrun, 0 ignored, 0 abort
70405 packets output, 11885724 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collisions, 0 deferred
0 lost carrier, 0 no carrier
input queue (curr/max blocks): hardware (128/128) software (0/1)
output queue (curr/max blocks): hardware (0/2) software (0/1)


interface ethernet2 "pix/intf2" is up, line protocol is down
Hardware is i82559 ethernet, address is 00d0.b792.409d
IP address 127.0.0.1, subnet mask 255.255.255.255
MTU 1500 bytes, BW 10000 Kbit full duplex
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
1 packets output, 64 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collisions, 0 deferred
0 lost carrier, 0 no carrier
```

```
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/2) software (0/1)
```

VLANs

Usually, firewalls have a physical hardware interface with a physical connector for each Local Area Network (LAN) to which they are connected, and a relatively small number of interfaces. For example, the Cisco PIX Firewall provides between 2 and 10 interfaces, depending upon the model. Typically multiple physical switch interfaces are combined into one or more logical or virtual LANs (VLANs) to simplify configuration management and improve performance.

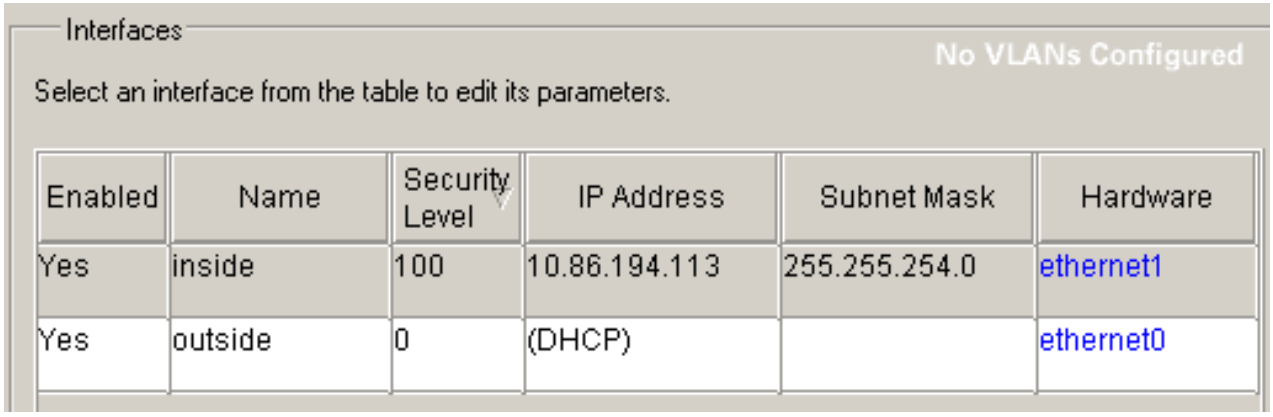
VLANs (virtual LANs) allow arbitrary combination of distinct physical LANs to be logically combined to appear as a single LAN network. Traffic within a VLAN is bridged/switched, while traffic between VLANs needs to be routed.

Security policies, such as **access control**, **nat/static**, and **AAA**, are enforced based on the two interfaces and their relative security levels, as they are with with normal hardware interfaces.

The change from hardware interface to logical VLAN interface should be transparent to CLI commands other than the **interface** and **nameif** commands.

Field Descriptions

Interfaces Table



Interfaces Table for VLAN Support

Enabled	Name	Security Level	IP Address	Subnet Mask	VLAN	Hardware
Yes	inside	100	172.23.58.166	255.255.255.0	native	ethernet1
Yes	test	52	1.1.1.1	255.255.0.0	vlan2	ethernet1
Yes	mydmz	11	192.168.1.1	255.255.255.0	native	ethernet2
Yes	outside	0	(PPPoE)		native	ethernet0

The **Interfaces** table provides the following information:

- **Enabled—**Enables the interface to the state of administratively up.
- **Name**—The logical name of the interface which relates to your use, such as inside or outside.

  Note: Unless you are an expert user, do not change the interface name.

- **Security Level**—The security level (1-99) the interface will enforce.
- **IP Address**—The IP Address of the interface.
- **Subnet Mask**—The mask for the IP address of the interface.

  Note: To avoid routing problems, the firewall defaults to 255.255.255.255 for the network mask. IP addresses and masks are usually provided together by your ISP or network administrator. Please set the correct mask for the number of static IP addresses assigned to you by your ISP or network administrator. For more information, see Uses for Subnet Masks.
- **VLAN**—Displays the ID of the VLAN used for this interface.
- **Hardware**—Displays the hardware name of the interface located on your PIX Firewall unit. The **Hardware Port** dialog box lets you view or modify hardware port attributes, such as speed. You can access the **Hardware Port** dialog box by selecting the desired hardware ID or by selecting **Properties** in the right-click pop-up menu or in the **Add/Edit Interface** dialog box.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Add**—Opens the **Add** dialog box.
- **Edit**—Opens the **Edit** dialog box.
- **Delete**—Deletes the selected item.

  Note: Do not delete an interface unless you know all parts of the configuration which will be affected. For example, Rules may require the interface to be defined.

▲

Add/Edit Interface

The **Edit Interface** panel provides the following information:

- **VLAN ID—**Lets you assign a VLAN ID for this interface, if the firewall supports VLANs.
- **Enable Interface**—Select to enable or disable this interface.

- **Interface Name**—Displays the logical interface name of the interface which is, by default, called *inside* on your firewall unit. The logical interface name of the interface relates to your use, such as inside, outside, or intf2.

  Note: Unless you are an expert user, do not change the interface name.
- **Security Level**—The security level (1-99) the interface will enforce.
- **IP Address**—The IP Address of the interface.
- **Subnet Mask**—The mask for the IP address of the interface.

  Note: In order to avoid routing problems, the firewall defaults to 255.255.255.255 for the network mask. IP Addresses and Masks are usually provided together by your ISP or network administrator. Please set the correct mask for the number of static IP Addresses assigned to you by your ISP or network administrator. For more information, see Uses for Subnet Masks.

Add/Edit Inside Interface>Properties

- **Hardware Port**
  - **Enable**—Enables or disables the hardware port.
  - **Speed and duplex mode**—The speed of the physical layer for this interface and the duplex mode.

    Note: Speed may not be changed if failover is enabled. The **Auto** setting cannot be used with failover.
  - **MTU**—Maximum transmission unit (MTU) of the hardware port.
  - **OK**—Accepts changes and returns to the previous panel.
  - **Cancel**—Discards changes and returns to the previous panel.
  - **Help**—Provides more information.

Add/Edit Interface>PPPoE>Advanced

- **Obtain IP Address using PPPoE**—The default method of obtaining an IP address is using PPPoE.
- **Specify an IP address**—Select to enter a static IP Address for the **outside** interface
  - **IP Address**—The static IP address for the **outside** interface
  - **Subnet Mask**—The subnet mask for the **outside** interface

    Note: To avoid routing problems, the firewall defaults to 255.255.255.255 for the network mask. IP addresses and masks are usually provided together by your ISP or network administrator. Please set the correct mask for the number of static IP addresses assigned to you by your ISP or network administrator. For more information, see Uses for Subnet Masks.

Adding an Interface

Follow these steps to **add** an interface:

1. Click **Add** to open the **Interface** panel.
2. Enter the interface information. See Field Descriptions for additional information.
3. Click **Properties** to open the **Hardware Port** dialog box.
4. Configure the hardware port. See Field Descriptions for additional information.
5. Click **OK** to return to the **Interface** panel.
6. Click **OK** to return to the **Interfaces** table.
7. Click **Apply**.

Enabling, Disabling, and Editing Interfaces

Follow these steps to **enable**, **disable**, and/or **edit** the configuration of an interface:

1. Select a interface from the table on the **Interface** panel.
2. Click **Edit** to open the **Edit Interfaces** panel.
3. Make any necessary changes to the fields provided. See Field Descriptions for additional information.
4. Click **Enable Interface** to enable or disable the interface. When disabled, the configuration information is retained, but the interface will not transmit or receive.
5. To return to the previous panel, click one of the following:
   - **OK**—Accepts changes and returns to the previous panel.
   - **Cancel**—Discards changes and returns to the previous panel.
   - **Help**—Provides more information.
6. After returning to the **Interfaces** panel, changes will not be applied unless you click one of the following:
   - **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
   - **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Deleting an Interface

Follow these steps to **delete** an interface:

1. Select a interface from the Interfaces table.
2. Click **Delete**.
3. Click **OK** to confirm.
4. Click **Apply**.

Setting Up VLANs

Setting up VLAN interfaces involves two separate configuration tasks performed on the switch console and the

firewall console, respectively. On the switch side, you create a vlan-group, which has all the secure VLANs to be protected, and apply the group to the firewall. Because this is outside the firewall, it is not managed by PDM. On the firewall side, you need to create interfaces corresponding to the VLANs assigned to the switch using the **nameif** command. Assigned VLANs can be obtained by the **show vlan** command. You can use PDM to manage these interfaces.

Once created, the VLAN interfaces should be populated to other panels in PDM so you can configure translation rules, access rules, and other policies.

VLANs can be dynamically added or removed from a vlan-group. PDM will show you the assigned VLANs, and which VLAN interfaces are no longer valid so you can make corrections if needed.

Applying Changes

Changes to the table made by **Add**, **Edit**, or **Delete** are not immediately applied to the running configuration. You must click one of the following buttons to apply or discard changes:

1. **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
2. **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

More ▸ Configuration Changes

The following is important information about how and when the running configuration is modified by PDM or CLI console sessions, and how to update Flash memory, TFTP servers, and failover standby units.

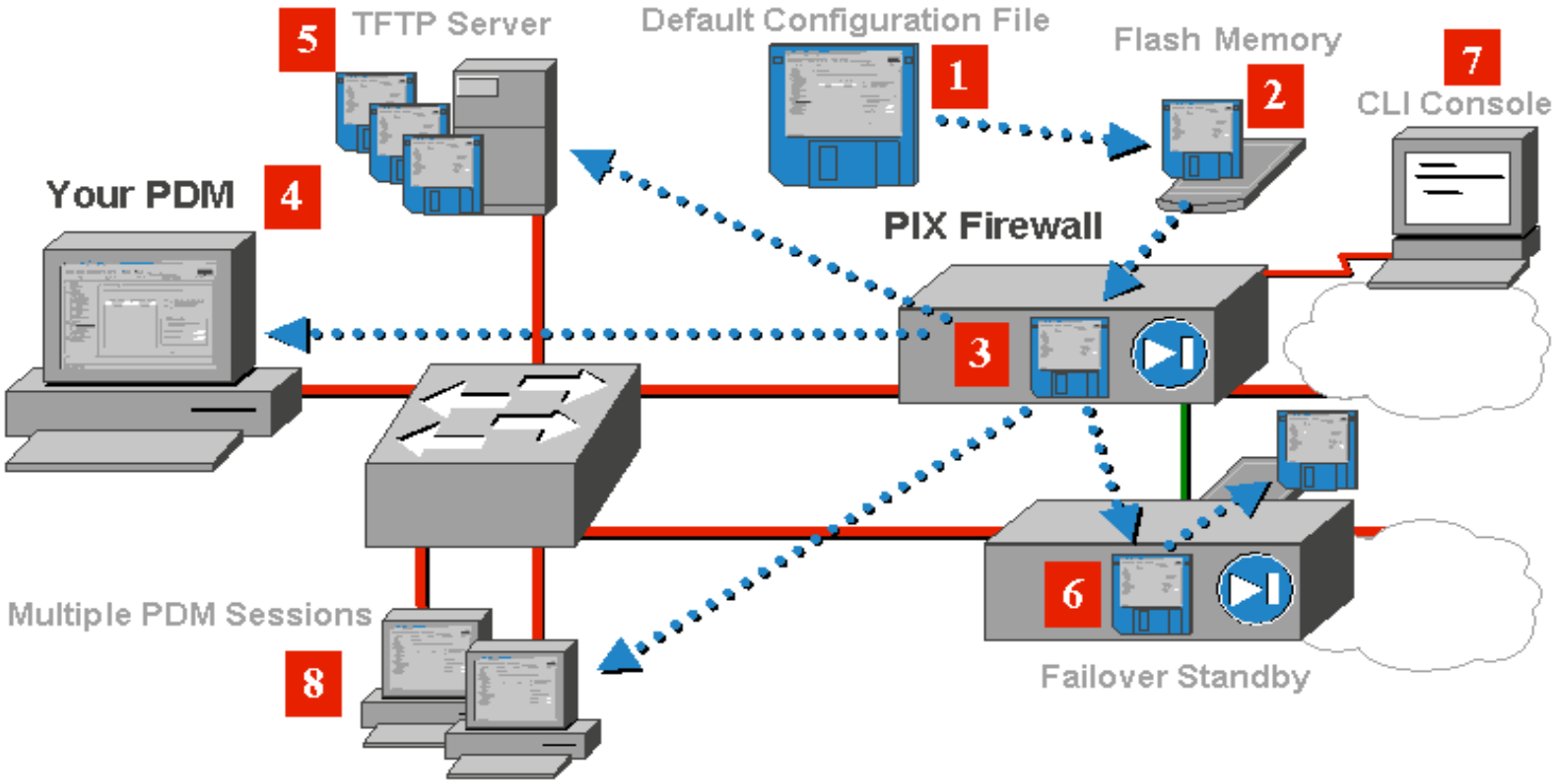
The following sections are included in this Help topic:

- Configuration File Terminology
- How and When Changes to Configuration Files are Applied
- CLI console sessions
- Multiple PDM and CLI Console Sessions
- Cisco Secure Policy Manager (CSPM) and PDM

When deployed for operation in your network, there are multiple copies of a PIX Firewall configuration file. There are the following are areas where a configuration can be stored:

- **Internal**
  - Running configuration
  - Flash memory
- **External**
  - TFTP server
  - Failover standby unit

Firewall Configuration File Terminology



The numbers in the following list correspond to the preceding figure.

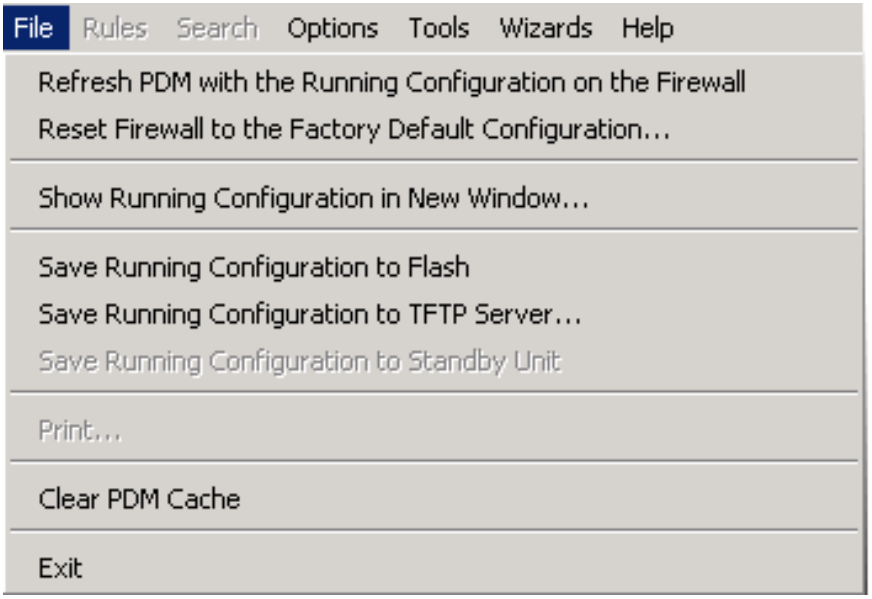
1. **Default configuration, factory default configuration**—The configuration file which shipped with the Cisco firewall unit in Flash memory. This file is loaded into RAM at boot and becomes the running configuration. See **File>Reset Firewall to Factory Default Configuration.**
2. **Flash memory file**—A running configuration copy, written by **File>Save Running Configuration to Flash** to nonvolatile storage**.** This file is loaded into RAM at boot or by command to become the running configuration.
3. **Running configuration**—The configuration currently running in RAM on the Cisco firewall unit which determines its operational characteristics.
4. **PDM session copy**—Each PDM session displays a copy of the running configuration made at the time it opened or the last time **Refresh** was clicked. Note: Multiple PDM sessions may be in operation at the same time and each will have a copy of the running configuration at the time their PDM opened or Refresh was clicked.
5. **TFTP server file**—Copies of the running configuration stored on a TFTP server by **File>Save Running Configuration to TFTP Server** which can also be download to become the running configuration.
6. **Failover Standby Unit**—A copy of the running configuration in the primary unit which becomes the running configuration of a failover standby unit using **File>Save Running Configuration to standby unit**. A copy of the running configuration of the standby unit can also be stored in its Flash memory by using **File>Save Running Configuration to Flash**.
7. **CLI Console (Terminal) Sessions**—Administrative sessions using the command line interface (CLI) to affect the running configuration immediately. A PC with terminal emulation software is connected directly to the console port or by a network. Refer to CLI console sessions.
8. **Multiple PDM Sessions**—The PIX Firewall can support multiple PDM sessions at the same time. If other PDM sessions make changes to the running configuration, you will not see them in your PDM session until you click **Refresh**. You may see if there are other PDM sessions active by using **Monitoring>PDM Users.**

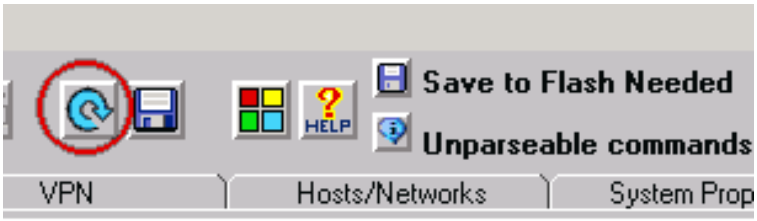
Help>About Cisco PIX Firewall will display, among other useful things, which user last changed the configuration:

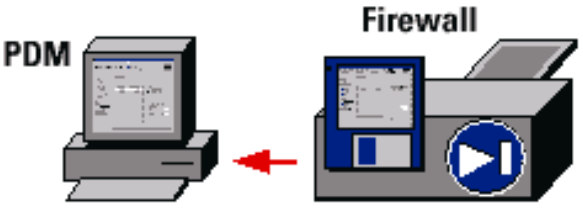
```
Configuration last modified by Robin_Smith at 00:48:40.498 UTC Tue May 14
2002
```

Note: For more information about the CLI commands used by each PDM screen, see **CLI Commands Used by PDM Screens**.

How and When Changes to Configuration Files are Applied







1. **Add**, **Edit**, **Delete, Enable, Disable**—Any changes made in a PDM panel do not immediately affect the running configuration.
2. **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover

standby firewall unit. See Configuration Changes.

3. **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open. The running configuration is not affected.
4. **File>Refresh PDM with Current Configuration from PIX** or —Loads a fresh copy of the configuration into your PDM.
5. **File>Reset Firewall to Factory Default Configuration**—Reloads the factory default configuration as the running configuration.
6. **File>Save Running Configuration to Flash** or —Writes a copy of the the running configuration to the Flash memory on the PIX Firewall.
7. **File>Save Running Configuration to TFTP Server**—Writes a copy of the running configuration to a TFTP server. Refer to **System Properties> Administration>TFTP Server** for more information.
8. **File>Save Running Configuration to standby unit**—Copies the running configuration of the primary firewall to the running configuration of another PIX Firewall configured as a failover standby unit.
9. **Tools>PDM Command Line Interface**—Changes made with the PDM CLI tool affect the running configuration *immediately*.
10. Other CLI Console Sessions—Changes made by other CLI console sessions affect the running configuration immediately.

CLI Console Sessions

In addition to PDM, PIX Firewall administrators may use command line interface (CLI) console sessions. One of the following types of preconfigured connections must be used for CLI console sessions:

1. Serial console port—PC with serial interface and terminal emulation software connected directly to the PIX Firewall console port.
2. Telnet protocol—A network connection using the Telnet protocol.
3. PDM/HTTPS protocol—A network connection using the HTTPS (HTTP over SSL) protocol for **Tools>CLI**. Note: PDM uses HTTPS for all communication with the PIX Firewall.
4. Secure Shell (SSH) protocol—A network connection using the Secure Shell (SSH) protocol.

Before configuring your firewall from the PDM CLI tool, we recommend that you review the *Cisco PIX Firewall Command Reference* for your respective version. Refer also to Password, Authentication.

For more information about the CLI commands used by each PDM screen, see **CLI Commands Used by PDM Screens**. **Help>About Cisco PIX Firewall** will display, among other useful things, which user last changed the configuration.

```
Configuration last modified by Joe_Smith at 00:48:40.498 UTC Tue May 14
2002
```

Multiple PDM and CLI Console Sessions

Changes made from **Tools>CLI** or other CLI console sessions take effect *immediately* in the running configuration. However, the changes will not be reflected in your PDM session until you exit the CLI tool and click **Refresh** or **File>Refresh PDM with Current Configuration from Firewall**.

You may view active PDM and CLI console sessions in the **Monitoring** panel:

- Monitoring>PDM Users
- Monitoring>Secure Shell Sessions
- Monitoring>Telnet Console Sessions

If any other PDM sessions are in operation, when you make changes using your PDM CLI tool, your changes will affect all the other PDM sessions when they click **Refresh**.

Refer also to Serial, Telnet, PDM/HTTPS, SSH, Password, Authentication.

Caution: PDM allows multiple PCs or workstations to each have one browser session open with the same firewall. However, only one session per browser per PC or workstation is supported for a particular firewall .

Cisco Secure Policy Manager (CSPM) and PDM

Caution: If you are using both CSPM and PDM to manage the same Cisco firewall unit, changes made by PDM can be lost.

CSPM keeps its own internal copy of the configuration file currently running in a Cisco firewall unit it manages and assumes that it is the only entity making changes. If changes are made by PDM (or any other method) to a firewall that CSPM is also managing, when it next checks the status of that firewall, CSPM will attempt to verify that the configuration matches the internal copy it maintains for that firewall. If it does not match, CSPM will change the running configuration on that Cisco firewall unit back to the "known good" copy it maintains for that unit.

While you can use PDM to modify the configuration of a firewall that is also managed by CSPM, any modification that you make with PDM will be negated the next time CSPM checks that firewall.

Copyright © 2001-2004, Cisco Systems, Inc.

TFTP Server

Configuration>System Properties>Administration>TFTP Server

The **TFTP Server** panel lets you configure the firewall to save its configuration to a file server using the Trivial File Transfer Program (TFTP).

Note: This panel does not write the file to the server. Configure the firewall for using a TFTP server in this panel, then click File>Save Running Configuration to TFTP Server.

The following sections are included in this Help topic: :

- TFTP Servers and the Firewall
- Field Descriptions
- Applying Changes

TFTP Servers and the Firewall

TFTP is a simple client/server file transfer protocol described in RFC783 and RFC1350 Rev. 2. This panel lets you configure the firewall as a TFTP *client* so that it can transfer a copy of its running configuration file to a TFTP *server* using File>Save Running Configuration to TFTP Server or Tools>Command Line Interface. In this way, you can back up and propogate configuration files to multiple PIX firewalls.

This panel uses the **configure net** command to specify the IP address of the TFTP server, and the **tftp-server** command to specify the interface and the path/filename on the server where the running configuration file will be written. Once this information is applied to the running configuration, PDM File>Save Running Configuration to TFTP Server uses the **write net** command to execute the file transfer.

The firewall supports only one TFTP server. The full path to the TFTP server is specified in **Configuration>System Properties>Administration>TFTP Server**. Once configured here, you can use a colon (:) to specify the IP address in the CLI **configure net** and **write net** commands. However, any other authentication or configuration of intermediate devices necessary for communication from the firewall to the TFTP server is done apart from this function.

The **show tftp-server** command lists the **tftp-server** command statements in the current configuration. The **no tftp**

server command disables access to the server.

For more information about TFTP, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

Field Descriptions

The **TFTP** panel provides the following fields:

- **Enable**—Click to select and enable these TFTP server settings in the configuration.
- **Interface**—Select the name of the firewall interface which will use these TFTP server settings..
- **IP Address**—Enter the IP address of the TFTP server.
- **Path/filename**—Type in the TFTP server path, beginning with "/" (forward slash) and ending in the file name, to which the running configuration file will be written.

  Example TFTP server path: **`/tftpboot/pixfirewall/config3`**

  Note: The path must begin with a forward slash (/).

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

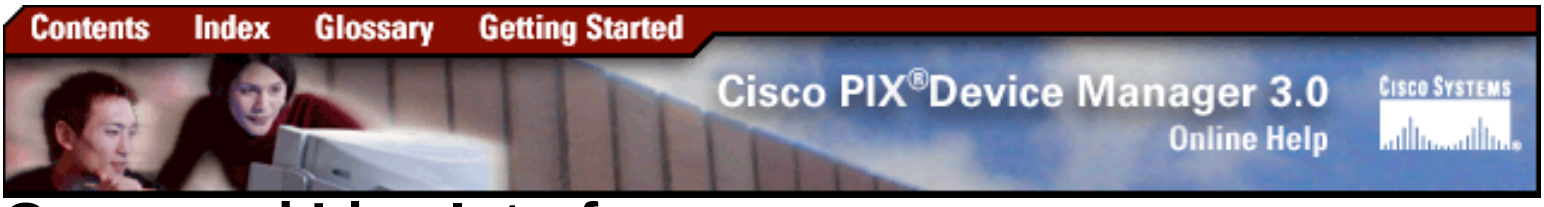
For more information about TFTP, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

Applying Changes

Changes to the table made by **Add**, **Edit**, or **Delete** are not immediately applied to the running configuration. You must click on one of the following buttons to apply or discard changes:

1. **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
2. **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.



Command Line Interface

Tools>Command Line Interface

The **Command Line Interface** (CLI) panel provides a text-based tool for sending commands to the firewall and viewing the results.

The following sections are included in this Help topic:

- Configuration Updates, CLI Console Sessions, and PDM
- Important Notes
- Field Descriptions
- Entering Command Lines
- Entering Multiple Commands
- Command Syntax
- Tips on Using CLI Commands
- Command Summary
- Command Reference and Access Modes

You can enter commands as a single line in the **Command** box and, optionally, enter subcommands in the **Subcommand** box. A subcommand is a key word that is related to the main command. Click **Send** or press the keyboard **Enter** key, to transmit the command(s) to the firewall. You can then view the response of the command(s) you entered in the **Response** box. The command and resulting text are retained in the **Response** box, as a record of the session, until you erase it by clicking **Clear Response** at the bottom of the screen.

In the **Multiple Line Commands** panel, you can enter multiples lines of commands or paste them in from other sources, like a text file. Click **Send** to send and process multiple commands at once. If an error occurs, the offending command is skipped and the remaining commands are processed anyway. A message displays in the **Response** box to let you know what, if any, errors were encountered as well as other pertinent information.

Configuration Updates, CLI Console Sessions, and PDM

Multiple administrative users can update the running configuration of the firewall, and there are multiple ways in which they can do it. Before using the PDM CLI tool to make configuration changes, follow these precautions:

1. **Check for Other Active Administrative Sessions**—If more than one user is configuring the firewall at the same time, the last changes take effect. (Click the **Monitoring** tab to view other administrative sessions that are currently active on the same firewall.)
2. **Understand Update Procedures**—Understand the effect of different administrative methods for changing and viewing the running configuration.

UPDATES TO THE RUNNING CONFIGURATION

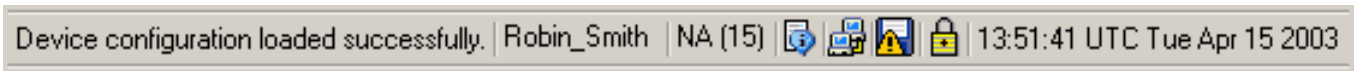
ADMIN TOOL	CONFIG CHANGES APPLIED	VIEW CHANGES IN CLI	VIEW CHANGES IN PDM
PDM	Apply Immediate effect on PDM screens and firewall	`show running-config`	1. or **File>Refresh...** 2. PDM screens updated 3. **File>Show Running Configuration...**
CLI Console Session	**Enter** Immediate effect on firewall	`show running-config`	1. or **File>Refresh...** 2. PDM screens updated 3. **File>Show Running Configuration...**.
PDM CLI Tool	Send Immediate effect on firewall and PDM CLI Tool	`show running-config`	1. Exit CLI Tool 2. or **File>Refresh**... 3. PDM screens updated 4. **File>Show Running Configuration...**
CSPM	CSPM overrides other changes with its own copy of the config from its last session.	`show running-config`	1. or **File>Refresh...** 2. PDM screens updated 3. **File>Show Running Configuration...**

- **PDM**—PDM sessions make changes to the running configuration when you click **Apply**. PDM views the running configuration as it was when PDM started up, or the last time you clicked **Refresh** or clicked **File>Refresh.**
- **CLI console session**—Administrators might use SSH, Telnet, or a serial connection for a CLI console session, in addition to PDM. You can make changes and view them immediately by entering the **show running-config** command. For more information, see Serial, Telnet, PDM/HTTPS, SSH, Password, and Authentication.
- **PDM CLI Tool—** The PDM CLI tool is another type of CLI console session. You can make changes and view them immediately by entering the **show config** command. However, any changes made in using the CLI tool are not reflected in PDM until you exit the CLI tool and click **File>Refresh**. If any other PDM sessions are in operation when you make changes using the PDM CLI tool, your changes will effect all other PDM sessions when you click the **Refresh** button or click **File>Refresh**.
- **CSPM (Cisco Secure Policy Manager)**—CSPM is a management tool used to manage multiple products, including the PIX Firewall. CSPM keeps an internal copy of the configuration file currently running in the firewall it is managing. Also, CSPM assumes that it is the only management tool making changes. If changes are made by PDM (or any other method) to a firewall that CSPM is also managing, the next time it checks the status of that firewall, CSPM attempts to verify that the configuration matches the internal copy it maintains for that firewall. If it does not match, CSPM changes the running configuration on that firewall back to the known good internal copy it maintains for that device. While you can use PDM to modify the configuration of a firewall that is also managed by CSPM, any modification that you make with PDM will be negated the next time CSPM checks the status of that firewall.

For additional information, see How and When Changes to Configuration Files are Applied and **Options>Show Unparsed Commands on Firewall**.

Important Notes

1. **Access Modes and Command Reference**—Before configuring your firewall using the PDM CLI tool, review the administrative access modes in the *Cisco PIX Firewall Command Reference* for your respective version of software.
2. For more information about the CLI commands used by each PDM screen, see CLI Commands Used by PDM Screens.
3. Review your privilege level in the status bar at the bottom of the main PDM window to ensure you have privileges to execute privileged-level CLI commands.



4. **Cisco IOS and PIX CLI Command Syntax**—The PIX Firewall CLI uses similar syntax and other conventions as the Cisco IOS CLI, but the PIX Firewall operating system is not a version of Cisco IOS software. Do not assume that a Cisco IOS CLI command works, or functions the same, on the PIX Firewall.
5. **Multiple Administrative Sessions**—Refer to CLI Console Sessions and PDM Configuration Updates, Multiple PDM and CLI Console Sessions for more information.
6. **Checking the Running Configuration**—To view the current configuration, click File>Refresh PDM with Current Configuration on Firewall..., File>Show Running Configuration in New Window, or enter the **show running-config** command.

Field Descriptions

The **Command Line Interface** (CLI) panel includes the following fields:

- **Subcommand** check box—Enables the **Subcommand** box.
- **Command**—Lets you enter or paste a main command in the **Command** box. Enter the related subcommand(s) in the **Subcommand** box, which is active only after you select the **Subcommand** check box.
- **Response**—Displays the results of the commands you entered in the **Command** box. For help on any command, enter the **?** command to display a brief description of Help for that command in the **Response** box.
- **Send**—Sends all commands to the firewall at once, then returns to the main CLI panel where the **Response** box displays the results.
- **Clear Response**—Clears all text displayed in the **Response** box.
- **Close**—Closes the **Command Line Interface** window.
- **Help**—Provides more information about using the CLI tool.
- **Multiple Line Command**—Opens the **Multiple Line Command** box, which lets you enter commands manually, paste commands from other sources, or edit multiple line commands.

The **Multiple Line Command** panel includes the following fields:

- **Multiple Line Command**—Lets you enter commands manually or paste commands from other sources.
- **Send**—Sends commands to the firewall, then returns to the **Command Line Interface** window where the **Response** box displays the results.
- **Cancel**—Returns to the **Command Line Interface** window without sending the command(s) you entered.
- **Help**—Provides more information about using multiple line commands.

Entering Command Lines

Follow these steps to enter and view results of single line commands, with or without subcommands:

1. Select the **Subcommand** check box, to enter subcommands for a main command. Skip this step if there are no subcommands.
2. Type or paste a main command in the **Command** box.
3. If the **Subcommand** check box is selected, type or paste the subcommand in the **Subcommand** box.
4. Click **Send** or press the **Enter** key on your keyboard to send the command to the firewall. The results of the command display in the **Response** box.

Note: Changes from the PDM CLI tool are applied immediately in the running configuration. However, the changes are not reflected in PDM until you exit the CLI tool and click **File>Refresh**, or click the **Refresh** button.

Entering Multiple Commands

Follow these steps to enter and view results of multiple commands:

1. Send multiple lines of commands, or a list of commands, to the firewall in two ways, typing or pasting:
    - **Typing**—Unlike the single line **Command** box, the **Enter** key on your keyboard does not send the command to the firewall. Instead, pressing **Enter** terminates the line and returns the cursor to the left margin of the next line. Type the first command in the **Multiple Line Command** box and press **Enter** to return to the left margin. Type the next command, and press **Enter**. Repeat until all commands are entered in the command list. Within the **Multiple Line Command** box, you can edit lines or cut, copy, and paste.
    - **Pasting**—You can copy a list of commands from another application, such as Microsoft Word, and then paste the list into the **Multiple Line Command** box.
2. Click **Send** to send all commands to the firewall immediately and return to the **Command Line Interface** window, or click **Cancel** to return to the window without sending any commands. The results of the commands you entered display in the **Response** box, including any errors.

Caution: If you are familiar with the Cisco IOS CLI syntax, see Important Notes. Some PIX Firewall CLI commands are unsupported in PDM.

Command Syntax

Help is available for individual command syntax and a command summary of all CLI commands. Follow these steps to get help on the syntax of a single command:

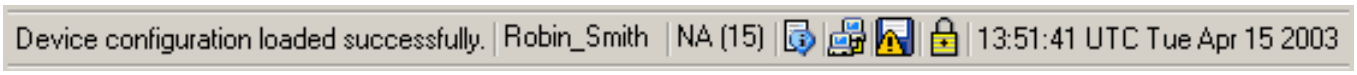
1. Enter the command(s) in the **Command** box or **Multiple Line Command** box, followed by the **?** command, or enter the **help** command followed by a command key word.
2. Click **Send** to view a description and the syntax of the command in the **Response** box.
   For example:

```
Result of PIX command: "help name"

USAGE:
[no] name <ip_address> <name>
DESCRIPTION:
name Associate a name with an IP address
SYNTAX:
<ip_address> The IP address of the host/network being named
<name> The name for the host/network. The name can be up to 4000 characters,
a-z,0-9,- and _, but it must begin with a letter
The <name> can then be used and displayed anywhere <ip_address> would
otherwise have occurred
see also: names,nameif
```

Tips on Using CLI Commands

- Understand the administration access modes before using the firewall.
- Review your privilege level in the status bar at the bottom of the main PDM window to ensure that you can execute privilege-level CLI commands.



- Check the syntax before entering a command. Enter a command and then press **Enter** to view a quick summary, or precede a command with **help**; for example, **help aaa**.
- Abbreviate commands to speed up the task of configuring the firewall. It is not necessary to type out commands completely. You need only enter the minimum unique string of characters for each command to distinguish it from other commands in the current command mode. For example, you can abbreviate the **banner login Welcome** commands by entering the **ban login Welcome** commands.
- Review possible port and protocol numbers at the following IANA websites: http://www.iana.org/assignments/port-numbers
  http://www.iana.org/assignments/protocol-numbers
- Create your configuration in a text editor and then cut and paste it into the configuration. The firewall lets you paste in one line at a time or the entire configuration at once. Always check your configuration after pasting large blocks of text to ensure that everything was copied.

The following table lists some basic firewall commands:

How can I..?	Use the following command:

Save my configuration	`write memory`
View my configuration	`show running-config`
Start accumulating system log (syslog) messages	`logging buffered debugging`
View system log (syslog) messages	`show logging`
Clear the message buffer	`clear logging`

Note: For more information about the CLI commands used by each PDM screen, see CLI Commands Used by PDM Screens.

Command Summary

Help is available for individual command syntax and a summary of all CLI commands. Follow these steps for a summary of all CLI commands:

1. Enter only a **?** or the **help** command in the **Command** box or the **Multiple Line Command** box.
2. Click **Send** to display a general description of all CLI commands in the **Response** box.

Command Reference and Access Modes

- **Cisco PIX Firewall Command Reference**—Refer to the Cisco PIX Firewall technical documentation web page. Select the version of software installed on your PIX Firewall, and then click the *Cisco PIX Firewall Command Reference*.
- **Administrative Access Modes, CLI Prompt**—A summary of the firewall administrative access modes is available from within PDM by clicking **Help>Glossary>Administrative Access Modes**.

Copyright © 2001-2004, Cisco Systems, Inc.

Telnet

Configuration>System Properties>Administration>Telnet

The **Telnet** panel lets you configure rules that permit only specific hosts or networks running PDM to connect to the firewall using the Telnet protocol.

The following sections are included in this Help topic:

- Field Descriptions
- Adding Rules
- Editing Rules
- Deleting Rules
- Applying Changes

The rules restrict administrative Telnet access through a firewall interface to a specific IP address and netmask. Connection attempts that comply with the rules must then be authenticated by a preconfigured AAA server or the Telnet password. You can monitor Telnet sessions using Monitoring>Telnet Sessions.

Note: Although a configuration file may contain more, there may be only 5 telnet sessions active at the same time.

Field Descriptions

The **Telnet** panel displays the following fields:

Telnet Rule Table:

- **Interface**—Displays the name of a firewall interface which will permit Telnet connections, an interface on which is located a PC or workstation running PDM.
- **IP Address**—Displays the IP address of each host or network permitted to connect to this firewall through the specified interface. Note: This is not the IP address of the firewall interface.
- **Netmask**—Displays the netmask for the IP address of each host or network permitted to connect to this firewall through the specified interface. Note: This is not the IP address of the firewall interface.
- **Max Idle Time**—Displays the number of minutes, 1 to 60, the Telnet session can remain idle before the firewall unit closes it. The default is 5 minutes.

- **Add**—Opens the **Add Telnet Configuration** dialog box.
- **Edit**—Opens the **Edit Telnet Configuration** dialog box.
- **Delete**—Deletes the selected item.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Adding Telnet Rules

Follow these steps to add a rule to the Telnet rule table:

1. Click the **Add** button to open the **Telnet>Add** dialog box.
2. Click **Interface** to add a firewall interface to the rule table.
3. In the IP Address box, enter the IP address of the host running PDM which will be permitted Telnet access through this Firewall interface. Note: This is not the IP address of the firewall interface.
4. In the **Mask** list, select or enter a netmask for the IP address to be permitted Telnet access. Note: This is not a mask for the IP address of the firewall interface.
5. To return to the previous panel click:

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Editing Telnet Rules

Follow these steps to edit a rule in the Telnet rule table:

1. Click **Edit** to open the **Telnet>Edit** dialog box.
2. Click **Interface** to select a firewall interface from the rule table.
3. In the IP Address box, enter the IP address of the host running PDM which will be permitted Telnet access through this Firewall interface. Note: This is not the IP address of the firewall interface.
4. In the **Mask** list, select or enter a netmask for the IP address to be permitted Telnet access. Note: This is not a mask for the IP address of the firewall interface.
5. To return to the previous panel click:

- **OK**—Accepts changes and returns to the previous panel.
-

Cancel—Discards changes and returns to the previous panel.

- **Help**—Provides more information.

Deleting Telnet Rules

Follow these steps to delete a rule from the Telnet table:

1. Select a rule from the Telnet rule table.
2. Click **Delete**.

Applying Changes

Changes to the table made by **Add**, **Edit**, or **Delete** are not immediately applied to the running configuration. Click one of the following buttons to apply or discard changes:

1. **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
2. **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Authentication/Authorization

Configuration>System Properties>Administration>Authentication/Authorization

The **Authentication/Authorization** panel lets you enable or disable required authentication, authorization, and accounting (AAA) verifications.

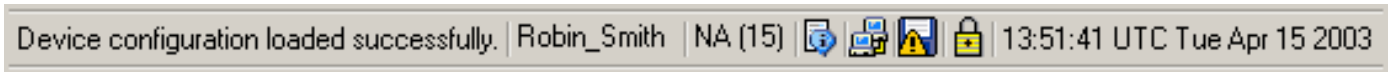
The following sections are included in this Help topic:

- Introduction
- Field Descriptions
  - Authentication
  - Command List
  - Predefined User Account Privileges Setup
- Applying Changes

Introduction to PDM Command Authentication/Authorization

Your user account privilege level is indicated in the status bar at the bottom of the main PDM window. Each screen in PDM generates PIX Firewall CLI commands which can read information from the PIX or write modifications to the configuration. For more information, see CLI Commands Used by PDM Screens.

The **Authentication** panel operates with user accounts to provide control over which users can access different functions within PDM, by associating a privilege level with certain CLI commands. You can assign each user a privilege level, as shown in the status bar.



If their privilege level is greater than or equal to the privilege level assigned to that CLI command, they are authorized to execute the command.

The **Authentication** panel lets you enable or disable AAA access to the firewall via the serial console or different types of network connections, and set other administrative access policies, such as specifying that AAA authentication must be from a specific server group. Refer to passwords, CLI console sessions, and Tools>Command Line Interface for more information.

Enabling **Command Authorization** restricts CLI access to privileged users only.

For more information about the CLI commands used by each PDM Screen, see CLI Commands Used by PDM Screens. **Help>About Cisco PIX Firewall** displays, along with other useful information, which user changed the configuration last.

```
Configuration last modified by Joe_Smith at 00:48:40.498 UTC Tue May 14
2002
```

Caution: If you choose TACACS+ server for authorization, make sure that you have configured a TACACS+ server properly or you may be locked out of the PIX.

The following should be configured in the AAA server:

- **Monitor Only** users have access to following commands in AAA
  ```
  show version
  show curpriv
  show pdm
  show blocks
  show ssh
  who
  show isakmp
  show ipsec
  show vpdn
  show local-host
  show interface
  show ip
  ping
  ```

- **Read Only** allows access to the following commands in addition to **Monitor Only**
  ```
  config terminal
  show running-config
  show privilege
  show clock
  show nt
  ```

- **Admin** allows access to following commands in addition to **Read Only** and **Monitor Only** users in AAA.

  ```
  write terminal
  ```

Predefined User Account Privileges

When **Command Authorization** is enabled, you have the option of enabling the **Predefined User Account Privileges:**

PREDEFINED	LEVEL	DESCRIPTION

Admin	15	Full access to all PIX Firewall CLI commands
Read Only	5	Read only access to all commands
Monitor Only	3	Monitoring tab only

When disabled you will be prompted to **Restore Predefined User Account Privileges** which will revert all CLI privilege levels back to the defaults when the PIX was shipped.

Predefined User Account Privileges Setup displays a list of commands and privileges PDM will issue to the PIX if **Yes** is selected. Yes allows PDM to support the three privilege levels **Admin**, **Read Only** and **Monitor Onl**y.

When you deselect Command Authorization a dialog will be displayed with a list of commands and privileges PDM is going to issue to the PIX. Yes restores all the CLI privilege levels to the same level as that when PIX was shipped. Following is an example of the CLI commands sent to the PIX after setting up Authentication/Authorization.

```
no aaa authentication enable console LOCAL
aaa authentication enable console LOCAL
aaa authentication http console LOCAL
privilege show level 0 command version
privilege show level 0 command curpriv
privilege show level 3 command pdm
privilege show level 3 command blocks
privilege show level 3 command ssh
privilege configure level 3 command who
privilege show level 3 command isakmp
privilege show level 3 command ipsec
privilege show level 3 command vpdn
privilege show level 3 command local-host
privilege show level 3 command interface
privilege show level 3 command ip
privilege configure level 3 command ping
privilege configure level 5 mode enable command configure
privilege show level 5 command running-config
privilege show level 5 command privilege
privilege show level 5 command clock
privilege show level 5 command ntp
aaa authorization command LOCAL
```

If Command Authorization is enabled and PDM detects that the PIX is not following the default privilege setup due to edits, then **Restore Predefined User Account Privileges** will be enabled. **Selecting Restore Predefined User Account Privileges** establishes the predefined privilege setup.

Field Descriptions

Authentication

- **Require AAA Authentication to allow use of privileged mode commands.**
  - **Enable**—Forces AAA authentication from a server group before you can access enable mode on the firewall. This option allows up to three tries to access the firewall console. If this number is exceeded, an access denied message appears.
  - **Server Group**—Provides a drop-down menu from which you can choose a server group to force AAA authentication.
  - **Use LOCAL when server group fails**—Uses the LOCAL server group in the event that the selected server group fails.
- **Require AAA Authorization for the following types of connections:**
  - **HTTPS/PDM**—Requires AAA authentication when you start an HTTPS connection to the firewall console. You can monitor PDM sessions using **Monitoring>PDM Users**.
    - **Server Group**—Provides a drop-down menu from which you can choose a server group to force AAA authentication.
    - **Use LOCAL when server group fails**—Uses the LOCAL server group in the event that the selected server group fails.
  - **Serial**—Requires AAA authentication when you connect to the firewall console via the serial console cable. PIX Firewall prompts you for your username and password before you can enter commands. If the authentication server is offline, wait until the console login request times out. You can then access the console with the **pix username** and the **enable password**.
    - **Server Group**—Provides a drop-down menu from which you can choose a server group to force AAA authentication.
    - **Use LOCAL when server group fails**—Uses the LOCAL server group in the event that the selected server group fails.
  - **SSH**—Requires AAA authentication when you start a Secure Shell (SSH) connection to the firewall console. This option allows up to three tries to access the firewall console. If this number is exceeded, an access denied message appears. This option requests a username and password before the first command line prompt on the SSH console. You can monitor SSH sessions using **Monitoring>Secure Shell Sessions**.
    - **Server Group**—Provides a drop-down menu from which you can choose a server group to force AAA authentication.
    - **Use LOCAL when server group fails**—Uses the LOCAL server group in the event that the selected server group fails.
  - **Telnet**—Requires AAA authentication when you start a Telnet connection to the firewall console. You are required to authenticate before you can enter a **Telnet** command. You can monitor Telnet sessions using **Monitoring>Telnet Sessions**.
  - **Server Group**—Provides a drop-down menu from which you can choose a server group to force AAA authentication.
  - **Use LOCAL when server group fails**—Uses the LOCAL server group in the event that the selected server group fails.
- **Require Authorization for PIX command access.**
  - **Enable**—Enables authorization to be required for accessing PIX commands.
  - **Server Group**—Provides a drop-down menu from which you can choose a server group for authorization.
  - **Use LOCAL when server group fails**—Uses the LOCAL server group in the event that the selected server group fails.
  - **Advanced**—Opens **Command List** to edit privilege levels of commands.
  - **Restore Predefined User Account Privileges**—Opens **Predefined User Account Privileges Setup** to confirm current setup or allow resetting to the factory default settings for user account privileges.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Command List
(System Properties>PIX Admin>Authentication/Auth>Advanced)

- **CLI Command**—Command Line Interface root command
- **Variant**—CLI variant of the root command
- **Privilege**—The privilege level associated with the CLI command variant. 0-15.
- **Edit**—After selecting a CLI Command from the table, Edit lets you change the Privilege level. Shift-click allows selection of multiple commands from the list or editing.
    - **Privilege Level**—Allows selection of the privilege level associated with the CLI command variant. 0-15.
    - **OK**—Accepts changes and returns to the previous panel.
    - **Cancel**—Discards changes and returns to the previous panel.
- **Select All**—Selects all Commands from the table. Edit then lets you change the Privilege level on all commands.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Predefined User Account Privileges Setup
(System Properties>PIX Admin>Authentication/Auth>Restore Predefined UAP)

- **CLI Command**—Command Line Interface root command
- **Variant**—CLI variant of the root command
- **Privilege**—The privilege level associated with the CLI command variant. 0-15.
- **Yes**—Restores User Account Privilege levels to factory default settings.
- **No**—Applies changes made to User Account Privileges.
- **Help**—Provides more information.

Applying Changes

Changes to the table made by **Add**, **Edit**, or **Delete** are not immediately applied to the running configuration. Click on one of the following buttons to apply or discard changes:

1. **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
2. **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

CLI Commands Used by PDM Screens

SCREEN	COMMANDS
MINIMUM	
Basic set of commands required to run PDM (for non Monitor-Only users)	`show version, show curpriv, show running-config, show privilege, configure configure (mode enable)`
MENUS	
File ▶	
Refresh PDM with the Running Configuration on the PIX	`show running-config, configure write`
Reset Firewall to the Factory Default Configuration	`configure factory-default`
Show Running configuration in new Window	`configure write`

Save Running Configuration to Flash	**configure write**
Save Running Configuration to TFTP Server	**configure write**
Save Running Configuration to standby unit	**configure write**
Tools	
Ping	**configure ping,**
Service Groups	**configure object-group, configure description, configure port-object, configure group-object**
TABS	
Access Rules	
Access Rules	**configure access-list, configure access-group, configure conduit, configure apply, configure outbound, configure filter, configure aaa**

Translation Rules	
Translation Rules	**configure nat, clear xlate, configure global,**
VPN	
IPSec Rules	**configure crypto, configure map, configure dynamic-map, configure access-list, configure nat**
Tunnel Policy	**configure crypto, configure dynamic-map, configure map**
Transform Sets	**configure crypto**
Policies	**configure isakmp,**
XAuth/Mode Config Setup	**configure crypto**
Pre-shared Keys	**configure isakmp,**
Certificate Configuration	**configure ca,**
Certificate Authentication	**configure ca,**
Certificate Enrollment	**configure ca,**

Cisco VPN Client	**configure vpngroup, configure access-list**
L2TP/PPTP Client	**configure vpdn,**
IP Pools	**configure ip**
VPN System Options	**configure sysopt**
Easy VPN Remote	**configure vpnclient,**
Host/Networks	
Host/Networks	**configure static, configure name, configure names, configure pdm, configure nat, configure global, configure object-group, configure description configure network-object, clear xlate, configure route**
System Properties	
Interfaces	**configure nameif, configure ip, configure interface, vpdn**
Failover	**configure failover,**

RIP	**configure rip,**
Static Route	**configure route,**
Proxy ARPs	**configure sysopt,**
DHCP Server	**configure dhcpd,**
Device	**configure hostname, configure domain-name**
Password	**configure passwd, configure enable (mode configure)**
Authentication	**configure aaa, configure privilege,**
User Accounts	**configure username,**
PDM/HTTPS	**configure http**
Telnet	**configure telnet,**
Secure Shell	**configure ssh,**
SNMP	**configure snmp-server, configure logging**
ICMP	**configure icmp,**

TFTP Server	**configure tftp-server,**
Clock	**configure clock, show clock**
NTP	**configure ntp,**
Logging setup	**configure logging,**
Pdm Logging	**configure pdm,**
Syslog	**configure logging,**
Others (Logging)	**configure logging,**
AAA Server Group	**configure aaa-server,**
AAA Server	**configure aaa-server,**
Auth. Prompt	**configure auth-prompt,**
URL Filtering	**configure url-server, configure url-cache, configure url-block,**
Auto Update	**configure remote-management,**
IDS Policy	**configure ip**

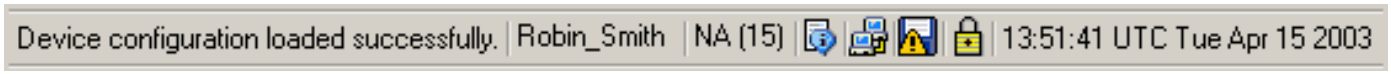
IDS Signature	**configure ip**
All Fixup Screens	**configure fixup,**
Anti Spoofing	**configure ip**
Fragment	**configure fragment,**
TCP Options	**configure sysopt,**
Timeout	**configure timeout,**
Turbo Access Rules	**configure access-list**
Stub Multicast Routing	**configure igmp, configure multicast, configure access-list**
IGMP Protocol	**configure igmp, configure multicast, configure access-list**
IGMP Access Group	**configure igmp, configure multicast, configure access-list**
IGMP Join Group	**configure multicast, configure igmp**
MRoute	**configure mroute,**

History Metrics	**configure pdm,**
Monitoring	
PDM Log	**show pdm**
Secure Shell Sessions	**show ssh, configure ssh**
Telnet Console Sessions	**configure who,**
User Liceses	**show local-host**
PDM Users	**show pdm**
DHCP Client	**show dhcp**
PPPoE Client	**show ip**
IKE SAs	**show isakmp**
IPSec VPNs	**show ipsec**
L2TP	**show vpdn**

PPTP	**show vpdn**
All Graphs	**pdm_handler (not a command)**
PDM Status Bar	**show curpriv, pdm_handler (not a command)**

Copyright © 2001-2004, Cisco Systems, Inc.

Status Bar



Click to navigate.

Copyright © 2001-2004, Cisco Systems, Inc.

User Accounts

Configuration>System Properties>Administration>User Accounts

The **User Accounts** panel lets you control user access to specific PDM functions.

The following sections are included in this Help topic:

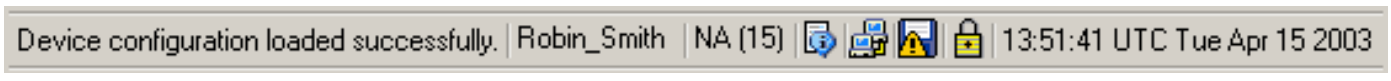
- Introduction
- Legacy Account Naming Support
- Field Descriptions

Introduction

The **User Accounts** panel lets you create a list of user accounts with a privilege level, in the range of 0 to 15, for each user. Each panel in PDM generates PIX Firewall CLI commands that can read information from the firewall or write modifications to the configuration.

User Accounts operates with **Authentication/Authorization**, where you can configure command group privileges for different functions within PDM according to their CLI commands. You can also assign each user a privilege level. If the privilege level is greater than or equal to the privilege level assigned to a specific CLI command, the user is authorized to execute the command.

There are two types of user accounts: those with fixed, predefined names for legacy support and PDM user account names, which can be unique and assigned to each individual user. To avoid confusion, use the User Account feature to assign privileges to user accounts with a real name. The user account name and privilege level is displayed in the status bar at the bottom of the main PDM window.



In order to enforce user accounts privileges, you must enable **Command Authorization**. If **Command Authorization** is disabled, all users have access to all commands.

For more information, see passwords, CLI console sessions, and CLI.

▲

Legacy Account Naming Support

PDM also lets you use the legacy-type user accounts based on the enable password, using the predefined names **enable_15**, **enable_14**, and so on, through **enable_0**. You cannot modify these predefined names or their privilege levels. To enable the predefined user accounts, simply provide a password.

The firewall previously shipped with only one user, called the"**enable_15**" user. In earlier releases, the password for this user account was called the *enable* password. This **enable_15** user was also referred to as the "**nameless**" user, because anyone who logged into the firewall without giving a user name, was treated as an **enable_15** user and was expected to provide the *enable* password.

Note: **User Account Passwords**

- Passwords are important. Always follow the password security policy for your organization and assign strong passwords.
- PIX user account names and passwords may not contain spaces.

Field Descriptions

User Accounts

- **User Name**—The name of the user.
- **Privilege** (Level)—Privilege level of commands authorized for this user account, in the range of 0 to 15.
- **Add**—Displays the User Details dialog to add a new user account.
- **Edit**—Displays the User Details dialog to edit an existing user account selected in User Accounts.
- **Delete**—Deletes the user account selected in User Accounts.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

User Account Details

- **User Name**—The name of the user. May not contain spaces.
- **Password**—Enter an optional password for this user. May not contain spaces.
- **Confirm Password**—Confirm the password.
- **Privilege Level**—Privilege level, 0-15, of commands authorized for this user account.
- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

Clock

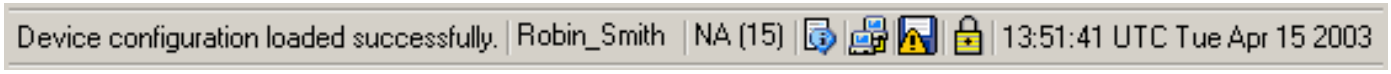
Configuration>System Properties>Administration>Clock

The **Clock** panel lets you set the time for use by the internal real time clock of the firewall for display, timestamp log entries, and other functions.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

The firewall time displays on the right of the status bar at the bottom of the main PDM window.



Important Notes

- The current firewall time displays at the bottom right corner of the PDM screen, and updates automatically every ten seconds. To get the latest firewall time on the **Clock** panel click **Update Display Time**.
- If NTP servers have been configured on the firewall, the NTP server time will overwrite the time set in the **Clock** panel. See NTP.
- If you choose a time zone that uses daylight saving time and deselect **Automatically adjust clock for daylight saving changes**, PDM may select a different time zone name after a refresh. This change occurs because the selected zone has the same zone parameters without the daylight saving time settings.

Field Descriptions

- **Time Zone**—Selects the GMT (UTC) time zone for this firewall.
- **Date**— Lets you set the Date of the clock.
  - **Month**—Selects the current month of the year.
  - **Year**—Selects the current year.

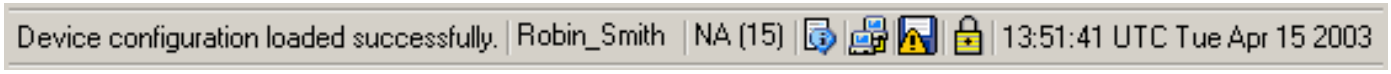
- **Time**—Sets the hh (hours), mm (minutes), and ss (seconds) of the clock.
- **Update Display Time**—Retrieves and displays the current time on the firewall.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

NTP

Configuration>System Properties>Administration>NTP

The **NTP** panel lets you synchronize the time on the firewall clock with a server that uses Network Time Protocol (NTP). The time displays in the status bar at the bottom of the main PDM window.



NTP is used to implement a hierarchical system of servers that provide a precisely synchronized time among network systems. This kind of accuracy is required for time-sensitive operations, such as validating Certificate Revocation Lists (CRLs), which include a precise time stamp.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Applying Changes

The firewall uses an NTP client that allows it to obtain the system time from NTP version 3 servers, like those provided with Cisco IOS routers. Once the firewall obtains reliable time information from a configured NTP server, it synchronizes with the time that server designates.

You can use PDM to configure multiple NTP servers. The firewall chooses the server with the least stratum—a measure of how reliable the data is.

PDM lets you configure the firewall to use NTP authentication, where the firewall synchronizes with only those NTP servers on which an NTP key is configured. This key is configured by checking the **Enable NTP Authentication** box, and configuring a **Key Number** and, if the key is trusted, by checking **Trusted** in the **NTP Server Detail** dialog box.

For more information about implementing NTP, see the Network Time Protocol: Best Practice White Paper.

See the National Institute of Standards (NIST) for an accurate source of the time in your time zone.

Important Notes

- The firewall listens for NTP packets (port 123) only on interfaces that have an NTP server configured. NTP

packets that are not responses from a request by the firewall are dropped.
- If authentication is used, the firewall and NTP server must be configured with the same key.
- When the firewall is synchronized with an NTP server, it overwrites the user selected time with the NTP server time, even if user changes the clock time using the Clock panel.
- To disable the use of NTP servers, remove all NTP servers from the PDM configuration.
- See UTC and GMT for more information.

Field Descriptions

The **NTP Server List** displays the following fields:

- **IP Address**—Specifies the IP Address of the NTP server.
- **Interface**—Specifies the interface from which the firewall gets NTP packets.
- **Preferred?**—Displays **Yes** if the selected server is a preferred, and **No** if it is not preferred. If several NTP servers have the same stratum, then the firewall chooses the preferred server. Generally, the firewall chooses the server with the lowest stratum. We recommend that you configure an NTP server as preferred only when multiple servers have the same stratum.
- **Key Number**—Specifies the authentication key number, a value from 1 to 4294967295.
- **Trusted Key?**—Specifies if the authentication key is trusted. A trusted key is similar to a password used to authenticate an NTP server.

Enable NTP Authentication—Enables or disables NTP authentication.

- **Add**—Adds an NTP Server.
- **Edit**—Edits an existing NTP server.
- **Delete**—Deletes and existing NTP server.

The **NTP Server Detail** box is opened when either **Add** or **Edit** is selected, and has the following configurable areas:

- **IP Address**—Specifies the IP Address of the NTP server, which is mandatory.
- **Preferred**—Enables this NTP server as the preferred NTP server.
- **Interface**—Selects the interface from which the firewall gets NTP packets.

Authentication Key—Configures an authentication key on the NTP server, if required.

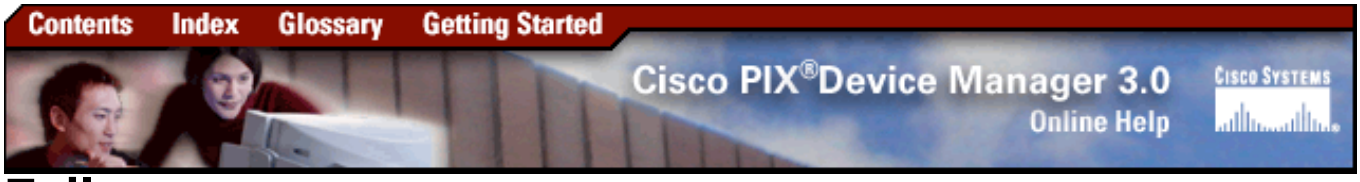
- **Key Number**—Specifies the authentication key number, a value from 1 to 4294967295.
- **Trusted**—Specifies if the NTP server is trusted.
- **Key Value**—Specifies the key value, an arbitrary string of up to 32 characters.
- **Reenter Key Value**—Verifies the key value you entered.

Applying Changes

Changes to the table made by **Add**, **Edit**, or **Delete** are not immediately applied to the running configuration. You must click on one of the following buttons to apply or discard changes:

1. **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
2. **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.



Failover

Configuration>System Properties>Failover

The **Failover** dialog box lets you configure two firewall units so that one will take over operation should the other fail.

The following sections are included in this Help topic:

- **Introduction**
  - Hardware Requirements
  - Failover
  - Failover Reset
  - Stateful Failover, Minimum Setup
  - LAN-based Failover
  - Failover on MAC Address
- **Important Notes**
  - Failover
  - LAN-Based Failover
- **Field Descriptions**
- **System Properties>Interfaces** and Failover
- **Enabling** Failover
- **Edit/Enable** Failover
  - Failover Poll Time
  - IP Address
  - MAC Addresses
  - Stateful Failover
  - LAN-based Failover
    - Enable LAN-Based Failover
    - Example LAN-Based Failover Configuration
- **Troubleshooting**
- **Sample Configurations**
- **FAQ** (Frequently Asked Questions)
  - General Questions About Failover
  - Cable-Based Failover
  - LAN-Based Failover
  - Stateful Failover Questions

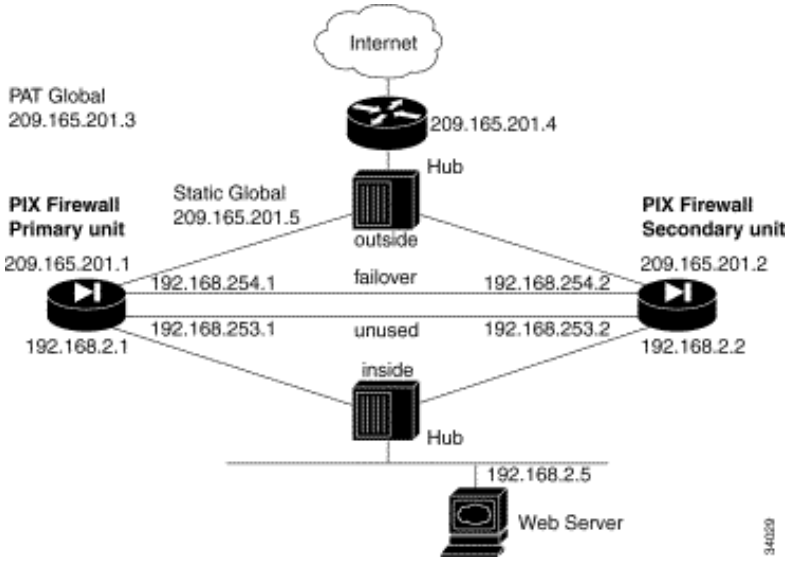
Introduction to PIX Firewall Failover

Hardware Requirements

Failover is supported for two identical PIX Firewall models with 3 or more Interfaces. Both units must have the same software version, encryption license, Flash memory, and the same amount of RAM. PIX Firewall 501 and PIX Firewall 506 do not support failover. The PIX Firewall 515, PIX Firewall 525, and PIX Firewall 535 can only be used as the primary unit in a failover pair if you have the optional "UR" license.

Failover

Failover Configuration



Failover configures two identical Cisco firewall units so that a secondary unit can take over processing network connections in the event the primary unit fails. Using a pair of identical firewalls (model, memory, NICs, OS), high availability can be provided with no operator intervention. One PIX is considered the active unit while the other is the standby unit. As the name implies, the active unit actively performs normal network functions while the standby unit only monitors, ready to take control should the active unit fail to perform its functionality.

Failover Modes

MODE	ACTIVE FIREWALL UNIT	STANDBY FIREWALL UNIT
Normal	Primary	Secondary
Failover	Secondary	Primary

The **`show failover`** command verifies that the primary unit is enabled by checking for the following statement:

```
This host: primary - Active
```

The two units each have a presence on the network. The active unit uses the System IP address and the MAC addresses of the primary unit (the primary unit is determined by the unit that has the end of the failover cable marked Primary plugged into it). The standby unit uses the Failover IP address and the MAC addresses of the secondary unit. If a switchover occurs, the units swap the IP address and MAC addresses they are using so as to replace each other's presence on the network. This action is invisible to the network. The IP to MAC address relationships remain exactly the same so no ARP tables in the network need to time out or be changed. No other piece of network equipment needs to know about the redundancy or that a switchover occurred. Note that the System IP and the Failover IP addresses must be on the same subnet, so there may not be a router between the two units.

In addition to monitoring all network interfaces, failover also monitors the power status of the other unit as well as the status of the failover cable itself. The failover cable provides the ability to detect if the other unit is plugged in and if the other unit is powered on. If the cable is unplugged from either unit, switching is disabled. If an active unit looses power, the standby unit will take over within 15 seconds. A unit in the failed state waits 15 seconds then tries to transition to standby state. If the transition triggers a failure, the unit will fail again.

Failover Reset

A unit in the failed state waits 15 seconds then tries to transition to standby state. The command **failover reset** can be used to manually reset the PIX from the failed to standby state. If the transition triggers a failure, the unit will fail again. A PIX in the failed state

cannot switch into active state.

If the failure is due to a link **downcondition** on an interface, a link **upcondition** will clear the failed state (i.e. if an interface is unplugged and later plugged in).

Whenever a failure or switch occurs, syslog messages are generated indicating exactly what happened. Fail back to the primary unit is not forced.

Stateful Failover

Stateful Failover allows the standby unit to maintain the state of all connections, except those started by web connections.

If Stateful Failover is used, then per-connection stateful information is passed from the Active to the Standby Cisco firewall unit. After a failover occurs, the same connection information is available at the new active unit. End user applications are not required to reconnect to keep the same communication session. Because the newly active unit assumes the same IP and MAC address as the previously active unit, no ARP entries need to change or timeout anywhere in the network.

The state information passed to the standby unit includes the global pool addresses and status, connection and translation information and status, the negotiated H.323 UDP ports, the port allocation bit map for PAT, and other details necessary to let the standby unit take over processing if the primary unit fails.

Depending on the failure, the PIX Firewall takes from 15 to 45 seconds to cause a switchover. Applications not handled by Stateful Failover will then require time to reconnect before the active unit becomes fully functional.

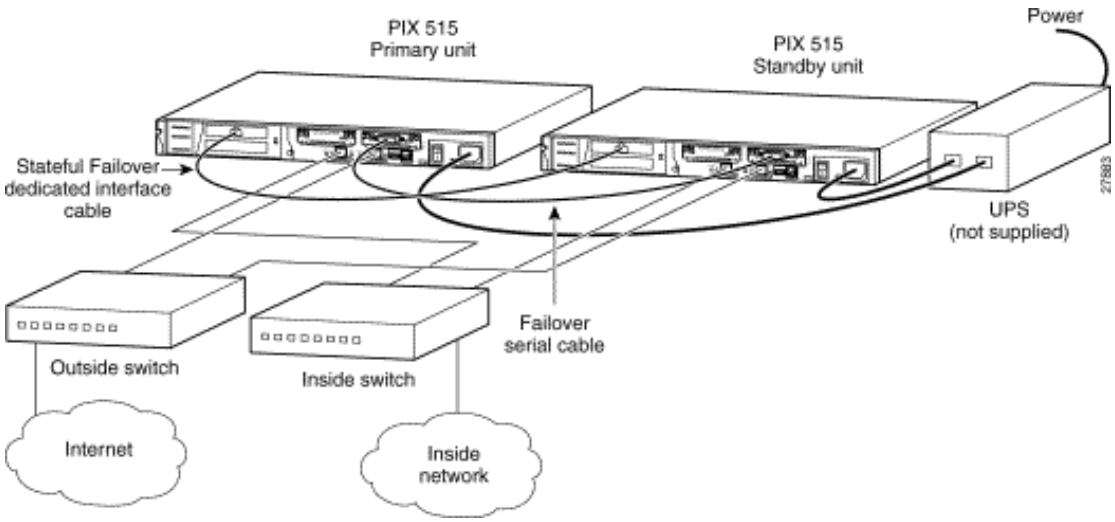
Stateful Failover requires a 100 Mbps or Gigabit Ethernet interface to be used exclusively for passing state information between the two PIX firewall units.

The Stateful Failover interface can be connected to any of the following:

- Cat 5 crossover cable directly connecting the primary unit to the secondary unit.
- 100BaseTX half-duplex switch using straight Cat 5 cables.
- 100BaseTX full-duplex on a dedicated switch or dedicated VLAN of a switch.
- 1000BaseTX full-duplex on a dedicated switch or dedicated VLAN of a switch.

Data is passed over the dedicated interface using IP protocol 105. No hosts or routers should be on this interface.

Stateful Failover Minimum Setup



All enabled interfaces should be connected between the active (primary) and standby units. If an interface is not in use, use **System Properties>Interfaces** to select the interface and disable it.

A PIX Firewall with two FDDI cards cannot use Stateful Failover because an additional Ethernet interface with FDDI is not supported.

The dedicated Fast Ethernet or Gigabit Ethernet ports on both Cisco firewall units to use Tera Term Pro with SSH be connected and fully functional.

LAN-Based Failover

The connection between the primary and secondary may be a failover cable up to 6ft. in length or a LAN-based connection for longer distances.The interface used for LAN failover management control can be shared with stateful failover, or can be configured separately. Since LAN-based failover requires IP messages to traverse longer distances on more open networks, message encryption and authentication are implemented using manual pre-shared keys to improve reliability and security. When using LAN-based failover, secondary status is the default and you must specify if the PIX is the primary unit.

To configure the secondary PIX, PDM will connect to the secondary PIX at the same interface through which PDM is connected to the Primary (current) PIX.

▲

Failover on MAC (Media Access Controller) Address

Unlike the IP address, the MAC addresses are not saved in the PIX flash memory. Instead they are retrieved from the NIC cards when PIX boots up. In the event that both the units are powered down and the secondary PIX boots up first, it doesn't have the MAC address of the primary PIX. Hence, it uses its own NIC burnt-in MAC address as the MAC address of the active unit. This combination of using the primary IP and secondary MAC can confuse the external switch/router. When the primary PIX boots at a later time, failover switches back to the primary IP and primary MAC which further disrupts the connections already in progress.

To overcome this problem, the PIX allows the user to configure the virtual MAC address for the PIX failover pair using the **failover MAC address <interface> <active_mac> <standby_mac>** CLI command.

For additional information, see Failover FAQ.

▲

Important Notes

1. You can use the **show failover** and **show failover lan** commands to view the configuration and status of PIX failover.
2. All enabled interfaces should be connected between the active and standby units. If an interface is not in use, use the **shutdown** option to the **interface** command to disable the interface.
3. Do not change interface **Speed** if Failover is enabled.
4. Perform the following on any switch that connects to the PIX Firewall:
   - Enable portfast on all ports on the switch that connect directly to the PIX Firewall.
   - Turn off trunking on all ports on the switch that connect directly to the PIX Firewall.
   - Turn off channeling on all ports on the switch that connect directly to the PIX Firewall.
   - Ensure the MSFC is not running a deferred Cisco IOS software version.

   Note: In CAT OS 5.4 a new command was added: **`set port host.`** This command executes the following commands: **`spantree portfast enable`**, **`set trunk off`**, and **`set port channel off`**. This command provides a convenient way to configure host/access ports to a mode that allows the port to forward traffic in less than one second from link up.
5. **UR License**—The PIX Firewall failover unit is intended to be used solely for failover and not in standalone mode. If a failover unit is used in standalone mode, the unit will reboot at least once every 24 hours until the unit is returned to failover duty. When the unit reboots, the following message displays at the console.

```
=========================NOTICE ==========================
```

```
This machine is running in secondary mode without a connection to an active primary PIX.
Please check your connection to the primary system. REBOOTING....
```

6. If a failover-only the PIX Firewall is not attached to a failover connection or is attached to the primary end of a Failover cable, then it will hang at boot time. It should be a secondary unit.
7. Changes made on the standby unit are not replicated on the active unit.
8. File>Save Running Configuration to Standby Unit can be used to replicate the configuration from the primary to the secondary unit.

Important Notes About LAN-Based Failover

- **CLI Commands**—The CLI commands **show failover lan** and **show failover lan detail** may be used to view the configuration and status of PIX failover. There are additional CLI commands specific to LAN-based failover. For additional information, see the command reference for your version of software.
- **Hub Required**—A dedicated LAN interface and a dedicated switch/hub (or VLAN) is required to implement LAN-based failover. You cannot use a crossover Ethernet cable to connect the two PIX Firewalls.
- **Restrictions**—The interface used for LAN failover management control can be shared with stateful failover, or can be configured separately. For the initial configuration replication, a minimum set of configuration is required to establish the network connectivity so that the Active PIX can replicate the firewall configuration to the standby unit. The minimum set of configuration is:

```
nameif <hardware_id> <fover_lan_if_name> <security_level>
                          ip address <fover_lan_if_name> <system_ip> <mask>
                          failover ip address <fover_lan_if_name> <failover_ip>
                          failover lan unit primary|secondary
                          failover lan interface <fover_lan_if_name>
                          failover lan key <preshare_key>
                          failover lan enable failover
```

Also, the above configuration information needs to be retained for configuration replication. In case any of the above is changed on one of the units, then the same change also needs to be applied on the peer (other failover unit). In case any of the minimum configuration commands are changed, the PIX failover pair will need to reload.

▲

Caution: **SSH, PDM, and Failover**

Do not use PDM over an SSH tunnel to configure LAN-based failover, as PDM is unable to configure the standby PIX Firewall. There is no problem if you are using SSH and configuring failover using a serial cable.

Field Descriptions

The **Failover** panel provides the following information fields:

Failover:

- **Enable Failover**—Selecting this check box allows the Failover Interface and IP Addresses displayed in the table to be selected and then edited by clicking on the **Edit** button. This lets you assign IP addresses for the standby unit. Before enabling failover, to change the IP address for the primary unit, change speed or other interface settings, use **Configuration>System Properties>Interfaces**.

Note: The speed may not be changed when Failover is enabled.

- **Interface**—Displays the name of the Interface on the active Cisco firewall unit which it will use for communication with the standby unit for failover. When configured for Stateful Failover, this interface is directly connected to the standby unit.
- **IP Address**—Displays the IP address of the interface on the standby unit which it will use to communicate the active unit. Use **Configuration>System Properties>Failover>Edit** to change. Note: Use this IP address with the Ping tool to check the status of the standby unit.
- **Failover Poll Time**—Specifies how long failover waits before determining if other units are still available between the primary and standby units over all network interfaces and the failover cable. The default is 15 seconds. The minimum value is 3 seconds and the maximum is 15 seconds.
- **Edit**—Opens the **Edit** dialog box.The **Configuration>System Properties>Failover>Edit** dialog box allows you to edit the IP address of the interface that you selected from the **Failover** dialog box and set the Active and Standby MAC addresses.

Stateful Failover:

- **Enable Stateful Failover**—Enables the Stateful Failover interface.
- **HTTP Replication**—Enables Stateful Failover to copy active HTTP sessions to the standby PIX Firewall.
- **Interface where a fast LAN link is available for Stateful Failover**—Choose which **interface** has the fastest LAN link. In addition to the failover cable, a dedicated fast LAN link is required to support Stateful Failover. We suggest you do not use FDDI because of its blocksize or Token Ring because Token Ring requires additional time to insert into the ring. The default Stateful Failover interface is the highest LAN port with failover configured.

LAN-Based Failover:

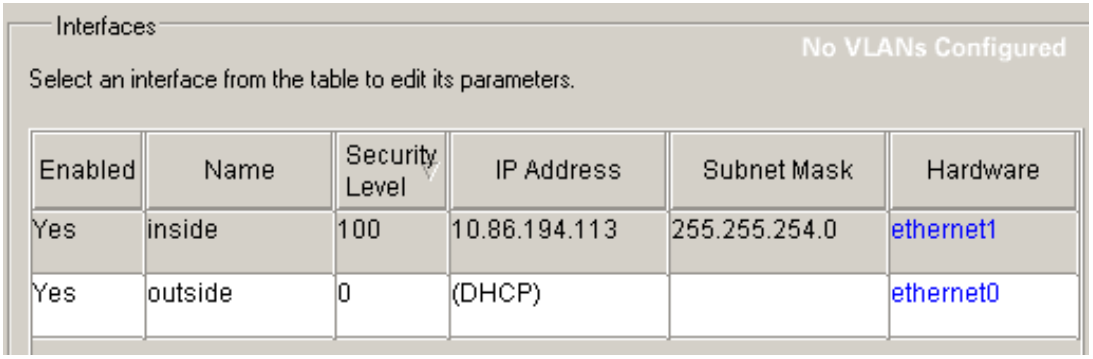
- **Enable LAN-based Failover**—Enables LAN-based Failover on the firewall unit.
- **LAN Interface**—Interface where a fast LAN link is available for communicating with the other PIX.
- **Shared Key**—Secret key used to encrypt traffic between the primary and standby PIX.
- **This PIX is**—By choosing either of the Primary or Secondary radio buttons you can indicate whether this PIX Firewall unit is the primary or secondary unit. If This unit is primary, he other will be secondary. If This Cisco firewall unit is secondary, the other will be primary.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.
- **Failover Reset**—Forces both primary and standby PIX to an unfailed state.

▲

Configuration>Systems Properties>Interfaces and Failover

Configuration>Systems Properties>Interfaces and **Configuration>System Properties>Failover** must be configured together.



Before enabling Stateful Failover or LAN-based Failover, the interface to be used for Failover on the Primary Cisco firewall unit must be configured in **Configuration>Systems Properties>Interfaces** as follows:

1. **Interface Name**—Failover requires a PIX Firewall model with 3 or more interfaces. Failover is usually the first interface available after **inside** and **outside**.
2. **IP Address**—A unique and valid IP address on the same network as the interface on the secondary Cisco firewall unit.
3. **Subnet Mask**—A valid Subnet Mask allowing for the number of nodes on the network connecting the Primary and Secondary failover interfaces, usually 255.255.255.0. PIX Firewall will default to 255.255.255.255, invalid, in order to avoid routing problems.
4. **Speed**—Do not set the interface speed to **Auto for** 10, 100, or 1000. Do not change **Speed** if Failover is enabled.
5. **Enabled**—Before enabling failover, the interface must be enabled or "administratively up" in Configuration>Systems Properties>Interfaces.

Caution: Do not change interface **Speed** if Failover is enabled.

Enabling Failover in Configuration>Systems Properties>Failover

Configuration>System Properties>Failover lets you create a new Failover setup and enable or disable the Failover feature in an existing configuration.

1. Before enabling Failover, verify that you have two identical Cisco firewall units which meet the hardware requirements and are properly connected for Failover.
2. Before enabling failover, verify that the IP address, speed, and other settings for the interfaces used by the primary unit are set correctly using **Configuration>System Properties>Interfaces**.
   Note: When Failover is enabled, the speed setting of an interface may not be changed.
3. Before enabling failover, make sure that the configuration in the standby unit is the same as the primary unit, using **File>Save Running Configuration to Standby Unit**, then update the Flash memory of the standby unit using **File>Save Running Configuration to Flash**. For more information, refer to Notes on Applying Configuration Changes.
4. Before enabling failover, synchronize the clocks on the Primary and Secondary Cisco firewall units using **Configuration>System Properties>Administration>Clock.**
5. In **Configuration>System Properties>Failover**, select **Enable Failover**. This will enable the Failover feature and allow you to edit the the **Failover**, **Stateful Failover**, and **LAN-based Failover** areas.
6. When you have completed your edits in **Configuration>Systems Properties>Failover**, you may select:

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.
- **Failover Reset**—Forces both primary and standby PIX to an unfailed state.

Edit Failover Setup in System Properties>Failover

After **Enable Failover** (check box) is enabled, follow these steps to edit the **Failover**, **Stateful Failover**, and **LAN-based Failover** areas:

Failover

Failover Poll Time

In **Configuration>System Properties>Failover>Failover Poll Time** enter the time, in seconds, that you want the firewall unit to ARP itself. The default is 15 seconds. The minimum is 3 seconds, and the maximum is 15 seconds.

Edit>Edit Failover

In **Configuration>System Properties>Failover>Edit>Edit Failover** you may edit the IP address and MAC addresses for the Failover feature.

1. Select the interface that you want to edit from the Failover table.
2. Click **Configuration>System Properties>Failover>Edit** to open **Edit Failover**
3. Make any changes necessary to the fields displayed for the selected interface in **Edit Failover**.

- **IP address**—The IP address of the interface on the standby unit which it will use to communicate the active unit. Note: Use this IP address with the Ping tool to check the status of the standby unit.

- These optional fields may be configured for the Failover on MAC address feature:
- **Active MAC address**—Enter the MAC address of the active PIX (usually primary).
- **Standby MAC address**—Enter the MAC address of the standby PIX (usually secondary).

  For more information on these fields, see Field Descriptions or Introduction to PIX Firewall Failover in this help topic.

To exit **Configuration>System Properties>Failover>Edit>Edit Failover** and return to **Configuration>System Properties>Failover**, click one of the following:

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Stateful Failover - Configuration>System Properties>Failover

Follow these steps to enable Stateful Failover:

1. Select **Enable Stateful Failover** in **Configuration>System Properties>Failover**.
2. Select an **interface** where a fast LAN link is available from LAN Interface
3. Optionally, **enable HTTP Replication**.
4. Select an **Interface** for the Stateful Failover LAN link.

For more information see the Stateful Failover FAQ and the firewall configuration guide for your version of software.

LAN-Based Failover - Configuration>System Properties>Failover

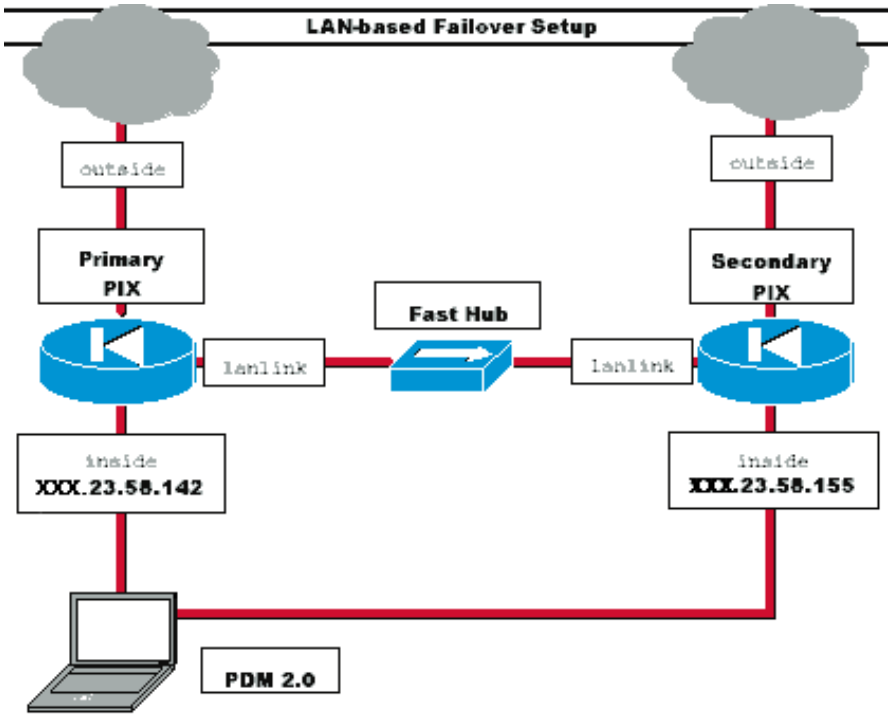
Follow these steps to enable LAN-Based Failover:

1. Confirm that the Primary PIX Firewall failover interface is configured correctly in **Configuration>Systems Properties>Interfaces** and is administratively up (enabled).
2. Do not use an SSH tunnel for your PDM session with the Primary Cisco firewall unit. For more information, see **Caution: SSH, PDM, and LAN-based Failover**
3. Confirm the interface on the Primary Cisco firewall unit to be used for LAN-based Failover is not being used for your PDM session. You may not select the same interface used by your current PDM session to access the Primary PIX as the LAN-based failover interface to the Secondary PIX.
4. Disconnect the standard failover cable if it is connected between the failover connectors of the Primary and Secondary Cisco firewall units.
5. **Confirm connectivity to the Secondary Cisco firewall unit.**
   PDM requires access to both the Primary PIX Firewall from which you are running PDM and the Secondary Cisco firewall unit which will be used for Failover. Confirm that the Secondary PIX is accessible from your PC or workstation currently running PDM by using **Tools>Ping** to send an echo packet from the Primary PIX failover interface to the IP address of the failover interface of the Secondary PIX Firewall. Connectivity is confirmed if you receive a response.
6. Before enabling failover, synchronize the clocks on the Primary and Secondary Cisco firewall units using **Configuration>System Properties>Administration>Clock.**
7. Select **Enable LAN-Based Failover** in **Configuration>System Properties>Failover**.
8. Select a **Interface** from **LAN Interface**
9. Enter the key value in **Shared Key** which the firewalls will use to authenticate each other.
10. Identify this PIX Firewall as the **Primary** or **Secondary** unit in the Failover configuration.
11. Use one of the following before you exit **Configuration>System Properties>Failover**:
    - **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
    - **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.
    - **Failover Reset**—Forces both primary and standby PIX to an unfailed state.

For more information see the LAN-based Failover FAQ , Sample Configurations, the firewall configuration guide, Using Failover.

Note: After enabling a LAN-based failover configuration you will be restricted from modifying the configuration again for more than a minute while the Primary Cisco firewall unit completes synchronization with the Secondary PIX.

Example LAN-Based Failover Configuration



Troubleshooting Failover - Configuration>System Properties>Failover

To verify the failover setup and status of your firewall Configuration, use **Tools>CLI** to execute the **show failover** command.

- Show Failover - Cable
- Show Failover LAN - LAN-based
- Show Failover LAN Detail

The **show failover** command verifies that the primary unit is enabled by checking for the following statement:

```
This host: primary - Active
```

Sample output from the show failover command

Show failover Command Output—Cable Failover Enabled

`show failover`

```
Failover On
Cable status: Unknown
Reconnect timeout 0:00:00
Poll frequency 15 seconds
This host: primary - Active
Active time: 225 (sec)
Interface 4th (aaa.16.1.1): Normal (Waiting)
Interface intf3 (bbb.yyy.3.1): Link Down
Interface intf2 (bbb.yyy.2.1): Normal (Waiting)
Interface outside (bbb.yyy.1.1): Normal (Waiting)
Interface inside (10.1.1.1): Normal (Waiting)
Other host: secondary - Standby
Active time: 0 (sec)
Interface 4th (0.0.0.0): Unknown (Waiting)
Interface intf3 (0.0.0.0): Unknown (Waiting)
```

```
Interface intf2 (0.0.0.0): Unknown (Waiting)
Interface outside (0.0.0.0): Unknown (Waiting)
Interface inside (0.0.0.0): Unknown (Waiting)
```

Show failover Command Output—LAN-Based Failover Enabled

```
pix(config)# show failover

Failover On
Cable status: Normal
Reconnect timeout 0:00:00
Poll frequency 15 seconds
      This host: Primary - Active
              Active time: 253515 (sec)
              Interface faillink (192.168.3.1): Normal
              Interface outside (172.23.58.70): Normal
              Interface inside (192.168.2.1): Normal
      Other host: Secondary - Standby
              Active time: 0 (sec)
              Interface faillink (192.168.3.2): Normal
              Interface outside (172.23.58.71): Normal
              Interface inside (192.168.2.2): Normal

Stateful Failover Logical Update Statistics
      Link : faillink
      Stateful Obj    xmit       xerr       rcv        rerr
      General         34177      0          34183      0
      sys cmd         34175      0          34173      0
      up time         2          0          2          0
      xlate           0          0          0          0
      tcp conn        0          0          8          0
      udp conn        0          0          0          0
      ARP tbl         0          0          0          0
      RIP Tbl         0          0          0          0
>
      Logical Update Queue Information
                      Cur     Max     Total
      Recv Q:         0       1       34184
      Xmit Q:         0       1       34179
>
LAN-based Failover is Active
      interface dmz (171.69.39.200) Normal, peer (171.69.39.201): Normal:
```

Show Failover LAN Command

The **show failover lan** command will only show the LAN failover section.

```
pix(config)# show failover lan
Lan Based Failover is Active
interface dmz (171.69.39.200): Normal, peer (171.69.39.201): Normal
```

Show Failover LAN Detail Command

The **show failover lan detail** command is used mainly for debugging purposes, and the output will be subject to many changes in the future

```
pix(config)# show failover lan detail
Lan Failover is Active
```

```
This Pix is Primary
Command Interface is dmz
Peer Command Interface IP is zzz.xz.39.201
My interface status is 0x1
Peer interface status is 0x1
Peer interface downtime is 0x0
Total msg send: 103093, rcvd: 103031, droped: 0, retrans: 13, send_err:  0
Total/Cur/Max of 51486:0:5 msgs on retrans
  msgs on retrans if any
LAN FO cmd queue, count: 0, head: 0x0, tail: 0x0
Failover config state is 0x5c
Failover config poll cnt is 0
Failover pending tx msg cnt is 0
Failover Fmsg cnt is 0
:
```

For more detailed information about failover, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

Cisco Technical Assistance Center (TAC) maintains an automated tool to assist you in troubleshooting output from the **show failover** command.
Https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl

---

Sample Failover Configurations

LAN-Based Failover primary unit Configuration

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 stateful security10
nameif ethernet3 lanfover security20
enable password xxx encrypted
passwd xxx encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 20
no logging timestamp
no logging standby
logging console errors
no logging monitor
no logging buffered
no logging trap
logging facility 20
logging queue 512
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
interface ethernet3 100full
mtu outside 1500
mtu inside 1500
```

```
mtu failover 1500
mtu unused 1500
ip address outside 209.165.201.1 255.255.255.224
ip address inside 192.168.2.1 255.255.255.0
ip address failover 192.168.254.1 255.255.255.0
ip address unused 192.168.253.1 255.255.255.252
failover
failover ip address outside 209.165.201.2
failover ip address inside 192.168.2.2
failover ip address stateful 192.168.254.2
failover ip address lanfover 192.168.253.2
failover link stateful
failover lan unit primary
failover lan interface lanfover
failover lan key 12345678
failover lan enable
arp timeout 14400
global (outside) 1 209.165.201.3 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 209.165.201.5 192.168.2.5 netmask 255.255.255.255 0 0
access-list acl_out permit tcp any 209.165.201.5 eq 80
access-list acl_out permit icmp any any
access-group acl_out in interface outside
access-list acl_ping permit icmp any any
access-group acl_ping in interface inside
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
no rip failover passive
no rip failover default
route outside 0 0 209.165.201.4 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
telnet timeout 5
terminal width 80
```

LAN-Based Failover Secondary Unit Configuration

```
nameif ethernet3 stateful security20
interface ethernet3 100full
ip address lanfover 192.168.253.1 255.255.255.252
failover ip address stateful 192.168.254.2
failover lan unit primary
failover lan interface lanfover
failover lan key 12345678
failover lan enable
failover
```

Frequently Asked Questions About Failover

- General Questions About Failover
- Cable-Based Failover
- LAN-Based Failover
- Stateful Failover Questions

General Questions About PIX Firewall Failover

1. **What are the hardware requirements for Failover configurations?**

   Refer to **Configuration>System Properties>Failover>**
   Introduction to PIX Firewall Failover>Hardware Requirements

2. **How is startup initialization accomplished between two units?**

   The default for failover is Off (no failover). However, if the failover cable is plugged into a unit when it is first booted failover will auto-detect the cable and turn failover on. This is only true at boot time even the failover IP is not configured properly. If the cable is installed to a running PIX, the command "failover" must be issued to start failover.

   (Note, for newer software releases, this can be changed, this is because config replication can accidentally disable the failover with "clear config"). If the failover cable is not present at boot time the unit will immediately become the active unit. However, the unit will show as "Secondary".

   The following discussions assume that failover is enabled and that both units have the failover cable plugged in.

   When a unit first boots it will default to standby and get MAC address from other unit. If no unit has taken active control within 30 seconds, the unit will switch to active. If the unit is primary and the other unit is not active, the primary unit becomes the active unit. This means that if the primary unit and the secondary both complete their bootups within 30 seconds of each other, the primary unit will become active. If the secondary is already active, the primary unit will remain standby (assume the secondary learned the primary MAC before). The primary unit will NOT automatically take active control. With failover enabled, do not boot the secondary unit without first booting the primary one, since the MAC address used is from the primary unit.

   Full configuration replication occurs from the active unit to the standby unit when the standby unit first boots up. From that point on commands are passed from the active to the standby as they are entered. To force a complete configuration replication, use the command "write standby". Any commands entered on the standby unit are NOT replicated to the active unit. A warning message is printed when you enter commands on the standby unit. This is just a warning telling you that the configurations are no longer synchronized.

3. **What constitutes a failure?**
   Fault detection is based on the following:

   - **Network Interface Card (NIC) status**.
     If the Link Status of a NIC is down, the unit will fail. Down means that the NIC is not plugged into an operation port. If a NIC has been configured as 'down', it will not fail this test.
   - **Failover Network communications**.
     The two units send "hello" packets to each other over all network interfaces. If no "hello" packets are heard in 30 seconds the offending interface is put in testing mode to determine who is a fault.
   - **Failover cable communication**.
     The two units send "hello" messages to each other over the failover cable. If the standby doesn't hear from the active within 30 seconds (and the cable status is OK) the standby will take over as active. Also, if failover commands sent over the failover cable are not acknowledged in 15 seconds, the standby will take over as active.
   - **Cable errors**. The failover cable is wired so that each unit can distinguish between:
     - A power failure in the other unit.

        - A cable unplugged this unit.
        - A cable unplugged other unit.
    - If the standby detects that the active is powered off (or reload/reset) it will take active control. If the failover cable is unplugged, a syslog is generated but NO SWITCHING will occur. An exception to this is at boot-up, at which point an unplugged cable will force the unit active. If both units are powered up without the failover cable installed they will both become active creating a duplicate IP address with different MAC which conflict on your network. The failover cable must be installed for failover to work correctly.

4. **How long does it take to detect a failure?**
    - Network communications errors are detected within 30 seconds.
    - Failover communications errors are detected with 30 seconds.
    - Power failure (and cable failure) is detected within 15 seconds

5. **What maintenance is required?**
   Use the **Monitoring>System Graphs>Failover** to monitor the two units' status. System log messages are generated when errors and switches occur.

6. **How do you disable failover?**
   Uncheck Enable Failover in PDM **Configuration>System Properties>Failover**. The failover cable, if used, should also be removed.

7. **What happens when failover is triggered?**
   Either unit can initiate a switchover. When a switch takes place, the units each change their states, as well as the IP address and MAC addresses they are using. From the network's point of view, the standby transparently replaces the previously active unit. Because configuration is already complete on the standby, no updates need to be made. Since the two units do not share dynamic connection states. Any active connections will be dropped when a failover occurs. The clients must reestablish the connections through the newly active unit (unless stateful failover is in use).

   For each switchover, the new active unit sends a syslog for the reason. See the following example:

    - Switching to ACTIVE (cause: no power detected from other side).
    - Other reasons :
        - "normal master",
        - "no failover cable",
        - "no power detected from other side",
        - "unable to talk to the other side",
        - "line interface failed at other side",
        - "do not see traffic count change",
        - "the other side wants me take over",
        - "fail reported by the other side",
        - "state check",
        - "set by the ioctl cm

Cable-Based Failover

- **What happens when failover is triggered?**

  A switch can be initiated by either unit. When a switch takes place, each unit changes state. The newly active unit assumes the IP address and MAC address of the previously active unit and begins accepting traffic for it. The new standby unit assumes the IP address and MAC address of the unit that was previously the standby unit.

- **How is startup initialization accomplished between two units?**

  When a unit boots up, it defaults to Failover Off and secondary, unless the failover connection is present or failover has been saved in the configuration. The configuration from the active unit is also copied to the standby unit. If the cable is not present, the unit automatically becomes the active unit. If a connection is present, the unit that has the primary end of the failover connection plugged into it becomes the primary unit by default.

- **How can both units be configured the same without manually entering the configuration twice?**

  Commands entered on the active unit are automatically replicated on the standby unit.

- **What happens if a primary unit has a power failure?**

  When the primary PIX firewall unit experiences a power failure, the standby PIX Firewall comes up in active mode. If the primary unit is powered on again it will become the standby unit.

- **What constitutes a failure?**
  Fault detection is based on the following:
  - Failover hello packets are received on each interface. If hello packets are not heard for two consecutive 15-second intervals, the interface will be tested to determine which unit is at fault. (You can change this duration with the **failover poll** command.)
  - Cable errors. The cable is wired so that each unit can distinguish between a power failure in the other unit, and an unplugged cable. If the standby unit detects that the active unit is turned off (or resets), it will take active control.

    Note: If the cable is unplugged, a syslog is generated but no switching occurs. An exception to this is at bootup, at which point an unplugged cable will force the unit active. If both units are powered on without the failover connection installed they will both become active creating a duplicate IP address conflict on your network. The failover connection has to be installed for failover to work correctly.

  - Failover communication. The two units share information every 15 seconds, but you can change this duration with the **failover poll** command. If the standby unit does not hear from the active unit in two communication attempts (and the cable status is OK) the standby unit will take over as active.

- **How long does it take to detect a failure?**
  - Network errors are detected within 30 seconds (two consecutive 15-second intervals).
  - Power failure (and cable failure) is detected within 15 seconds.
  - Failover communications errors are detected within 30 seconds (two consecutive 15-second intervals).

- **What maintenance is required?**

  Syslog messages will be generated when any errors or switches occur. Evaluate the failed unit and fix or replace it.

LAN-Based Failover

- **What is the advantage of using LAN-based failover?**

  Using LAN-based failover, the distance between PIX Firewall units can be longer than 6 feet (the maximum Failover Cable length).

- **What is the disadvantage of using LAN-based failover?**
  - The PIX Firewall cannot detect peer failure due to loss of power or reload, so it will take longer for a PIX firewall unit to failover if that happens.
  - User need to configure the secondary PIX firewall unit before it can communicate with the primary unit.

- **Can users put a router between the firewall units when running LAN-based failover?**

  No, Only switch/hub/VLAN are allowed. All interfaces of the two units still need to be on the same subnet.

- **What happens if the interface for LAN-based failover is down?**

  If the LAN-based failover command interface link goes down, then the PIX Firewall notifies the peer through "other" interfaces, and if the active PIX Firewall's interface goes down, then the standby unit will take over.

Note: When the command interface goes down and the PIX Firewall becomes a standby unit, the PIX Firewall cannot become active until the interface comes back up again

---

- **What happens if the connectivity of LAN-based failover command interface is down due to reasons other than the link down (for example, each PIX is connected to a separate switch and two switches are connected using ISL).**

  The PIX Firewall will try to use "other" interfaces to poll the peer status, and then failover if necessary.

- **Is it possible to have both PIX firewall unites become active at the same time?**

  If all connectivity between the two PIX firewall units is lost, then this can happen. Therefore, it is best to use a separate switch/hub for the LAN-based failover command interface, so a failed switch will not cause all connectivity to be lost between the two Cisco firewall units.

▲

Stateful Failover Questions

- **What causes Stateful Failover to occur?**
  - A power off or a power down condition on the active PIX Firewall.
  - Reboot of the active PIX Firewall.
  - A link goes down on the active PIX Firewall for more than twice the configured poll time or a maximum of 30 seconds.
  - "Failover active" on the standby PIX Firewall.
  - Block memory exhaustion for 15 consecutive seconds or more on the active unit.

- **What information is replicated to the standby PIX Firewall on Stateful Failover?**
  - The configuration.
  - TCP connection table including timeout information of each connection.
  - Translation (xlate) table.
  - System up time; that is, the system clock is synchronized on both PIX firewall units.

- **What information is not replicated to the standby PIX Firewall on Stateful Failover?**
  - The user authentication (uauth) table.
  - The ISAKMP and IPSec SA table.
  - The ARP table.
  - Routing information.

- **What are Stateful Failover hardware requirements?**
  - Two identical PIX firewall units with a Fast Ethernet or Gigabit Ethernet LAN port dedicated to Stateful Failover are required. Connect the LAN ports for Stateful Failover on both PIX firewall units with a crossover cable or through a switch. Full duplex is required between the Stateful Failover ports.
  - For better performance, a PIX Firewall 520 or later model of PIX Firewall is recommended.
  - You need a dedicated LAN connection or a Failover cable to connect the two failover ports on both PIX firewall units.

- **What are Stateful Failover hardware restrictions?**
  - A PIX Firewall with two FDDI cards cannot use Stateful Failover because an additional Ethernet interface with FDDI is not supported.
  - The dedicated LAN connection or Failover cable should be installed and be working correctly.
  - The dedicated Fast Ethernet or Gigabit Ethernet ports on both PIX firewall units to use Tera Term Pro with SSH be

connected and fully functional.

- **What are Stateful Failover software requirements?**
  - PIX Firewall version 5.1 or later is required for Stateful Failover.
  - Both PIX firewall units should run the same version of PIX Firewall software.

- **What are Stateful Failover license requirements?**

  Stateful Failover requires a feature-based license key with failover feature support or connection-based license key.

Copyright © 2001-2004, Cisco Systems, Inc.

Password

Configuration>System Properties>Administration>Password

The **Password** panel lets you set the **enable** and **telnet** passwords.

The following sections are included in this Help topic:

- Important Notes About Passwords
- Field Descriptions
- Changing Enable Passwords
- Changing Telnet Passwords
- Applying Changes

In addition to PDM, administrators can use Command Line Interface (CLI) console sessions. One of the following types of preconfigured connections must be used for CLI console sessions:

1. Serial console port—PC with serial interface and terminal emulation software connected directly to the console port of the firewall.
2. Telnet protocol—A network connection using the Telnet protocol.
3. PDM/HTTPS protocol—A network connection using the HTTPS (Hypertext Transfer Protocol-Secure) protocol for **Tools>Command Line Interface**. Note: PDM uses HTTPS for all communication with the firewall.
4. Secure Shell (SSH) protocol—A network connection using the Secure Shell (SSH) protocol.

RADIUS or TACACS+ servers may be defined to authenticate any of these connection types. See PIX Administrative AAA Authentication for more information.

The **enable** password is set to authenticate administrators using the Command Line Interface for management to enter the privilege mode required to view and modify the configuration. The same password is also used by PDM to authenticate an administrator. When using Serial, Telnet, or SSH, the **enable** password is required to enter privilege mode after other authentication allows connection.

The **Telnet** password is set to authenticate administrators using the Telnet protocol for management. The same password is also used to define authentication for administrators using SSH if PIX Administrative AAA Authentication is not defined for the SSH protocol. The default password is cisco.

To gain access to the console via SSH, at the SSH client, enter the username as pix and enter the Telnet password. Note: SSH permits up to 100 characters in a username and up to 50 characters in a password.

For more information, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

Important Notes About Passwords

1. It is important to set the passwords on each PIX Firewall you deploy.
2. All passwords should be set in accordance with the password security policy of your organization. If you do not have one, please refer to these guidelines for password security policy.
3. PIX passwords may be a maximum of 16 characters in length. SSH permits up to 100 characters in a username and up to 50 characters in a password.
4. PIX password characters can consist of alphanumeric or special characters except for the question mark or space.
5. PIX passwords are case-sensitive, for example, an uppercase "A" is recognized differently from a lowercase "a".
6. Make sure caps lock or num lock on your keyboard is not set when entering passwords.
7. Choose strong passwords. Avoid weak passwords. Passwords should not be any word or syllable that would be found in the dictionary of common languages, the word "password", your date of birth, organization name, or anything very easy to guess about you or your organization.
8. Write down new passwords and store them in a manner consistent with the password security policy of your organization. Once you change a PIX password, you cannot view it again.
9. PIX passwords may be entered in encrypted form.

Field Descriptions

The **Password** panel provides the following fields:

Enable (and PDM) Password region

- **Old Password**—Enter previous 16 character, case-sensitive password.
- **New Password**—Enter a new 16 character, case-sensitive password. See Important Notes About Passwords.
- **Confirm New Password**—Reenter your new password.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Note: Ensure that all users who access the console are given this password.

Telnet (and non-AAA authenticated SSH) Password region

- **Old Password**—Enter previous 16 character, case-sensitive password.
- **New Password**—Enter a new 16 character, case-sensitive password. See Important Notes About Passwords.
- **Confirm New Password**—Reenter your new password.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Note: Write down the new passwords and store it in a manner consistent with your site's password security policy. Once you change the passwords, you cannot view them again.

Changing Enable (and PDM) Passwords

Follow these steps to change **Enable** (and PDM) passwords:

1. In the **Old Password** box, enter in a 16 character, case-sensitive password. See Important Notes About Passwords.
2. In the **New Password** box, enter in a 16 character, case-sensitive password.
3. In the **Confirm New Password** box, reenter your new password.

Changing Telnet Passwords

Follow these steps to change **Telnet** (and non-AAA server authenticated SSH) passwords:

1. In the **Old Password** box, enter in a 16 character, case-sensitive password. See Important Notes About Passwords.
2. In the **New Password** box, enter in a 16 character, case-sensitive password.
3. In the **Confirm New Password** box, reenter your new password.

Applying Changes

If you do not wish to apply your recent change to the configuration click:

Reset—Discards changes and reverts the panel to the information displayed when it was opened or

the last time **Refresh** was clicked while open.

Changes are not immediately applied to the running configuration. To apply your changes:

Apply—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

Copyright © 2001-2004, Cisco Systems, Inc.

PDM/HTTPS

Configuration>System Properties>Administration>PDM/HTTPS

The **PDM/HTTPS** panel lets you configure rules that permit only specific hosts or networks running PDM to connect to the firewall using Hypertext Transfer Protocol, Secure (HTTPS).

The following sections are included in this Help topic:

- Field Descriptions
- Adding Rules
- Editing Rules
- Deleting Rules
- Applying Changes

A secure connection is needed so that a PC or workstation client running PDM in a network browser window can communicate with the firewall. The rules restrict PDM/HTTPS access through a firewall interface to a specific IP address and netmask. PDM/HTTPS connection attempts that comply with the rules must then be authenticated using a preconfigured AAA server or the enable password. Once established, data is encrypted using the Secure Sockets Layer (SSL) protocol. You can monitor PDM/HTTPS sessions using Monitoring>PDM Users. Refer to Multiple PDM and CLI Console Sessions.

Field Descriptions

The **PDM/HTTPS** panel displays the following fields in a rule table:

- **Interface**—Displays the name of a firewall interface which will permit PDM/HTTPS connections, an interface on which is located a PC or workstation running PDM.
- **IP Address**—Displays the IP address of each host or network permitted to connect to this PIX through the specified interface. Note: This is not the IP address of the firewall interface.
- **Netmask**—Displays the netmask for the IP address of each host or network permitted to connect to this PIX through the specified interface. Note: This is not a netmask for the IP address of the firewall interface.

- **Add**—Opens the **Add** dialog box.
- **Edit**—Opens the **Edit** dialog box.
- **Delete**—Deletes the selected item.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover

standby firewall unit. See Configuration Changes.

- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Cisco Easy VPN Remote

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Adding PDM/HTTPS Rules

Follow these steps to add a rule to the PDM/HTTPS rule table:

1. Click on **Add** to open the **PDM/HTTPS>Add** dialog box.
2. Click on **interface** to add a firewall interface to the rule table.
3. Enter the **IP address** of the host running PDM which will be permitted HTTPS access through this Firewall interface. Note: This is not the IP address of the firewall interface.
4. Select or enter a **netmask** for the IP address to be permitted HTTPS access. Note: This is not a mask for the IP address of the firewall interface.
5. To return to the previous panel click:
   - **OK**—Accepts changes and returns to the previous panel.
   - **Cancel**—Discards changes and returns to the previous panel.
   - **Help**—Provides more information.

Editing PDM/HTTPS Rules

Follow these steps to edit a rule to the PDM/HTTPS rule table:

1. Click on **Edit** to open the **PDM/HTTPS>Edit** dialog box.
2. Click on **interface** to add or change a firewall interface to the rule table.
3. Enter the **IP address** of the host running PDM which will be permitted HTTPS access through this Firewall interface. Note: This is not the IP address of the firewall interface.
4. Select or enter a **netmask** for the IP address to be permitted HTTPS access. Note: This is not a mask for the IP address of the firewall interface.
5. To return to the previous panel click:
   - **OK**—Accepts changes and returns to the previous panel.
   - **Cancel**—Discards changes and returns to the previous panel.
   -

Help—Provides more information.

Deleting PDM/HTTPS Rules

Follow these steps to delete a rule from the PDM/HTTPS table:

1. Select a rule from the PDM/HTTPS rule table.
2. Click the **Delete** button**.**

Applying Changes

Changes to the table made by **Add**, **Edit**, or **Delete** are not immediately applied to the running Firewall configuration. You must click on one of the following buttons to apply or discard changes:

1. **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
2. **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

PDM Users

Monitoring>PDM Users

The **PDM Users** panel allows you to monitor connections made to the firewall using PIX Device Manager (PDM). A snapshot of the current PDM user sessions to the firewall is displayed. The display is not automatically updated as new PDM user sessions are created. To view new PDM user sessions, you must click **Refresh**.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Disconnecting PDM User Sessions

Important Notes

Be careful not to accidentally disconnect your own PDM session by selecting your IP address and clicking **Disconnect**.

Field Descriptions

The **PDM Users** panel displays the following fields:

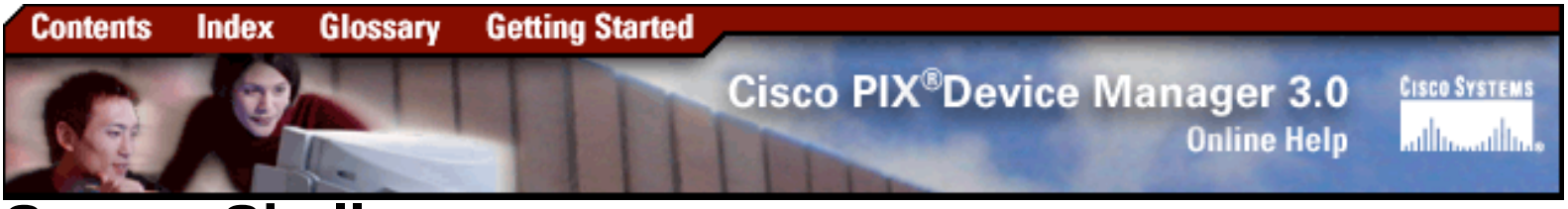
- **Session ID**—Displays a unique number that identifies each PDM user session.
- **IP Address**—Displays the IP address of the client connected to the firewall, via PDM. If PDM knows the client host name associated with the IP address, the host name will appear in this field.
- **Refresh**—Refreshes the current display by retrieving the PDM Users currently connected to the PIX.
- **Disconnect**—Disconnects the PDM User session currently selected in the table. Note that by disconnecting a PDM user session, the user that is disconnected will receive an error message on their PDM screen and, after the user acknowledges the error, their PDM applet will be terminated. Any unapplied configuration changes made by that user will be lost.

Disconnecting PDM User Sessions

Follow these steps to disconnect:

1. Select a PDM User session from the table.
2. Click **Disconnect**.
3. Click **Refresh** to verify that the PDM session has been disconnected.

Copyright © 2001-2004, Cisco Systems, Inc.



Secure Shell

Configuration>System Properties>Administration>Secure Shell

The **Secure Shell** panel lets you configure rules that permit only specific hosts or networks to connect to the firewall unit for administrative access using the Secure Shell (SSH) protocol.

The following sections are included in this Help topic:

- Field Descriptions
- Adding Rules
- Editing Rules
- Deleting Rules
- Applying Changes

The rules restrict SSH access through a firewall interface to a specific IP address and netmask. SSH connection attempts which comply with the rules must then be authenticated by a preconfigured AAA server or the Telnet password. You can monitor SSH sessions using Monitoring>Secure Shell Sessions.

Field Descriptions

The **Secure Shell** (SSH) panel displays the following fields:

Secure Shell Rule Table:

- **SSH Timeout (minutes)**—Displays the number of minutes, 1 to 60, the Secure Shell session can remain idle before the firewall unit closes it. The default is 5 minutes.
- **IP Address**—Displays the IP address of each host or network permitted to connect to this firewall through the specified interface. Note: This is not the IP address of the firewall interface.
- **Mask**—Displays the netmask for the IP address of each host or network permitted to connect to this firewall through the specified interface. Note: This is not a netmask for the IP address of the firewall interface.
- **Interface**—Displays the name of a firewall interface which will permit SSH connections, an interface on which is located a PC or workstation running PDM.
- **Add**—Opens the **Add Secure Shell Configuration** dialog box.
- **Edit**—Opens the **Edit Secure Shell Configuration** dialog box.
- **Delete**—Deletes the selected item.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last

time **Refresh** was clicked while open.

Cisco Easy VPN Remote

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Adding Secure Shell Rules

Follow these steps to add a rule to the Secure Shell rule table:

1. Click the **Add** button to open the **Add** dialog box.
2. Add a firewall interface to the rule table.
3. Enter the **IP address** of the host running PDM which will be permitted SSH access through this Firewall interface. Note: This is not the IP address of the firewall interface.
4. Select or enter a **netmask** for the **IP address** to be permitted SSH access. Note: This is not a mask for the IP address of the firewall interface.
5. To return to the previous panel click:
   - **OK**—Accepts changes and returns to the previous panel.
   - **Cancel**—Discards changes and returns to the previous panel.
   - **Help**—Provides more information.

Editing Secure Shell Rules

Follow these steps to edit a rule in the Secure Shell rule table:

1. Click the **Edit** button to open the **Edit** dialog box.
2. Select a firewall interface from the rule table.
3. Enter the **IP address** of the host running PDM which will be permitted SSH access through this Firewall interface. Note: This is not the IP address of the firewall interface.
4. Select or enter a **netmask** for the **IP address** to be permitted Secure Shell access. Note: This is not a mask for the IP address of the firewall interface.
5. To return to the previous panel click:
   - **OK**—Accepts changes and returns to the previous panel.
   - **Cancel**—Discards changes and returns to the previous panel.
   - **Help**—Provides more information.

Deleting Secure Shell Rules

Follow these steps to delete a rule from the Secure Shell table:

1. Select a rule from the Secure Shell rule table.
2. Click **Delete**.

Applying Changes

Changes to the table made by **Add**, **Edit**, or **Delete** are not immediately applied to the running Firewall configuration. You must click on one of the following buttons to apply or discard changes:

1. **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
2. **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Secure Shell Sessions

Monitoring>Secure Shell Sessions

The **Secure Shell Sessions** panel lets you monitor connections made to the firewall using Secure Shell (SSH). When the **Secure Shell** panel is displayed, a snapshot of the current Secure Shell sessions to the firewall is available . The display is not automatically updated as new Secure Shell sessions are created. To view new Secure Shell sessions, you must click Refresh.

The following sections are included in this Help topic:

- Field Descriptions
- Disconnecting Secure Shell Sessions

Field Descriptions

The **Secure Shell Sessions** panel displays the following fields:

- **IP Address**—Displays the IP address of the client connected to the firewall via SSH. If PDM knows the client hostname associated with the IP address, the host name will appear under IP Address in the table.
- **Ver**—Displays the version of SSH being used by the client.
- **Type**—Displays the type of encryption the SSH client is using (for example, DES, 3DES).
- **State**—Displays the progress the client is making in its SSH connection to the firewall. State values are as follows:
  - 0 = SSH_CLOSED
  - 1 = SSH_OPEN
  - 2 = SSH_VERSION_OK
  - 3 = SSH_SESSION_KEY_RECEIVED
  - 4 = SSH_KEYS_EXCHANGED
  - 5 = SSH_AUTHENTICATED
  - 6 = SSH_SESSION_OPEN
  - 7 = SSH_TERMINATE
  - 8 = SSH_SESSION_DISCONNECTING
  - 9 = SSH_SESSION_DISCONNECTED
  - 10 = SSH_SESSION_CLOSED
- **User**— Displays the username of the client accessing the firewall. The "pix" username appears when an SSH client is accessing the firewall console.
- **ID**—Displays a unique number that identifies each SSH session.
- **Disconnect**—Disconnects the Secure Shell session currently selected in the table.

- **Refresh**—Refreshes the information on the current panel.

Disconnecting Secure Shell Sessions

Follow these steps to disconnect an existing SSH session:

1. Select an SSH session from the table.
2. Click **Disconnect**.
3. Click **Refresh** to verify that the SSH session has been disconnected.

Copyright © 2001-2004, Cisco Systems, Inc.

Password Security Policy

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of an entire private network. As such, all users of the private network share responsibility for taking the appropriate steps to select and secure their passwords. If your organization does not have a well defined policy regarding the management of passwords. This help topic provides some suggested guidelines.

The following sections are included in this Help topic:

- Suggested Guidelines for Password Security Policy
- Password Construction
  - Weak Passwords
  - Strong Passwords
- Password Protection
- Passphrases
- Password Security Audits

- Network Security Policy: Best Practices White Paper
- More **TAC Resources>Network Security Emergency Response, Advisory Organizations**

Note: For information about the technical requirements for firewall passwords, see **System Properties>Administration>Passwords>Important Notes About Firewall Passwords**.

Suggested Guidelines for Password Security Policy

1. All system-level passwords, including root, enable, OS admin, VPN dial in, PDM and application administration accounts, should be changed on at least a quarterly basis.
2. All production system-level passwords should be part of a globally administered password management database.
3. All user-level passwords, such as email, Web, and desktop computer, should be changed at least every six months. The recommended change interval is every four months.
4. User accounts which have system-level privileges granted through group memberships should have a unique password from all other accounts held by that user.
5. Use automated password update tools to encourage user to change passwords.
6. Passwords should not be inserted into email messages or other forms of electronic communication.
7. Where SNMP is used, the community strings should be defined as something other than the standard

defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (for example, SNMPv2).
8. Common names, such as your organization, or numbers, such as your personal name, birthday, house number or any derivation thereof must not be used as a password.
9. All user-level and system-level passwords must conform to the guidelines described that follow.

Password Construction Guidelines

- Passwords are used for various purposes. Some of the more common uses include the following:
- user level accounts
- web accounts
- email accounts
- screen saver protection
- voicemail password
- local router login
- Firewall CLI or PDM logins

Because very few systems have support for one-time tokens or dynamic passwords which are only used once, everyone should be aware of how to select strong passwords.

Weak Passwords

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)

The password is a common usage word such as:

- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- Your location, for example "sanjose", "sanfran" "sfo", "sjo", or similar derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the preceding spelled backwards.
- Any of the preceding preceded or followed by a digit (for example, secret1, 1secret)

Strong Passwords

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (for example, a-z, A-Z)
- Have digits and punctuation characters as well as letters (for example, 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./) Avoiding the use of characters beyond the standard ASCII characters. The pound sterling symbol (£) has been documented to cause login problems on some systems.
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.

- Are not based on personal information, names of family, etc.
- Are not used in movies, television, or public media.
- Are not published examples of suggested passwords.

Passwords should never be written down or stored online. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase, such as a song phrase. Here is an example using a song phrase, "This May Be One Way To Remember": "TmB1w2R!" or "Tmb1W>r~" are two relatively strong passwords which are made easier to remember by the phrase.

NOTE: Do not use either of these examples as passwords!

Password Protection Guidelines

Do not use the same password for work as for other non-work access, such as personal ISP accounts, option trading, benefits. Where possible, do not use the same password for multiple work access needs. For example, select one password for Engineering systems and a separate password for IT systems. Also, select a separate password to be used for accounts on each type of operating system you use.

Do not share passwords with anyone, including coworkers or friends. All passwords should be treated as sensitive, confidential information.

Here is a list of "do nots":

- Do not reveal a password over the phone to ANYONE
- Do not reveal a password in an email message or customer service case record
- Do not reveal a password to the boss
- Do not talk about a password in front of others
- Do not hint at the format of a password (for example, "my family name")
- Do not reveal a password on questionnaires or security forms
- Do not share a password with family members
- Do not reveal a password to co-workers while on vacation

If someone demands a password, refer them to your organization's Password Policy document or have them call someone in your IT or Information Security Department.

Do not use the "Remember Password" feature of applications such as Eudora, Netscape Messenger.

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months. If an account or password is suspected to have been compromised, report the incident to IT or Information Security Department and change all passwords.

Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

```
"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"
```

All of the preceding rules that apply to passwords apply to passphrases.

Password Security Audits

It is recommended that properly trained IT or Information Security Department representatives periodically or randomly conduct network security audits, including password strength. If a password is guessed or cracked during one of these scans, the user will be required to change it and encouraged to use stronger passwords in the future.

See Network Security Policy: Best Practices White Paper

Copyright © 2001-2004, Cisco Systems, Inc.

More ▸ TAC Resources for PIX Firewall

Cisco Technical Assistance Center (TAC) provides specific support resources for firewalls managed by PDM. For more information, see **More ▸ Obtaining Technical Assistance>TAC**.

Note: These are external links, unless otherwise noted.

The following sections are included in this Help topic:

TAC Firewall Support

- TAC Home Page
- PIX Product Support Page
- PIX FAQ (Frequently Asked Questions)
- PIX Software Upgrades
- DES (Data Encryption Standard) License
- TAC Sample Configurations for PIX Firewall, **More ▸ Example Configurations**
- PIX Top Issues (and Sample Configurations)
- PIX Hardware Support Library
- PIX Hardware Troubleshooting Registered | Public
- PIX Firewall Performance Monitoring
- Intrusion Detection Systems (IDS)
- More PIX Firewall Technical Tips

- Catalyst FWSM (Firewall Services Module)
- Catalyst Best Practices
- Troubleshooting Catalyst Switch Hardware
- Troubleshooting Switch Ports
- Catalyst Error Messages

- Internetworking Troubleshooting Guide
- TAC LAN Technologies Top Issues

▲

Security Emergency, Attack, Viruses

- Network Security Policy: Best Practices White Paper
- Security Product Field Notices (including PIX)
- Security Customer Email Notices
- PSIRT (Product Security Incident Response Team)
    - Advisories
    - Non-emergency Contact
    - Emergency Contact
- Computer Security Organizations
    - CERT/CC (Computer Emergency Response Team/Coordination Center)
    - FIRST (Forum of Incident Response and Security Teams)
    - ISA (Internet Security Alliance)

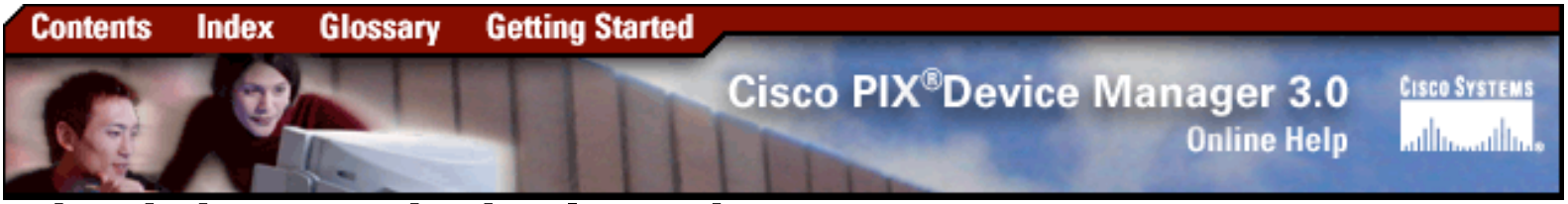
TAC Firewall VPN Support

- PIX VPN Top Issues (and Sample Configurations), More **VPN**
- TAC IPSec Support
- DES Licenses for IPSec
- Certificate Authorities - How to enroll from a PIX.
- Cisco VPN Client (3.x and later)
- IP Security Troubleshooting - Understanding and Using debug Commands
- TAC Online Newsletter

Reference

- Requests for Comments (RFCs)
- PIX Firewall Documentation
- PIX Firewall Design Guides
- Cisco Documentation Orders and Subscriptions
- PIX Command Reference
- Catalyst 6000 Documentation
- Cisco Network Security Products
- Cisco SNMP MIB Documentation
- Networking Professionals Forum

Copyright © 2001-2004, Cisco Systems, Inc.



Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

The following sections are included in this Help topic:

- Cisco.com
- Technical Assistance Center (TAC)
  - TAC Website
  - TAC Escalation Center
- Documentation
  - Ordering Documentation
  - Documentation Feedback

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:
http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center. Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- **Priority level 4 (P4)**—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- **Priority level 3 (P3)**—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- **Priority level 2 (P2**)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- **Priority level 1 (P1**)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site lets you resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:
http://www.cisco.com/tac

PDM Help> More **TAC Resources for PIX Firewall** provides quick access to some of the most popular TAC links for PIX Firewall support.

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:
http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL: http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these

classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

PIX Documentation

- PIX Firewall Documentation
- PIX Firewall Product Literature
- PIX Command Reference
- PIX Software Updates
- DES (Data Encryption Standard) License
- Upgrading Configurations
- PIX Bug Navigator II

- PIX Firewall-TAC Home
- Security Product Field Notices (including PIX)
- PIX Firewall Technical Tips
- PIX Firewall Top Issues

- TAC Security Tools
- IPSec VPN Support
- IPSec Technical Tips

- More **TAC Resources for PIX Firewall**

Ordering Documentation

Cisco documentation is available in the following ways:

Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace: http://www.cisco.com/cgi-bin/order/order_root.pl

Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

http://www.cisco.com/go/subscription

Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click the Fax or Email option under the “Leave Feedback” at the bottom of the Cisco Documentation home page.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Copyright © 2001-2004, Cisco Systems, Inc.

Introductory Configurations

- Factory Default Configuration
- TAC Sample Configurations
- Troubleshooting Basic Firewall Configuration
- Using the PDM Ping Tool for Troubleshooting
- LAN-Based Failover
- PIX Firewall Design Guides

VPN Configurations

- PIX VPN Top Issues (and sample configurations)
- Configuring a Simple PIX to PIX VPN Tunnel Using IPSec
- Configuring the VPN 3002 Hardware Client to PIX Firewall 6.0.X
- Cisco Hardware and VPN Clients Supporting IPSec/PPTP/L2TP
- Configuring IPSec Between Two PIX Firewalls and a VPN Client with Extended Authentication
- Configuring Cisco IOS(R)-to-VPN 5000 Site-to-Site Tunnels Using IP Security (IPSec) Reliable Mode with Cisco IOS(R) 12.1.x or Later
- Configuring a Central Cisco VPN 3000 Concentrator to Allow Communication Between Spokes
- Configuring Cisco PIX(R)-to-Router Dynamic-to-Static IP Security (IPSec) with Network Address Translation (NAT)

- More ▸ **TAC Resources for PIX Firewall**
- More ▸ **VPN**

Reference

- Documentation for PIX Firewall
- PIX Command Reference
- Catalyst 6000 Documentation
- Cisco SNMP Documentation

- Requests for Comments (RFCs)

- Obtaining Technical Assistance ▸

Factory Default Configuration

See File>Reset Firewall to Factory Default Configuration.

This example shows the output of the **show running-config** command for the PIX Firewall 501 with 10-user licenses. The DHCP server and HTTP configuration actually varies if you provide an inside IP address.

show running-config

```
Building configuration...
: Saved
:
PIX Version 6.2(0)247
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
pager lines 24
interface ethernet0 10baset
interface ethernet1 10full
mtu outside 1500
mtu inside 1500
ip address outside dhcp setroute
ip address inside 192.168.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm logging informational 100
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
timeout xlate 0:05:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
```

```
http server enable
http 192.168.1.1 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
no sysopt route dnat
telnet timeout 5
ssh timeout 5
dhcpd address 192.168.1.2-192.168.1.33 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd auto_config outside
dhcpd enable inside
terminal width 80
Cryptochecksum:839509d6df72f5d255f2715e0a986673
: end
[OK]
```

LAN-Based Failover

LAN-Based Failover Primary Unit Configuration

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 stateful security10
nameif ethernet3 lanfover security20
enable password xxx encrypted
passwd xxx encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 20
no logging timestamp
no logging standby
logging console errors
no logging monitor
no logging buffered
no logging trap
logging facility 20
logging queue 512
```

```
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
interface ethernet3 100full
mtu outside 1500
mtu inside 1500
mtu failover 1500
mtu unused 1500
ip address outside 209.165.201.1 255.255.255.224
ip address inside 192.168.2.1 255.255.255.0
ip address failover 192.168.254.1 255.255.255.0
ip address unused 192.168.253.1 255.255.255.252
failover
failover ip address outside 209.165.201.2
failover ip address inside 192.168.2.2
failover ip address stateful 192.168.254.2
failover ip address lanfover 192.168.253.2
failover link stateful
failover lan unit primary
failover lan interface lanfover
failover lan key 12345678
failover lan enable
arp timeout 14400
global (outside) 1 209.165.201.3 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 209.165.201.5 192.168.2.5 netmask 255.255.255.255 0 0
access-list acl_out permit tcp any 209.165.201.5 eq 80
access-list acl_out permit icmp any any
access-group acl_out in interface outside
access-list acl_ping permit icmp any any
access-group acl_ping in interface inside
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
no rip failover passive
no rip failover default
route outside 0 0 209.165.201.4 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
telnet timeout 5
terminal width 80
```

LAN-Based Failover Secondary Unit Configuration

```
nameif ethernet3 stateful security20
interface ethernet3 100full
ip address lanfover 192.168.253.1 255.255.255.252
failover ip address stateful 192.168.254.2
failover lan unit primary
failover lan interface lanfover
failover lan key 12345678
failover lan enable
failover
```

Troubleshooting Basic Firewall Configuration

These documents from Cisco TAC (Technical Assistance Center) combine the strength of step-by-step troubleshooting guidance with embedded links the Cisco Output Interpreter tool which can provide customized analysis of your Cisco device using output from the **show config** command in **Tools>CLI**.

With these interactive documents, you can read about technical issues, paste your own **show** command output into the Output Interpreter, and see precisely how the documentation relates to your situation. The Output Interpreter's analysis will point out specific configuration or performance issues and give you suggestions for resolution, speeding you through the troubleshooting process.

- Configuring the Cisco PIX Firewall with a Single Internal Network
  http://www.cisco.com/tac/newsflash/041802_secure_pix_seg8.html
- Configuring the Cisco PIX Firewall with Two Internal Networks
  http://www.cisco.com/tac/newsflash/041802_pix_firewall_seg8.html
- Configuring the Cisco PIX Firewall with Three Internal Networks
  http://www.cisco.com/tac/newsflash/041802_secure_pix_firewall_seg8.html
- Configuring the Cisco PIX Firewall with Two Routers
  http://www.cisco.com/tac/newsflash/041802_conf_secure_pix_firewall_seg8.html

- Using NAT and PAT Statements on the Cisco PIX(R) Firewall
  http://www.cisco.com/tac/newsflash/041802_nat_pat_statements_seg8.html
- Configuring a Simple PIX to PIX VPN Tunnel Using IPSec
  http://www.cisco.com/tac/newsflash/041802_simple_pix_seg8.html

More **TAC Resources.**

Copyright © 2001-2004, Cisco Systems, Inc.

VPN Tutorial, Resources and Reference

The following sections are included in this Help topic:

Cisco PIX Firewall VPN Standards

- **IPSec** RFC 2401
  - Modes
  - Terms
  - RFCs
  - PIX IPSec Standards
- **Internet Key Exchange** (IKE) RFC 2409
  - IKE Crypto Components
  - PIX IKE Standards
- **Certificates**, **Authorities** ITU X.509
  - **Certificates**
  - **RSA** Public Key Cryptography Standards PKCS# 7, 1
  - **CA** (Certificate Authorities)
  - PIX CAs Supported
- VPN Terms
- VPN Help Topic
- More ▸ **TAC Resources for PIX Firewall**
- Obtaining Technical Assistance ▸

VPN Configuration and Troubleshooting

- TAC PIX VPN Top Issues (and Sample Configurations)
- TAC Top VPN Issues
- Cisco Network Security Products
- TAC IPSec Support
- IP Security Troubleshooting - Understanding and Using debug Commands

Reference

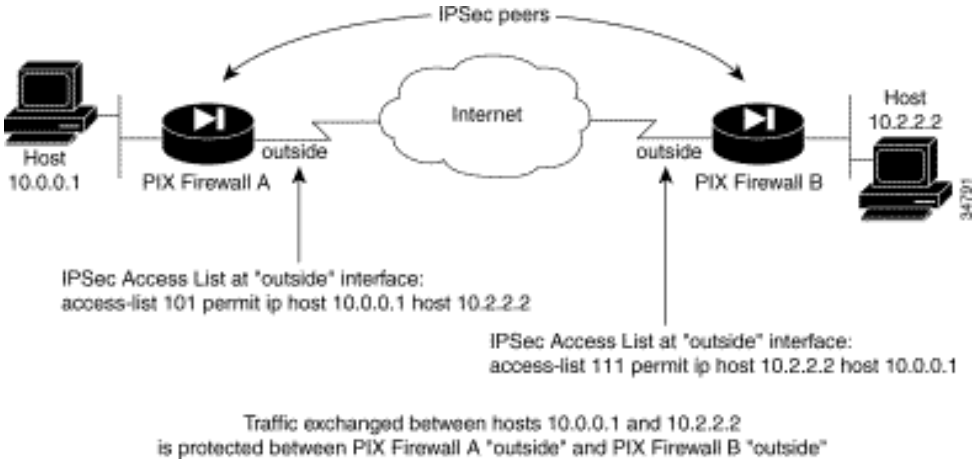
- PIX Documentation
- Network Security Policy: Best Practices White Paper
- Requests for Comments (RFCs)

- Internet Security Glossary (RFC 2828)
- PIX Command Reference

Cisco PIX Firewall VPN Standards

IPSec

IP Security Protocol. IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers in a VPN.. IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.



IPSec Modes

IPSec operates in two modes:

- **Transport Mode**—An encapsulation mode for AH/ESP. Transport Mode encapsulates the upper layer payload (such as Transmission Control Protocol (TCP) or User Datagram Protocol (UDP)) of the original IP datagram. This mode can only be used when the peers are the endpoints of the communication. The contrast of Transport Mode is Tunnel Mode.
- **Tunnel Mode**—Encapsulation of the complete IP Datagram for IPSec. Tunnel Mode is used to protect datagrams sourced from or destined to non-IPSec systems (such as in a Virtual Private Network (VPN) scenario).

IPSec Phases

IPSec operates in two phases:

Phase 1—The first phase of negotiating IPSec, which includes the key exchange, and the ISAKMP portions of IPSec.

Phase 2—The second phase of negotiating IPSec, where ecryptions occurs. Phase two determines:

1. What encryption rules will be used for payload
2. What source and destination will be used for encryption
3. What defines interesting traffic, according to access lists
4. The IPSec peer.

Phase two is where IPSec is applied to the interface.

IPSec Terms

- **Authenticate, Authentication**—Cryptographic protocols and services which verify the identity of users and the integrity of data. One of the functions of the IPSec framework. Authentication establishes the integrity of datastream and ensures that it is not tampered with in transit. It also provides confirmation about datastream origin.See AH, AH Authentication, AAA, encryption,VPN, encryption.
- **CA**—Certificate Authority, Certification Authority. A third-party entity that is responsible for issuing and revoking certificates. Each device that has its own certificate and public key of the CA can authenticate every other device within a given CA's domain. This term is also applied to server software that provides these services. A trusted source which issues Digital Certificates.
- **Certificate**—A cryptographically signed object that contains an identity and a public key associated with this identity
- **Certificate Revocation List (CRL)**—A digitally signed message that lists all of the current but revoked certificates listed by a given CA. This is analogous to a book of stolen charge card numbers that allow stores to reject bad credit cards.
- **Classic crypto**—Cisco proprietary encryption mechanism used in Cisco IOS release 11.2. Classic crypto will be available in Cisco IOS release 11.3, however, IPSec will not be "retrofitted" to Cisco IOS release 11.2. You may also see the name "classic crypto" referred to as "Encryption Express" or "Cisco Encryption Technology" (CET) in the marketing literature.
- **Cryptography, crypto, cryptographic services**—Encryption, authentication, integrity, keys and other services used for secure commmunications over networks. See VPN, IPSec.
- **Crypto map**—A crypto map is applied to an interface. A data structure with a unique name and sequence number which is used for configuring VPNs on the firewall. A Crypto Map performs two primary functions:(1) it selects data flows that need security processing and (2) defines the policy for these flows and the crypto peer that traffic needs to go to. The concept of a crypto map was introduced in Cisco's classic crypto for IOS but was expanded for IPSec. Crypto maps contain the ACLs, encryption standards, peers, and other parameters necessary to specify security policies for VPNs using IKE and IPSEC.
- **Data integrity**—Data integrity mechanisms, through the use of secret key based or public key based algorithms, that allow the recipient of a piece of protected data to verify that the data has not been modified in transit.
- **Data confidentiality**—Method where protected data is manipulated so that no attacker can read it. This is commonly provided by data encryption and keys that are only available to the parties involved in the communication.
- **Data origin authentication**—A security service where the receiver can verify that protected data could have originated only from the sender. This service requires a data integrity service plus a key distribution

mechanism, where a secret key is shared only between the sender and receiver.

- **Encryption**, **Decryption**—Application of a specific algorithm or *cipher* to data, *cleartext*, so as to alter the appearance of the data making it incomprehensible, *ciphertext*, to those who are not authorized to see the information without a public key, pre-shared key, or other means of *deciphering* it. The encryption algorithms supported by the firewall include DES, 3-DES (triple DES). See PIX Firewall Requirements.
- **Hash, Hash Algorithm**—A hash algorithm is a one way function which operates on a message of arbitrary length to to create a fixed length message digest used by cryptographic services to ensure its data integrity. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has been a successful (but extremely difficult) attack demonstrated against MD5. Cisco uses both Secure Hash Algorithm (SHA) and Message Digest 5 (MD5) hashes within our implementation of the IPSec framework. See VPN, encryption, HMAC.
- **Key, Cryptographic key**—A data object used for encryption, decryption and/or authentication. Keys are only available to the parties involved in the communication.
- **Message Digest**—A message digest is created by a hash algorithm , such as MD5 or SHA-1, which is used for ensuring message integrity. MD5 has a smaller digest and is considered to be slightly faster than SHA-1.
- **Replay-detection**—A security service where the receiver can reject old or duplicate packets in order to defeat replay attacks (replay attacks rely on the attacker sending out older or duplicate packets to the receiver and the receiver thinking that the bogus traffic is legitimate). Replay-detection is done by using sequence numbers combined with authentication, and is a standard feature of IPSec.
- **Security Association (SA)**—An instance of security policy and keying material applied to a data flow.
- **Security Services**—See cryptographic services.
- **Transform**—A transform describes a security protocol, such as AH or ESP, with its corresponding algorithms. For example, ESP with the DES cipher algorithm and HMAC-SHA for authentication.
- **Transform, Transform Set**—A transform set specifies the cryptographic services to use on traffic matching the IPSec policy.
- **Tunnel, Tunneling**—Tunneling allows a remote VPN client encrypted access to a private network through the Internet. See VPN>IPSec>Transform Set>Tunnel Mode, Split Tunneling, VPN>IPSec>Tunnel Policy.
- **VPN**—Virtual Private Network. A network connection between two peers over the public network which is made private by strict authentication of users and the encryption of all data traffic. VPNs can be established between clients, such as PCs, and a headend, such as PIX Firewall. See IPSec, IKE, VPN>IKE Policies, Tunnel, Site-to-Site VPN, SA, ESP, PPP, L2TP, PPTP. See VPN Topics, VPN Wizard Topics, VPN Terms.

▲

IPSec RFCs

IPSec is documented in a series of Internet RFCs, all available at the following website:
http://www.ietf.org/html.charters/ipsec-charter.html

The overall IPSec implementation is guided by "Security Architecture for the Internet Protocol, RFC 2401.

PIX IPSec Standards

IPSec as implemented in PIX Firewall supports the following additional standards:

- **Authentication Header (AH)**—Authentication Header. A security protocol that provides authentication and optional replay-detection services. AH is embedded in the data to be protected (a full IP datagram, for example). AH can be used either by itself or with Encryption Service Payload (ESP). This is an older IPSec protocol that is less important in most networks than ESP. AH provides authentication services but does not provide encryption services. It is provided to ensure compatibility with IPSec peers that do not support ESP, which provides both authentication and encryption. See VPN, encryption. Refer to the RFC 2402.
- **Data Encryption Standard (DES)**—The DES was published in 1977 by the National Bureau of Standards and is a secret key encryption scheme based on the Lucifer algorithm from IBM. The contrast of DES is public-key. Cisco uses DES in classic crypto (40-bit and 56-bit key lengths), IPSec crypto (56-bit key), and on the firewall (56-bit key).
- **Diffie-Hellman**—A method of establishing a shared key over an insecure medium. Diffie-Hellman is a component of Oakley.
- **ESP**—Encapsulated Security Payload. This is the most important IPSec protocol, which provides authentication and encryption services for establishing a secure tunnel over an insecure network. See VPN, encryption. Refer to RFC 2406—IP Encapsulating Security Payload (ESP). and RFC 1827 for more information. The PIX Firewall implements the mandatory 56-bit DES-CBC with Explicit IV (RFC 2405); as the encryption algorithm, and MD5-HMAC (RFC 2403) or SHA-HMAC (RFC 2404) as the authentication. 3DES is also supported.
- **Hash**—A one way function that takes an input message of arbitrary length and produces a fixed length digest. Cisco uses both Secure Hash Algorithm (SHA) and Message Digest 5 (MD5) hashes within our implementation of the IPSec framework (see HMAC below).
- **HMAC**—A mechanism for message authentication using cryptographic hashes such as SHA and MD5. For an exhaustive discussion of HMAC, check out RFC 2104.
- **Internet Key Exchange** (IKE)—A hybrid protocol that implements Oakley and SKEME key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. While IKE can be used with other protocols, its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec security associations, and establishes IPSec keys. See RFC 2409.
- **Internet Security Association and Key Management Protocol (ISAKMP)**—A protocol framework that defines the mechanics of implementing a key exchange protocol and negotiation of a security policy. ISAKMP is defined in the Internet Security Association and Key Management Protocol (ISAKMP).
- **ISAKMP/Oakley**—The Internet Security Association and Key Management Protocol. A protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association. See IKE.
- **MD5**—Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and are designed to strengthen the security of the MD4 hashing algorithm. SHA is more secure than MD4 and MD5. Cisco uses hashes for authentication within the IPSec framework. Cisco uses hashes for authentication within the IPSec framework. Also used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.
- **Oakley**—A key exchange protocol that defines how to acquire authenticated keying material. The basic mechanism for Oakley is the Diffie-Hellman key exchange algorithm. You can find the standard in RFC 2412—The OAKLEY Key Determination Protocol.
- **Perfect Forward Secrecy (PFS)**—PFS ensures that a given IPSec SA's key was not derived from any other secret (like some other keys). In other words, if someone were to breaks a key, PFS ensures that the attacker would not be able to derive any other key. If PFS were not enabled, someone could hypothetically break the IKE SA secret key, copy all the IPSec protected data, and then use knowledge of the IKE SA secret to compromise the IPSec SAs setup by this IKE SA. With PFS, breaking IKE would not give an attacker immediate access to IPSec. The attacker would have to break each IPSec SA individually. Cisco's

IOS IPSec implementation uses PFS group 1 (D-H 768 bit) by default.

- **SA**—An instance of security policy and keying material applied to a data flow. Security associations (SAs) are established in pairs by IPSec peers during both phases of IPSec. SAs specify the encryption algorithms and other security parameters used to create a secure tunnel. Phase 1 SAs (IKE SAs) establish a secure tunnel for negotiating Phase 2 SAs. Phase 2 SAs (IPSec SAs) establish the secure tunnel used for sending user data.

  Both IKE and IPSec use SAs, although SAs are independent of one another. IPSec SAs are *unidirectional* and they are unique in each security protocol. A set of SAs are needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports ESP between peers, one ESP SA is required for each direction. SAs are uniquely identified by destination (IPSec endpoint) address, security protocol (AH or ESP), and security parameter index (SPI).

  IKE negotiates and establishes SAs on behalf of IPSec. A user can also establish IPSec SAs manually.

  An IKE SA is used by IKE only, and unlike the IPSec SA, it is *bi-directional*.

  See IPSec, IKE, Site-to-Site VPN, ESP.

- **SHA-1**— SHA is closely modeled after MD4 and produces a 160-bit digest. Because SHA produces a 160-bit digest, it is more resistant to brute-force attacks than 128-bit hashes (such as MD5), but it is slower. Secure Hash Algorithm 1 is a joint creation of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). This algorithm, like other hash algorithms, is used to generate a hash value, also known as a message digest, which acts like the cyclic redundancy check (CRC) used in lower-Layer Protocols to ensure that message contents are not changed during transmission. SHA-1 is generally considered more secure than MD5. It produces a 160-bit message digest for which no known attacks or partial attacks have yet been demonstrated. See encryption, VPN.
- **Secure Hash Algorithm (SHA)**—A one way hash put forth by NIST. SHA is closely modeled after MD4 and produces a 160-bit digest. Because SHA produces a 160-bit digest, it is more resistant to brute-force attacks than 128-bit hashes (such as MD5), but it is slower.
- **Transform, IPSec Transform Set**—A transform set specifies the IPSec protocol, encryption algorithm, and hash algorithm to use on traffic matching the IPSec policy. A transform describes a security protocol (AH or ESP) with its corresponding algorithms. The IPSec protocol used in almost all transform sets is the Encapsulated Security Protocol (ESP) with the DES cipher algorithm and HMAC-SHA for authentication.

For additional information about IPSec, see:

- TAC IPSec Support
- IPSec Technical Tips
- IP Security Troubleshooting - Understanding and Using debug Commands
- Topics>VPN>IPSec

Internet Key Exchange (IKE)

IKE is implemented per "The Internet Key Exchange" (RFC 2409).

- **ISAKMP**—The Internet Security Association and Key Management Protocol. A protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association. ISAKMP is implemented per "Internet Security Association and Key Management Protocol (ISAKMP)" (RFC 2408).
- **Oakley**—A key exchange protocol that defines how to derive authenticated keying material.
- **Skeme**—A key exchange protocol that defines how to derive authenticated keying material, with rapid key refreshment.

IKE Cryptographic Components

The component technologies implemented for use by IKE include:

- **DES**—Data Encryption Standard (DES) is used to encrypt packet data. IKE implements the 56-bit DES-CBC with Explicit IV standard. See "CBC.
- **Triple DES** (3DES)—A variant of DES, which iterates three times with three separate keys, effectively doubling the strength of DES.
- **CBC**—Cipher Block Chaining. A cryptographic tedchnique which increases the encryption strength of an algorithm. CBC requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet.
- **Diffie-Hellman**—A public-key cryptography protocol which allows two parties to establish a shared secret over an unsecure communications channel. Diffie-Hellman is used within IKE to establish session keys. 768-bit and 1024-bit Diffie-Hellman groups are supported.
- **MD5** (HMAC variant)—Message Digest 5 (MD5)is a hash algorithm used to authenticate packet data. HMAC is a variant which provides an additional level of hashing.
- **Oakley**—A key exchange protocol that defines how to derive authenticated keying material.
- **RSA signatures**—RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adelman. RSA signatures provide non-repudiation.
- **Skeme**—A key exchange protocol that defines how to derive authenticated keying material, with rapid key refreshment.
- **SHA** (HMAC variant)—Secure Hash Algorithm (SHA) is a hash algorithm used to authenticate packet data. HMAC is a variant which provides an additional level of hashing.

PIX IKE Standards

- **Xauth**, I**KE Extended Authentication**—PIX Xauth is implemented per the IETF draft-ietf-ipsec-isakmp-xauth-04.txt ("extended authentication" draft). This provides this capability of authenticating a user within IKE using TACACS+ or RADIUS.
- **Mode Config, IKE Mode Configuration**— PIX IKE Mode Configuration is implemented per the IETF draft-ietf-ipsec-isakmp-mode-cfg-04.txt. IKE Mode Configuration provides a method for a security gateway to download an IP address (and other network level configuration) to the VPN client as part of an IKE negotiation.

See IETF RFC Search.

Certificates, Certification Authorities (CA)

Digital Certificates

IKE features support the following standards for digital certificates and CAs:

- **X.509v3** certificates—ITU (International Telecommunications Union) standard X.509 is used with the IKE protocol when authentication requires public keys. Certificate support that allows the IPSec-protected network to scale by providing the equivalent of a digital ID card to each device. When two peers wish to communicate, they exchange digital certificates to prove their identities (thus removing the need to manually exchange public keys with each peer or to manually specify a shared key at each peer). These certificates are obtained from a certification authority (CA). X.509 is part of the X.500 standard by the ITU.
- **Public-Key Cryptography Standard #7** (PKCS #7)—Cryptographic Message Syntax Standard. A standard from RSA Data Security, Inc. (RSA) used to encrypt and sign certificate enrollment messages.
- **Public-Key Cryptography Standard #10** (PKCS #10)—Certification Request Syntax Standard. A standard syntax from RSA Data Security, Inc. for certificate requests.
- **RSA Keys**—RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adelman. RSA keys come in pairs: one public key and one private key.

RSA PKCS (Public-Key Cryptography Standard)

For additional information about PKCS, see RSA's, Introduction to the PKCS Standards, PKCS Standards Listing.

Certificate Authorities (CA)

Digital certificates (also known as public key certificates) are an efficient way to manage the security keys used for establishing the IKE SA.

CAs are responsible for managing certificate requests and issuing digital certificates. A digital certificate contains information that identifies a user or device, such as a name, serial number, company, department or IP address. A digital certificate also contains a copy of the owner's public key. A CA can be a trusted third-party, such as VeriSign, or a private (in-house) CA that you establish within your organization.

With digital certificates, each peer is enrolled with a CA and when two peers wish to communicate, they exchange certificates and digitally sign data to authenticate each other. When a new peer is added to the network, it simply enrolls with a CA, and none of the other peers need any additional configuration. Using manual configuration of pre-shared keys, each IPSec peer has to be configured for every peer with which it communicates.

PIX Firewall CAs Supported

PIX Firewall supports the following Certificate Authorities:

- Baltimore
- Entrust
- Microsoft
- VeriSign

For more Information about the CAs supported by PIX and how to enroll in them, see:

- Cisco.com>VSec>CA Authorities.
- Certificate Authorities - How to enroll from a PIX
- Topics>VPN>Certificates

▲

Cisco PIX Firewall VPN Terms

VPN TERMS

0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

3-DES

ACL

AH

AH Authentication

ASA

Asymmetric Encryption

Authentication

CA

Certificate

CRL

Crypto Map

DES

Diffie-Hellman

Digital Certificate

Encryption

ESP

ESP Authentication

ESP Encryption

GMT

GRE

Hash

Headend

Host

Host/Network

HTTPS

IKE

IKE Policies

ILS

Inside

IPSec

IPSec Phase 1

IPSec Phase 2

ISAKMP

L2TP

LDAP

Message Digest

MD5

PFS

Phase 1

Phase 2

PPP

PPTP

Pre-Shared-Key

Public Key

RA

RFC

RSA, RSA Data Security, Inc.

SA

SHA-1

Site-to-Site VPN

Split-Tunnelling

SSL

TACACS+

Transform Set

Triple DES

Tunnel

UTC

VPN

VPN>IKE Policies

VPN Tab

VPN Wizard

Xauth

Copyright © 2001-2004, Cisco Systems, Inc.

Transform Sets

Configuration>VPN>IPSec>Transform Sets

To view **Transform Sets**, click the **VPN** tab and then click **IPSec**>**Transform Sets** in the **Categories** area. The **Transform Sets** panel lets you define transform sets that can be applied to tunnel policies. A transform set specifies the IPSec protocol, encryption algorithm, and hash algorithm to use on traffic matching the IPSec policy. Your configuration edits are captured by PDM but are not sent to the firewall unit until you click **Apply**.

The following sections are included in this Help topic:

- Transform Sets
- Set Name
- Mode
- ESP Encryption
- ESP Authentication
- AH Authentication
- Adding a Transform Set
- Deleting a Transform Set

Transform Sets

This box lists the currently defined transform sets, which are available to apply to tunnel policies. By default, the following transform sets are already defined:

- ESP-DES-SHA
- ESP-DES-MD5
- ESP-3DES-SHA
- ESP-3DES-MD5
- ESP-AES-128-SHA
- ESP-AES-128-MD5
- ESP-AES-192-SHA
- ESP-AES-192-MD5
- ESP-AES-256-SHA
- ESP-AES-256-MD5

To define a new transform set, type an identifier in the **Set Name** box, select the **Mode**, **ESP Encryption**, **ESP Authentication**, or **AH Authentication** options you want, and click **Add**.

Set Name

Enter a name for a new transform set.

Mode

The **Tunnel** and **Transport** options let you choose the mode in which IPSec functions.

- **Tunnel Mode**—This is the normal way in which IPSec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the public Internet.

  Note: Tunnel mode encapsulates the entire IP header and datagram, prefixes an IPSec header, and then creates an outer IP header to tunnel the packet. Tunnel mode is used when the firewall is protecting traffic to and from hosts positioned behind the firewall.

- **Transport Mode**—This method of implementing IPSec is typically done with L2TP to allow authentication of remote Windows 2000 VPN clients.

  Note: Transport mode places the IPSec header after the original outer IP header and before the upper layer protocol. Transport mode can be performed only by the sender of the original datagram and therefore requires special software to be installed on the source and destination hosts.

ESP Encryption

Encapsulating Security Protocol (ESP) is the IPSec protocol used in the default transform sets provided with PIX Firewall. ESP is an IP protocol (type 50) that ensures message privacy through encryption, as well as data integrity, authentication, replay detection.

The encryption algorithms supported by the firewall include Data Encryption Standard (DES), which uses a 56-bit key, 3DES (Triple DES), which performs encryption three times using a 56-bit key, and Advanced Encryption Standard (AES). The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits. 3DES is more secure than DES but requires more processing for encryption and decryption. DES is generally considered secure enough for most business purposes.

ESP Authentication

A hash algorithm is used to create a message digest, which is used for ensuring message integrity. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has been a successful (but extremely difficult) attack demonstrated against MD5.

AH Authentication

Authentication Header is an IP protocol (type 51) that can ensure data integrity, authentication, and replay detection. AH does not provide encryption and has been largely superseded by ESP. AH may be required when the remote peer does not support ESP.

A hash algorithm is used to create a message digest, which is used for ensuring message integrity. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has been a successful (but extremely difficult) attack demonstrated against MD5.

Adding a Transform Set

Follow these steps to define a new transform set:

1. Type the name of the transform set in the **Set Name** box.
2. Click **Add**.
3. Select the mode and algorithms you want to use in the transform set.
4. Click **Apply**.

Deleting a Transform Set

Follow these steps to delete a transform set:

1. Select the transform set in the **Specify Transform Sets** table.
2. Click **Delete**.
3. Click **Apply**.

Copyright © 2001-2004, Cisco Systems, Inc.

Tunnel Policy

Configuration>VPN>IPSec>Tunnel Policy

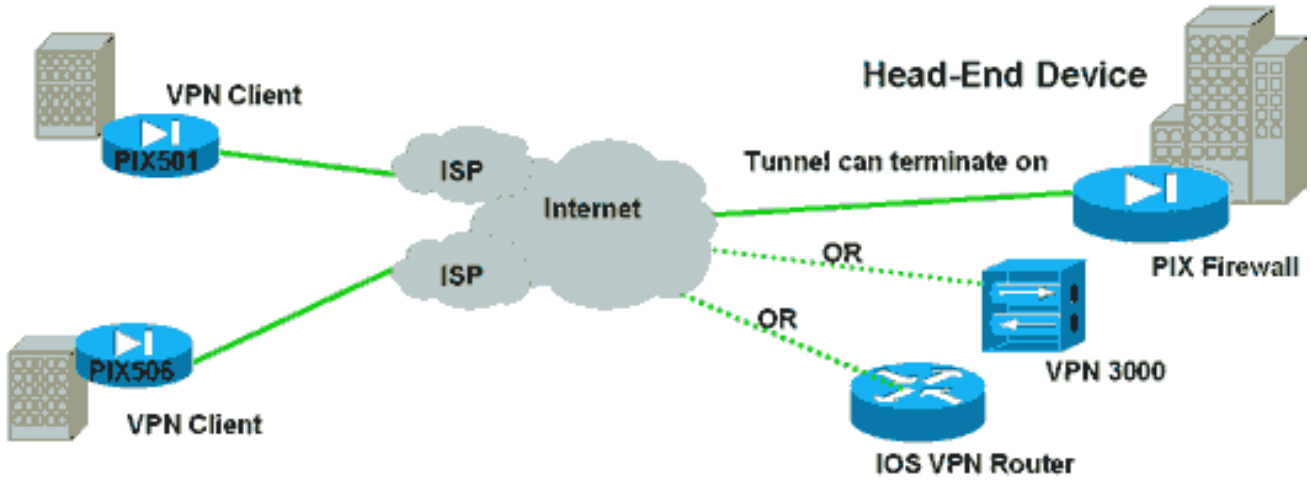
To view the **Tunnel Policy** panel, click the **VPN** tab and then select **IPSec>Tunnel Policy** from the Categories tree. The **Tunnel Policy** panel lets you define a tunnel policy that is used to negotiate an IPSec (Phase 2) security association (SA). Your configuration edits are captured by PDM but are not sent to the firewall unit until you click **Apply**.

The following sections are included in this Help topic:

- Introduction
- Specify Tunnel Policy
- Adding a Tunnel Policy
- Changing a Tunnel Policy
- Deleting a Tunnel Policy

Introduction to IPSec Tunnel Policy

Every tunnel policy must specify a transform set and identify the firewall interface to which it applies. The transform set identifies the encryption and hash algorithms used to perform IPSec encryption and decryption operations. Because not every IPSec peer supports the same algorithms, you may want to specify a number of policies and assign a priority to each. your firewall will then negotiate with the remote IPSec peer to agree on a transform set that is supported by both peers.



Tunnel policies can be *static* or *dynamic*. A static tunnel policy identifies one or more remote IPSec peers or

subnetworks to which your firewall will permit an IPSec connection. A static policy can be used whether your firewall initiates the connection or receives a connection request from a remote host. A static policy requires you to enter the information necessary to identify permitted hosts or networks.

A dynamic tunnel policy is used when you cannot or do not want to provide information about remote hosts that are permitted to initiate a connection with the firewall. If you are only using your firewall as a VPN client in relation to a remote VPN headend, you will not need to configure any dynamic tunnel policies. Dynamic tunnel policies are most useful for allowing remote access clients to initiate a connection to your network through a PIX Firewall acting as the VPN headend. A dynamic tunnel policy is useful when the remote access clients have dynamically assigned IP addresses or when you do not want to configure separate policies for a large number of remote access clients.

Specify Tunnel Policy

Interface—The interface on the firewall to which the tunnel policy applies.

Type & Priority—Identifies the type (static or dynamic) and the priority of the tunnel policy.

You can define multiple tunnel policies and assign a priority to each. When your firewall negotiates an IPSec SA with the remote peer, it will propose to use the parameters in the highest priority tunnel policy first. If the remote peer cannot match the parameters proposed in the first tunnel policy, your firewall will use each lower priority tunnel policy until it finds one that matches a policy acceptable to the remote peer.

A tunnel policy is *static* when it applies to one or more remote peers that can be accurately identified by IP address or DNS host name. A tunnel policy is *dynamic* when it applies to an unknown remote peer that seeks to initiate an IPSec connection with the firewall. A static policy is more secure than a dynamic policy. However, a dynamic policy is necessary when a remote IPSec peer has a dynamically assigned IP address or when the firewall is configured to allow connections from unknown remote hosts.

Transform Set—Identifies the transform set that is included in this policy. A transform set specifies the IP Sec protocol, encryption algorithm, and hash algorithm to use on traffic matching the IPSec policy. These options are described as follows:

- The IPSec protocol used in the default transform sets is the Encapsulating Security Protocol (ESP), which provides both encryption and authentication. The alternative protocol is Authentication Header (AH), which is an older protocol providing only authentication. AH has been largely superseded by ESP but may be used when the remote peer does not support ESP.
- The encryption algorithms supported by the firewall include Data Encryption Standard (DES), which uses a 56-bit key, 3DES (Triple DES), which performs encryption three times using a 56-bit key, and Advanced Encryption Standard (AES). The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits. 3DES is more secure than DES but requires more processing for encryption and decryption. DES is generally considered secure enough for most business purposes.
- A hash algorithm is used to create a message digest, which is used for ensuring message integrity. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has been a successful (but extremely difficult) attack demonstrated against MD5.

Peer—Identifies the host name or IP address of the remote IPSec peer for static tunnel policies.

SA Lifetime—Identifies the lifetime of the IPSec security association in terms of the length of time it can be used or the amount of traffic that can flow through the tunnel created with the SA before it expires.

PFS—Identifies if perfect forward secrecy (PFS) is included in a specific tunnel policy. PFS enhances security by using different security keys for the Phase 1 and Phase 2 SAs. Without PFS, the same security key is used to establish SAs in both phases.

Note: The vulnerability of a security key to attack is a factor of time and the amount of traffic transmitted. A Phase 1 SA is only used to negotiate the security parameters for the Phase 2 SA, while the Phase 2 SA is used for the actual transmission of user data. Because the Phase 2 SA is used to transmit much more data than the Phase 1 SA, the security key used to establish the Phase 2 SA should theoretically be assigned a shorter lifetime than the key used for establishing a Phase 1 SA. PFS lets you assign different lifetimes to the security keys used for establishing Phase 1 and Phase 2 SAs.

Adding a Tunnel Policy

Follow these steps to define a new IPSec (Phase 1) tunnel policy:

1. Click **Add**.
2. In the **Tunnel Policy** dialog box that appears, select the security parameters you wish to use for this policy.
3. Click **OK**.
4. Click **Apply**.

Changing a Tunnel Policy

Follow these steps to change an existing IPSec (Phase 1) tunnel policy:

1. Select a policy in the **Specify Tunnel Policy** table and click **Edit**.
2. In the **Tunnel Policy** dialog box that appears, change any security parameters you wish to modify.
3. Click **OK**.
4. Click **Apply**.

Deleting a Tunnel Policy

Follow these steps to delete an existing IPSec (Phase 1) tunnel policy:

1. Select a policy in the **Specify Tunnel Policy** table and click **Delete**.
2. Confirm the operation.
3. Click **Apply.**

Copyright © 2001-2004, Cisco Systems, Inc.

Policies

Configuration>VPN>IKE>Policies

To view the **Configure IKE Policies** panel, click the **VPN** tab and then select **Configure IKE policies** from the Categories tree. The **Configure IKE Policies** panel describes how to configure Internet Key Exchange (IKE) policies used for establishing Phase 1 security associations (SAs). Your configuration edits are captured by PDM but are not sent to the firewall unit until you click **Apply**.

IPSec operates in two phases:

- Phase 1 negotiates the security associations (SAs) used to establish a single, reusable secure tunnel between two IPSec peers.
- Phase 2 uses the Phase 1 tunnel to negotiate SAs and establish secure tunnels for transmitting user data.

To establish a secure tunnel, either in Phase 1 or Phase 2, both peers must agree on the encryption algorithm and other security parameters to use. Once negotiation is completed, each peer establishes an SA that defines the security parameters to use with the other peer. An IKE policy defines the security parameters that you want your firewall to use in negotiation with a remote peer for creating a Phase 1 SA.

The following sections are included in this Help topic:

- IKE Policy
- General Information
- Adding an IKE Policy
- Changing an IKE Policy
- Deleting an IKE Policy

IKE Policy

IKE policy defines the security parameters used to create the IKE (Phase 1) SA. These policies are listed in tabular form on the **Configure IKE Policies** panel, which lists the following properties for each policy:

- **Priority**—When you define a policy, you assign a numeric priority, so if the remote IPSec peer does not support the parameters selected in your first priority policy, the firewall will try to use the parameters defined in the policy with the next highest priority.
- **Encryption**—Specifies the symmetric encryption algorithm used to establish the Phase 1 SA for protecting Phase 2 negotiations. The encryption algorithms supported by the firewall include Data Encryption Standard (DES), which uses a 56-bit key, 3DES (Triple DES), which performs encryption three times using a 56-bit

key, and Advanced Encryption Standard (AES). The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits. 3DES is more secure than DES but requires more processing for encryption and decryption. DES is generally considered secure enough for most business purposes.

- **Hash**—Specifies the hash algorithm used for authentication and ensuring data integrity. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has been a demonstrated successful (but extremely difficult) attack against MD5. However, the Keyed-Hash Message Authentication Code (HMAC) version used by PIX Firewall prevents this attack.
- **D-H Group**—Specifies the Diffie-Hellman group identifier, which is used by the two IPSec peers to derive a shared secret without transmitting it to each other. The default, Group 1 (768-bit Diffie-Hellman) requires less CPU time to execute but is less secure than Group 2 (1024-bit Diffie-Hellman). Diffe-Hellman Group 5 uses a 1536-bit prime number, is the most secure, and is recommended for use with AES.
- **Authentication**—Specifies the method of authentication used to establish the identify of each IPSec peer.
- When you select the **rsa-sig** (RSA signatures) option, you use digital certificates for managing the public keys required for completing IKE Phase 1 negotiation. Digital certificates scale well for large or growing networks with many IPSec peers.

General Information

This tab lists each firewall interface and identifies if IKE is enabled on the interface.

- **Enable**—To enable the current IKE policy on a firewall interface, select the interface from the list in the **General Information** area and click **Enable**.
  - Select the interface under **General Information**.
  - Click **Enable** to enable IKE on the interface.
- **Disable**—To disable the current IKE policy on a firewall interface, select the interface from the list under **General Information** and click **Disable**.
- **Set Keepalive and Retry Values**—Select this check box to modify keepalive and retry values.
- **Keepalive**—Specify an interval between 10 seconds and 3600 seconds (1 hour). You can specify the Keepalive interval with or without specifying the Retry interval.
- **Retry**—Specify an interval between two and ten seconds. The default is two seconds. The Retry interval is the interval between retries after a Keepalive response has not been received. To specify a Retry interval, you must also specify the Keepalive interval.
- **Enable Event Tracing**—Select to enable a simple event tracing buffer for troubleshooting. It is helpful for detailed troubleshooting when a syslog server is unavailable such as in Cisco PIX Firewall 501 Easy VPN Remote deployments. The range of number of events you can trace is 0 (disabled) to 50,000. This is disabled by default.
- **Enable NAT Traversal**—Select this check box to enable NAT traversal, which lets Encapsulated Security Payload (ESP) packets pass through one or more NAT devices. NAT traversal is described by Version 2 and Version 3 of the draft IETF standard, UDP Encapsulation of IPsec Packets," which is available at the following URL: http://www.ietf.org/html.charters/ipsec-charter.html
- **NAT Keepalive**—Specify an interval between 10 seconds and 3600 seconds (1 hour).
- **Identity**—From this drop-down list, select whether the IP address, the DNS host name, or key-id is used to identify the firewall. The **key-id** option may be used for a DHCP enabled firewall at the remote site to interoperate with a headend VPN device that uses the information in the key-id box to look up the pre-shared key.
- **Key Id String**—This box is enabled when you select **key-id** from the **Identity** list. The key-id string will be passed to the headend VPN device using aggressive mode negotiation.

Note: Digital certificates also establish non-repudiation for IKE negotiation, which means that you can prove to a third party that IKE negotiation was completed with a specific peer.

When you select the **pre-share** option, you use manually configured pre-shared keys for completing IKE (Phase 1) negotiation. Pre-shared keys do not scale well with a growing network but are easier to set up in a smaller network with a limited and stable number of IPSec peers.

Lifetime(secs)—Specifies the SA lifetime. The default is 86,400 seconds or 24 hours. As a general rule, a shorter lifetime (up to a point) provides more secure IKE negotiations. However, with longer lifetimes, future IPSec security associations can be set up more quickly.

Adding an IKE Policy

Follow these steps to define a new IKE policy:

1. Click **Add**.
2. In the **Add IKE Rule** dialog box that appears, select the security parameters you wish to use for this policy.
3. Click **OK**.
4. Click **Apply**.

Changing an IKE Policy

Follow these steps to change an existing IKE policy:

1. Select an existing IKE policy from the table.
2. Click **Edit**.
3. In the **Edit IKE Rule** dialog box that appears, change any security parameters you wish to modify for this policy.
4. Click **OK**.
5. Click **Apply**.

Deleting an IKE Policy

Follow these steps to delete an existing IKE policy:

1. Select an existing IKE policy from the table.
2. Click **Delete**.
3. Click **OK** to confirm the operation.
4. Click **Apply**.

Copyright © 2001-2004, Cisco Systems, Inc.

Telnet Console Sessions

Monitoring>Telnet Console Sessions

The **Telnet Console Sessions** panel lets you monitor connections made to the firewall using Telnet. A snapshot of current Telnet sessions to the firewall is displayed. The display is not automatically updated as new Telnet sessions are created. To view new Telnet sessions, you must click **Refresh**.

The following sections are included in this Help topic:

- Field Descriptions
- Showing Sessions by IP Address

Field Descriptions

The **Telnet Console Sessions** panel displays the following fields:

- **Current Telnet Console Sessions Connected**—Displays a unique session ID and the IP address of each Telnet client connected to the firewall in the form: **ID: IP Address**. If PDM knows the client host name associated with the IP address, the host name will also appear in the display.
- **Show Sessions for this IP Address**—Allows you to enter a client IP address of the connected Telnet session(s) you want to show.
- **Refresh**—Refreshes the panel with current information from the firewall. If an IP address is specified, only the information about the Telnet session using that IP address is refreshed. If no IP address is specified, information is refreshed for all Telnet sessions.

Showing Telnet Sessions by IP Address

Follow these steps to display Telnet Console Sessions for a specific IP address:

1. Enter a client IP address in **Show Sessions for this IP address,** if you want to refresh only the information about the Telnet session using that IP address.
2. Click **Refresh**.

Showing All Telnet Sessions

Follow these steps to display all Telnet Console Sessions:

1. Do not enter a client IP address in **Show Sessions for this IP address,** if you want to refresh the information about all Telnet sessions.
2. Click **Refresh**.

Copyright © 2001-2004, Cisco Systems, Inc.

Unsupported Commands

The Cisco PIX Device Manager (PDM) does not support the complete command set of the command line interface (CLI). PDM cannot function normally when certain unsupported commands are in the running configuration. This has important implications when using PDM.

The following sections are included in this Help topic:

Introduction

- Effects of Unsupported Commands
- Monitor Only Mode
- How to Exit Monitor Only Mode

PDM Support for PIX Firewall CLI Commands

	Supported	Parsed	Visible	Editable	Ignored	Restrictions/ Combination	Monitor Only Mode
1		✓	✓				✓
2		✓	✓			✓	✓
3					✓		
4	✓	✓	✓	CLI Edit Only			
5	✓✓	✓	Invisible	CLI Execute Only		✓	
6	✓✓✓	✓	✓	✓			

1. Unsupported, Parsed Commands Causing Monitor Only Mode
2. Unsupported Command *Combinations* Causing Monitor Only Mode
3. Unsupported, Unparsed Commands, Ignored
4. Supported Partially Commands, NO PDM Changes
5. Supported Invisible and CLI-Only Commands
6. Fully Supported Commands

Reference

- PIX Firewall Command Reference and Access Modes

Note: For more information about the CLI commands used by each PDM screen, see **CLI Commands Used by PDM Screens**.

Effects of Unsupported Commands

- As PDM opens, it loads the running configuration from the firewall unit. If it encounters no unsupported commands, access to all PDM functions is granted for normal operation mode.
- If PDM loads an existing running configuration and finds certain unsupported commands, it will enter the Monitor Only mode.
- Multiple PDM and CLI sessions may be in operation at the same time as your PDM session. During normal operation, if unsupported commands are entered via other CLI console sessions or your CLI tool, PDM will enter Monitor Only mode when you **Refresh**.

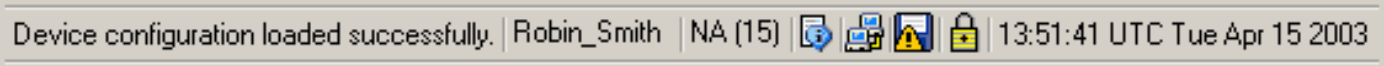
Monitor Only Mode

Monitor Only mode only allows access to the following functions:

- The **Monitoring** tab
- The CLI tool (**Tools>CLI**) will let you use the CLI commands allowed by the Privilege level set in your user account in **System Properties>Administration>Authentication**.
- File>**Reset Firewall to the Factory Default Configuration**

You may have entered Monitor Only mode for the following reasons:

- **Configuration**—An unsupported command is in the running configuration of the PIX Firewall from which you loaded PDM.
- **Privileges**—Your user account privilege level, indicated in the status bar at the bottom of the main PDM window, was set up as less than or equal to 3 by your system administrator to only allow Monitor Only mode. For more information, see **System Properties>Administration>User Accounts** and **System Properties>Administration>Authentication/Authorization**.



How to Exit Monitor Only Mode

If you entered Monitor Only Mode due to a configuration issue, follow these steps to regain access to the all the functions of PDM in normal operation mode which are allowed by your privilege level:

- Click **Tools>CLI** to repair or remove the unsupported command statement(s) or, Click **File>Reset Firewall to the Factory Default Configuration** to replace the current running configuration.
- **Refresh** will reload the repaired or replaced configuration.

If you entered Monitor Only mode due to your user account privileges and need additional access, contact your system administrator.

Unsupported Parsed Commands Causing Monitor Only Mode

These commands can be parsed, but PDM does not support them in a configuration. If the commands are present in your configuration, PDM will enter Monitor Only mode.

COMMAND	DESCRIPTION
`alias`	Administer overlapping addresses with dual NAT. Also permits inside interface access to a DNS server on a perimeter interface.
`outbound id except`	Create an access list to control **outbound** connections.
`access-list acl1 deny igmp any any` `access-group acl1`	An **access-list** cannot be applied to an interface and an IGMP access group. The following is not allowed: access-list acl1 deny igmp any any access-group acl1 in interface outside multicast interface outside igmp access-group acl1

Unsupported Command Combinations Causing Monitor Only Mode

:

In addition, the following command *combinations* will cause PDM to enter the Monitor Only mode when detected in the configuration:

- **aaa** command with the **match** option appearing in the configuration with other **aaa** commands that contain the **include** or **exclude** options. For example, the following commands would not be parsed by PDM:

```
access-list 101 permit tcp any any
aaa authentication include http inside 1.1.1.1 255.255.255.255 0.0.0.0 0.0.0.0
portal
aaa accounting match 101 inside portal
```

You can fix this by changing **aaa** commands exclusively to either the **match acl style** or to the **include/exclude** style.

- **Access-list**—Certain combinations of access control lists are unsupported.
    - Combining the **access-list** and **access-group** command statements with **conduit** and/or **outbound** command statements. For example, the following commands appearing anywhere in the configuration (not necessarily together) would not be parsed by PDM:

```
access-list 101 permit ip 172.21.3.0 255.255.0.0 172.22.2.0 255.255.0.0
access-group 101 in interface outside
conduit permit icmp any any
```

    - Using an ACL (access control list) for multiple interfaces. For example, the **access-list eng permit ip any** *server1* **255.255.255.255**

```
access-group eng in interface perim
access-group eng in interface outside
```

    - Using an ACL name for multiple purposes such as in an **access-group** command statement and in an **aaa** command statement. For example, the following commands would not be parsed by PDM:

```
access-list acl_out permit tcp 10.16.1.0 255.255.255.0 209.165.201.0
255.255.255.224
access-group acl_out in interface outside
aaa authentication match acl_out outside AuthIn
```

      In this example, the **access-list** command statement is applied to the outside interface by the **access-group** command. The same ACL name cannot then be used by the **aaa** command statement. You can fix this example by creating an **access-list** command statement without an accompanying **access-group** command statement and then applying that to the **aaa** command statement. For example:

```
access-list acl_out2 permit tcp 10.16.1.0 255.255.255.0 209.165.201.0
255.255.255.224
aaa authentication match acl_out2 outside AuthIn
```

- Using an ACL for multiple purposes (such as authentication, authorization, or accounting). For example, the following command statements cannot be parsed by PDM:

```
access-list acl_out2 permit tcp 10.16.1.0 255.255.255.0 209.165.201.0
255.255.255.224
aaa authentication match acl_out2 outside AuthIn
aaa authorization match acl_out2 outside AuthIn
```

In this example, the **access-list** command statement is applied to the outside interface by the **aaa authentication** command. Using the **acl_out2** ACL name for both authentication and authorization cannot be parsed by PDM. You can fix this by creating another **access-list** command statement the same as the first and applying that in the **aaa authorization** command. For example:

```
access-list acl_out2 permit tcp 10.16.1.0 255.255.255.0 209.165.201.0
255.255.255.224
access-list acl_out3 permit tcp 10.16.1.0 255.255.255.0 209.165.201.0
255.255.255.224
aaa authentication match acl_out2 outside AuthIn
aaa authorization match acl_out3 outside AuthIn
```

- **Outbound**
  - Any **outbound** command statement that contains the **except** option. In most cases, you should be able to rewrite the **outbound** command statements using the **permit** or **deny** options to eliminate the use of the **except** option. Once the **except** option is replaced with **permit** or **deny**, PDM functions normally.
  - Applying an **outbound** command statement group to multiple interfaces. For example, the following would not be parsed by PDM:

```
outbound 13 deny 0.0.0.0 0.0.0.0 0 0
outbound 13 permit 0.0.0.0 0.0.0.0 389 tcp
outbound 13 permit 0.0.0.0 0.0.0.0 30303 tcp
outbound 13 permit 0.0.0.0 0.0.0.0 53 udp
apply (inside) 13 outgoing_src
apply (perim) 13 outgoing_src
```

- **User Lacks Privilege**—User lacks privilege to run the following basic commands:
  - **write**
  - **show pdm**
  - **show version**
  - **show curpriv**

- **ACL and IGMP Access Group**—An **access-list** cannot be applied to an **interface** command and an **igmp access group** command. The following is not allowed:
  - `access-list acl1 deny igmp any any`
  - `access-group acl1 in interface outside`
  - `multicast interface outside`

- igmp access-group acl1

Unsupported Unparsed Commands, Ignored

The following commands are unsupported, but will not cause PDM to enter Monitor Only mode. They are ignored when encountered by PDM, and are displayed in the list of unparsed commands invoked by **Options>View Unparsed Commands...** or an informational message button which appears near the top of PDM. Note: PDM does not change or remove these commands from your configuration.

COMMAND	DESCRIPTION
`isakmp client configuration address-pool local <pool> <interface>`	Internet Security Association and Key Management Protocol (ISAKMP) limitation.
`acl not applied to any interface`	Must be applied to an interface.
`outbound list not applied to any interface`	Must be applied to an interface.
`established`	Permit return connections on ports other than those used for the originating connection based on an **established** connection.
`prefix-list not bound to an OSPF area`	Must be linked to an OSPF area using 'area xxx filter-list prefix' command.
`Mac-list not bound to an aaa mac-exempt rule will be ignored`	Must be linked to an aaa rule using 'aaa mac-exempt match <mcl-id>' command.

Note: The following commands are not supported or changed by PDM:

- arp
- sysopt ipsec pl-compatible
- sysopt nodnsalias inbound
- sysopt nodnsalias outbound

Supported Partially Commands, No PDM Changes

The following table lists commands which PDM supports in the configuration when added by the CLI or other means, but which cannot be edited in PDM. PDM parses these commands and handles them transparently.

COMMAND	DESCRIPTION
`arp`	Change or view the ARP cache, and set the timeout value.
`floodguard`	Enable or disable Flood Defender to protect against flood attacks.
`mtu`	Specify the MTU (maximum transmission unit) for an interface.
`name-server`	Name server command feature.
`object-group (protocol, icmp-type)`	PIX **ICMP-type** and **protocol** object types are not supported in PDM object grouping.
`object-group (network) nested not supported`	PDM may not be used to create nested or hierarchical **network-type** object-groups. Nested means that the group that has other groups has its members. If a nested group is configured using the CLI or otherwise, and it is used in an **access-list** command or **conduit** command, PDM will parse it, and show it in the rule table. However, it cannot be edited within PDM. Nested **service groups** are supported.
`pager`	Enable or disable screen paging.
`sysopt ipsec pl-compatible`	Limitation on IPSec support.
`sysopt nodnsalias inbound`	Disable inbound embedded DNS A record Fixups according to aliases that apply to the A record address.
`sysopt nodnsalias outbound`	Disable outbound DNS A record replies.

`sysopt route dnat`	Specify that when an incoming packet does a route lookup, the incoming interface is used to determine which interface the packet should go to, and which is the next hop.
`sysopt security fragguard`	FragGuard feature.
`sysopt uauth allow-http-cache`	HTTP cache feature.
`terminal`	Change console terminal settings.
`virtual`	Access PIX Firewall virtual server.
`ca`	PDM does not support more than one FQDN in the VPN>IKE>Certificate>Configuration.

Supported Invisible Commands, CLI-Only Commands

- The **clear uauth**, **kill**, **ping**, **reload**, **show**, **who**, and **write** commands that also do not appear in the configuration are incorporated directly into the PDM user interface.
- **CLI only commands**—PIX Firewall commands that you enter at the command line, but do not appear in the configuration are not supported in PDM. These are the **configure**, **copy**, **debug**, **disable**, **enable**, **exit**, **flashfs**, **help**, **perfmon**, **quit**, **session**, and **setup** commands.

Fully Supported Commands

The following table lists commands fully supported by PDM. PDM parses these commands, operates normally, and allows editing of these commands in the configuration.

Exceptions are noted in the table and occur when PDM cannot parse certain combinations of command statements. For all exceptions, refer to the *Cisco PIX Device Manager Installation Guide* for your respective version, "Understanding PDM Access, Handling Configuration Limitations" for information on how to correct each problem. Commands that PDM cannot parse stay in the configuration, their values cannot be changed with PDM, and they appear in the list of unparseable commands.

COMMAND	DESCRIPTION
`aaa` command, `include` option	Enable, disable, or view TACACS+ or RADIUS user authentication, authorization, and accounting (AAA) for the server previously designated with the **aaa-server** command.
`aaa` command, `match acl_name` option	Apply authentication, authorization, or accounting to an access list. Exception: PDM cannot parse this command if an **access-group** command statement shares the same *acl_name*.
`aaa-server`	Specify a AAA server.
`access-list` and `access-group`	Create an access list and bind it to an interface. Exceptions: PDM cannot parse these commands if: • Combining the **access-list** command with the **conduit** and/or **outbound** command. • Configuring **access-list** command statements without an associated **access-group** command, unless the **access-list** command statement is used in conjunction with an **aaa** command statement. • Configuring multiple **access-group** command statements with the same *acl_name* for different interfaces. • Using an *acl_name* for multiple purposes, such as in an **access-group** command and in a **aaa** command, or in a **aaa authentication match** command statement and in a **aaa authorization match** command statement.
`access-list` compiled	Turbo Access Rules. Enable turbo ACL globally.
`apply`	Apply **outbound** command statements to an interface.
`ca`	Certification authority (CA) for VPN support of digital certificates.
`clock`	PIX real-time clock commands.

`auth-prompt`	Change the AAA challenge text.
`conduit`	PIX Conduit support. Add, delete, or **show conduits** comands through the firewall for incoming connections. Exception: PDM cannot parse this command if you combine it with the **access-list** command.
`crypto map`	Crypto Map setup for VPN configuration.
`crypto dynamic-map`	Crypto Map setup for VPN configuration.
`crypto ipsec`	Crypto Map setup for IPSec VPN configuration.
`dhcpd`	Implement the DHCP server feature.
`domain-name`	Specify the firewall domain name for the DNS protocol.
`enable password`	Set the privileged mode password.
`failover`	Change or view access to the optional failover feature.
`failover lan and` `show failover lan detail`	failover lan configures LAN-based failover. Show failover lan detail provides debugging information.
`filter`	Enable or disable outbound URL filtering or HTML object filtering.
`fixup protocol`	Change, enable, disable, or list a PIX Firewall application protocol feature.
`fragment`	Memory management of packet fragments.
`global`	Create or delete entries from a pool of global addresses.
`hostname`	Change the host name in the firewall command line (CLI) prompt.
`http`	Configure PDM access using HTTP.

`icmp`	ICMP—Internet Control Message Protocol.
`igmp`	IGMP—Internet Group Management Protocol.
`interface`	Identify network interface speed and duplex.
`ip address`	Identify ip addresses for network interfaces.
`ip audit`	Configure IDS signature use.
`ip local pool`	IP pool management,
`ip verify reverse-path`	Implement Unicast RPF IP spoofing protection.
`isakmp identity` [address | hostname]	Internet Security Association and Key Management Protocol. VPN IPSec related command.
`logging`	Enable or disable syslog and SNMP logging.
`mroute`	Multicast routing (MCR) protocol configuration.
`multicast`	Multicast routing protocol (MCR) configuration.
`name`	Associate a name with an IP address.
`nameif`	Specify name and security level for an interface.
`nat`	Network Address Translation (NAT). Associate a network with a pool of global IP addresses.
`nat [(if_name)] 0 access-list acl_name`	Associate Network Address Translation (NAT) to an access list.
`ntp`	Network Time Protocol (NTP) support.
`object-group (network, service)`	Firewall object group support.

`outbound`	Create an access list to control outbound connections. Exceptions: • Using the **outbound** command with the **except** option. • Combining the **access-list** command with the **conduit** and/or **outbound** command.
`passwd`	Set password for Telnet access to the firewall console.

`pdm`
`pdm group`
`pdm history`
`pdm location`
`pdm logging`
	PDM commands.

`privilege`	Set access privileges.
`remote-management`	Auto Update feature.
`rip`	Change RIP settings.
`route`	Enter a static or default route for the specified interface.
`service resetinbound`	Reset inbound connections.
`snmp-server`	Provide SNMP event information.
`ssh`	Specify a host for Firewall console access via Secure Shell (SSH).
`static` [used for inbound PAT]	Funnel inbound connections through a single IP address.
`sysopt`	Change PIX Firewall system options. Exception: The **route dnat** and **nodnsalias** options cannot be parsed.
`telnet`	Specify host for Firewall console access via Telnet.
`tftp-server`	Specify the IP address of the TFTP configuration server.

`timeout`	Set the maximum idle time duration.
`url-block`	URL filtering feature used with Websense or N2H2.
`url-cache`	Cache responses to URL filtering requests to the Websense or N2H2 server.
`url-server`	Designate a server running Websense or N2H2 for use with the **filter url** command.
`user-name`	User accounts feature.
`vpdn`	VPN related command.
`vpnclient`	VPN related command.
`vpngroup`	VPN related command.

PIX Firewall Command Reference and Access Modes

Before configuring your firewall from the PDM CLI tool, we recommend that you review the *Cisco PIX Firewall Command Reference*, and the *Cisco PIX Device Manager Installation Guide* for your respective version.

The complete *Cisco PIX Firewall Command Reference* for your respective version is available on Cisco.com: http://www.cisco.com/warp/public/110/pix_command_ref.shtml

A summary of the firewall administrative access modes is in *PDM Glossary>(PIX) Administrative Modes.*

For more information about the CLI commands used by each PDM screen, see CLI Commands Used by PDM Screens.

For more information about currently unsupported command combinations, see the *Cisco PIX Device Manager Installation Guide* for your respective version.

Copyright © 2001-2004, Cisco Systems, Inc.

Building Graph Windows

Monitoring>Building Graph Windows

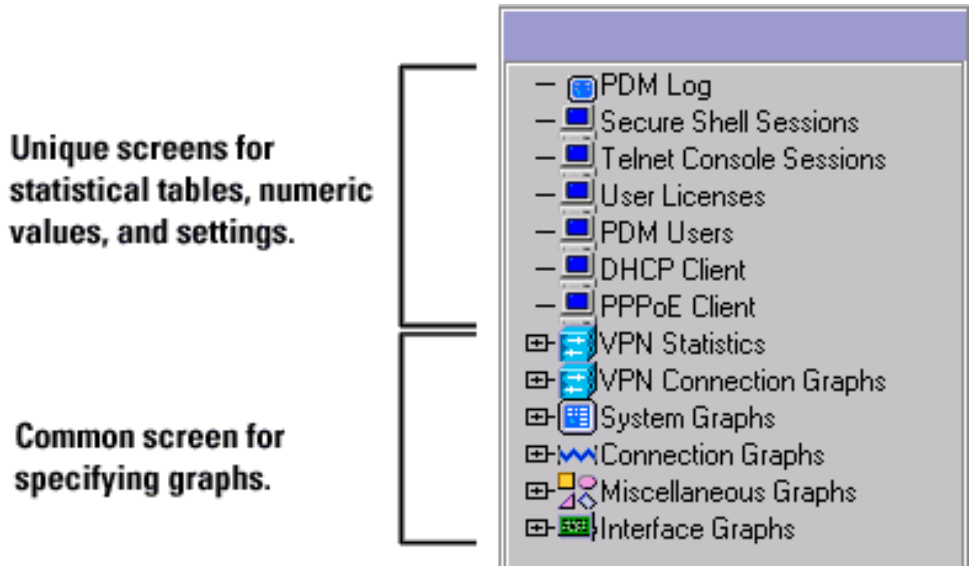
This main help topic for the Graph function of the **Monitoring** tab provides information about building **Graph Windows**, which is common to all the Graph Categories and Graph Types.

The following sections are included in this Help topic:

- Overview of PDM Graphs
- Field Descriptions
- Building a New Graph Window
- Displaying a Graph Window

Overview of PDM Graphs

The **Monitoring** tab features two types of graphing and monitoring functions.



The first type has a unique screen for each menu selection that shows the table of statistics, numeric values or settings for that menu selection.

The second type uses the same screen which allows the building of **Graph Windows** that combine up to four graphs in a single window, following these basic steps:

- Select a Graph Category from the tree list to the left
- Select a Graph Type under the Category
- Select an individual Graph from the **Available Graphs** list
- **Add** it to the **Selected Graph(s)** list
- Name the **Graph Window**
- **Graph It!**

Graph It! opens new **Graph Window** and displays the graphs which were added to the **Selected Graphs** list. The graphs displayed in the New Graph Window can be bookmarked in your browser for later recall, printed, and their data may be exported for use by other applications.

Field Descriptions

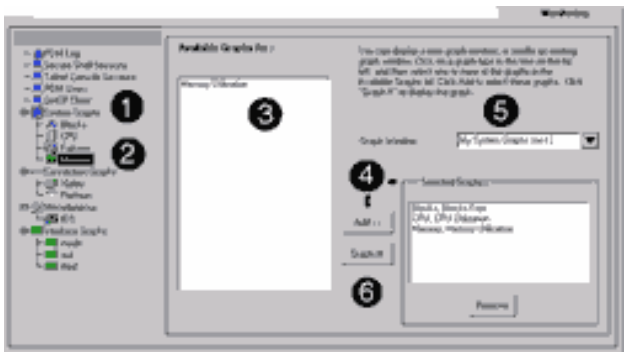
The main panel of the common graph generation menu items displays the following fields for the Graphs function:

- **Graph Category>Type** tree—Displays in a tree list of available Graph Categories and Types on the left.
- **Available Graphs for**—Displays the list of individual graphs available for each Interface.
- **Graph Window**—Lets you give the Graph Window a name. If unspecified, the graph window name will be "Unnamed (n)" where n increments as each unnamed graph window is created.
- **Selected Graph(s)**—Displays up to four graphs you have selected from the **Available Graphs for** list and added to the **Graph Window**.

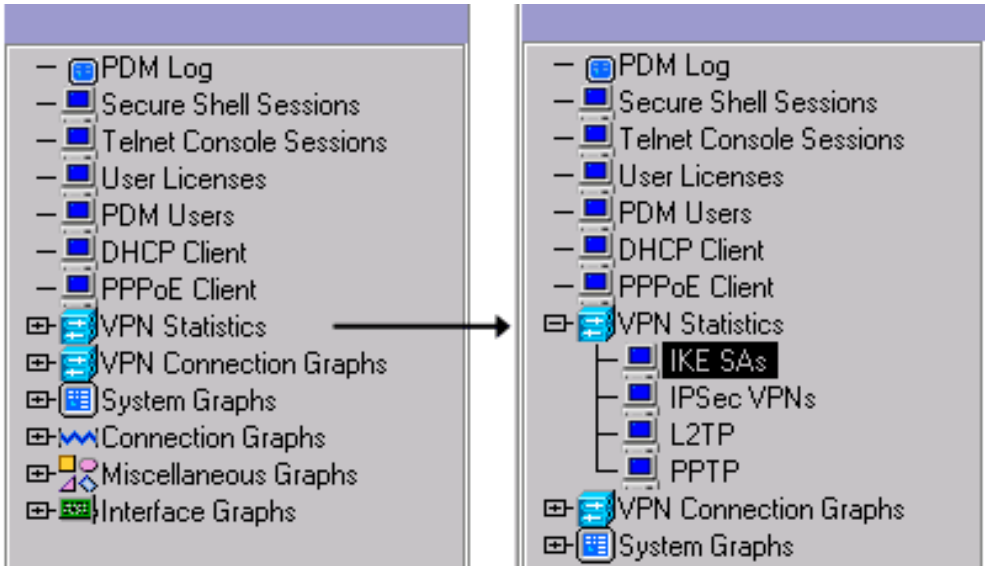
- **Add**—Adds to the **Selected Graph(s)** list all graphs you have selected from the **Available Graphs for** list.
- **Remove**—Removes graphs you have currently selected in **Selected Graph(s)** list.
- **Graph It!**—Opens a Graph Window which displays the graphs in the **Selected Graph(s)** list.

Building a New Graph Window

Follow these steps to build a new **Graph Window**:



1. Select one of the following **Graph Categories** from the graph selection tree on the left of the **Monitoring** tab:



2. Select one or more of the **Graph Types** under your selected graph **Category**.
3. A list of **Available Graphs** for that Category>Type will be displayed in a list at the right of the graph selection tree.
4. Click **Add** to add your selections to the **Selected Graph(s)** list.
5. You may also select additional Graph Category>Types from the graph tree and add them to the **Selected Graph(s)** list.
6. Optionally, you can name the Graph Window in **Graph Window** box or select previous Graph Windows by clicking the drop down list.

Displaying a Graph Window

Click

to open a new **Graph Window** and display the graph(s) which can be bookmarked, printed and exported.

Copyright © 2001-2004, Cisco Systems, Inc.

Interface Graphs

Monitoring>Interface Graphs

The **Interface Graphs** panel lets you monitor per-interface statistics, such as packet counts and bit rates, for each enabled interface on the firewall. These graphs may be bookmarked for quick opening by your browser, printed, and the data may also be exported to other applications.

The following sections are included in this Help topic:

- Important Notes
- Interface Graph Types

- Building a New Graph Window
- Displaying a New Graph Window
  - Bookmarking Graphs
  - Printing Graphs
  - Exporting Data

Important Notes

If an interface is not enabled using the **Configuration>System Properties>Interfaces** panel, no graphs will be available for that interface.

Interface Graph Types

The following graphs are available for each enabled hardware interface:

- **Packet Rates**—Displays the number of packets per second (pps) input and output on the interface. The Packet Rates displayed in the **Real-time** and **Last 10 minute** views are calculated based on a 10-second time period. The rates displayed for the other history views are calculated based on an average of the 10-second periods between each data point on the graph.
- **Bit Rates**—Displays the bits per second (bps) of traffic input and output on the interface. The Bit Rates displayed in the Real-time and Last 10 Minute views are calculated based on a 10-second time period. The rates displayed for the other history views are calculated based on an average of the 10-second periods between each data point on the graph.
- **Byte Counts**—Displays the total number of kilobytes (KB) input and output on the interface since the

interface counters were last cleared or the firewall was rebooted.

- **Packet Counts**—Displays the total number of packets (KP) input and output on the interface since the interface counters were last cleared or the firewall was rebooted.
- **Buffer Resources**—Displays the total number of buffer overruns, underruns and nobuffer conditions, in packets, on the interface since the interface counters were last cleared or the firewall was rebooted.
- **Packet Errors**—Displays the total number of CRC errors, frame errors, input errors, runts, giants, and deferred packets on the interface since the interface counters were last cleared or the firewall was rebooted.
- **Miscellaneous**—Displays the total number of received broadcasts, in packets, on the interface since the interface counters were last cleared or the firewall was rebooted.
- **Collision Counts**—Displays the total number of output errors, collisions and late collisions, in packets, on the interface since the interface counters were last cleared or the firewall was rebooted.
- **Input Queue**—Displays the instantaneous hardware and software input queue depths, in blocks, on the interface.
- **Output Queue**—Displays the instantaneous hardware and software output queue depths, in blocks, on the interface.

The following graphs are available for each enabled VLAN interface:

- **Byte Counts**—Displays the total number of kilobytes (KB) input and output on the interface since the interface counters were last cleared or the firewall was rebooted.
- **Packet Counts**—Displays the total number of packets (KP) input and output on the interface since the interface counters were last cleared or the firewall was rebooted.
- **Packet Rates**—Displays the number of packets per second (pps) input and output on the interface. The Packet Rates displayed in the Real-time and Last 10 minute views are calculated based on a 10-second time period. The rates displayed for the other history views are calculated based on an average of the 10-second periods between each data point on the graph.
- **Bit Rates**—Displays the bits per second (bps) of traffic input and output on the interface. The Bit Rates displayed in the Real-time and Last 10 Minute views are calculated based on a 10-second time period. The rates displayed for the other history views are calculated based on an average of the 10-second periods between each data point on the graph.

Copyright © 2001-2004, Cisco Systems, Inc.

Graph Windows

Monitoring>Graph Windows

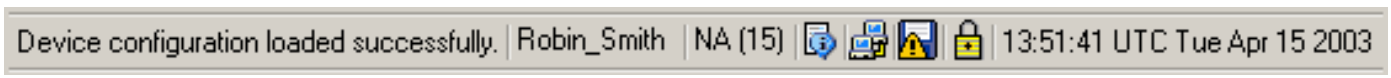
Graph Windows display up to four graphs which were added to the **Selected Graphs** list for that Graph Window. Graph Windows can be bookmarked for later recall in your browser, printed, and their data may be exported for use by other applications.

The following sections are included in this Help topic:

- Important Notes, PIX System Time
- Field Descriptions
- Bookmarking Graph Windows
- Recalling Previously Bookmarked Graph Windows
- Printing
- Exporting Graph Data

Important Notes, PIX System Time

- The time values displayed on the PDM graphs, tables, and other screens are based on PIX Firewall time converted to your local time zone. We recommend that you set the GMT (UTC) time zone as the PIX system time.
- The time zone for graphs is the time zone set on the firewall in **Configuration>System Properties>Administration>Clock**. If you are running PIX Firewall version 6.1 and have not entered the time zone information, PDM uses the time zone on your workstation.
- PIX Firewall version 6.2 or higher lets you use a NTP server to set the PIX system time in **Configuration>System Properties>Administration>NTP**.
- The PIX System Time is displayed in the status bar at the bottom right of the main PDM window.



▲

Field Descriptions

Each graph in a Graph Window has a pane which displays the following fields:

- **Graph**—The Graph tab at the top enables data to be displayed in graph form in the Graph Window.
- **Table**—The Table tab at the top enables data to be displayed in table form in the Graph Window.
- **View**—The View drop-down menu allows selection of the time frame or horizon of the data displayed in the Graph Window.
    - **Real-time**, starting when the graph is displayed, with a new data point every 10 seconds
    - **Last 10 minutes**, with a data point every 10 seconds
    - **Last 60 minutes**, with a data point every 1 minute
    - **Last 12 hours**, with a data point every 12 minutes
    - **Last 5 days**, with a data point every 2 hours

    Note: Time horizons other than **Real-time** are available for viewing only when the **History Metrics** feature is enabled using the **System Properties>History Metrics** panel. When you enable **History Metrics**, data will be stored, even when a Graph Window is not being displayed.

    The time values displayed on the graph X-axis and in the corresponding table are based on PIX Firewall time converted to your local time zone. The GMT time zone is recommended. Up to four graphs can be displayed within each Graph Window, however, there is no limit to the number of Graph Windows which can be concurrently displayed.

- **Export**—Allows Graph Window data to be exported for use by other applications.
- **Bookmark**—Allows Graph Window to be bookmarked in your browser.
- **Print**—Opens Print dialog for printing of the Graph or Table.
- **Help**—Provides more information.

▲

Bookmarking Graph Windows

Note: Bookmarking is available with PIX Firewall version 6.1 or later.

1. While in the Graph Window, click the **Bookmark** button.
2. Select the appropriate URLs for the graphs you want to bookmark in the **Bookmark Graphs** dialog box that appears. There is one link for all Graphs in a Graph Window, and a separate link for each Graph in the Graph Window.
3. To add a bookmark to your web browser, click the right mouse button on the link and choose **Add Bookmark**. (Actual text for the bookmark menu item may vary, depending on the browser.)

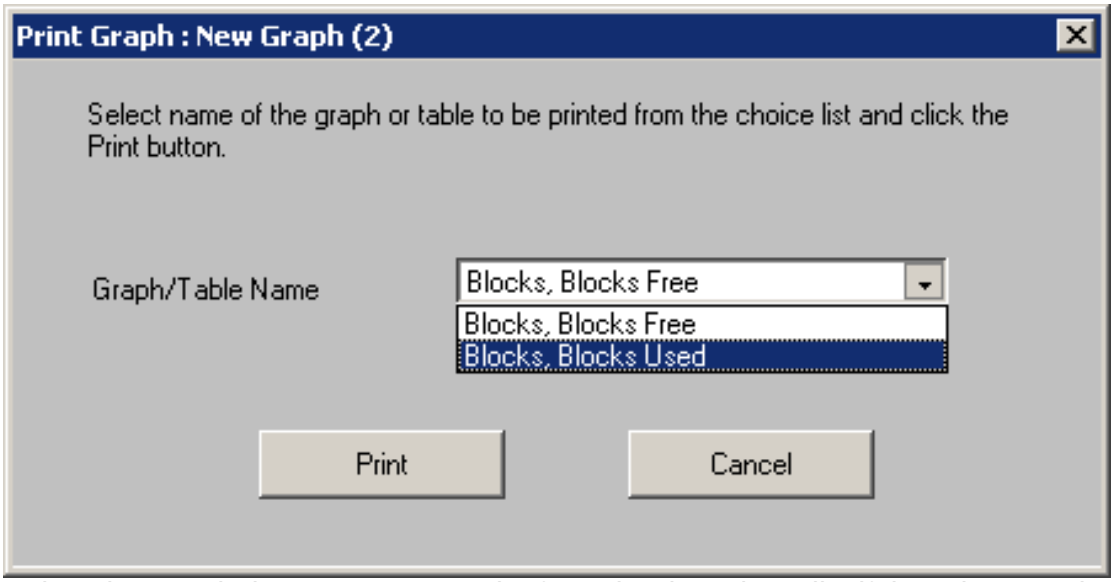
Recalling Previously Bookmarked Graph Windows

To recall a previously bookmarked Graph Window, select the bookmark in your browser. If the Graph Window already exists, it will be brought to the front. PDM does not have to be running when you select the bookmark you previously created for a Graph Window. If PDM is not running, the browser will launch PDM from the firewall from which the bookmark was created and then display the Graph Window.

The graph data starts as if you made the selection manually, unless the Graph Window is already created. The graph data is not persistent and does not continue where it left off the last time.

Printing Graphs

1. In the Graph Window, click the **Print** button
2. If there is more than one Graph in the Graph Window, the **Print Graph** dialog box appears.



3. Select the Graph that you want to print from the drop-down list if there is more than one Graph.
4. Click on the Print button to proceed to the operating system Print dialog. Data will be printed in the format, Graph or Table, currently being displayed.

Note: If PDM is running in Netscape Navigator and the browser has not yet given print privileges to the applet, then this brings up a security dialog requesting print privileges be granted. Click the **Grant** button to give the applet printing privileges. When using Internet Explorer, permission to print is already granted when you originally accepted the signed applet.

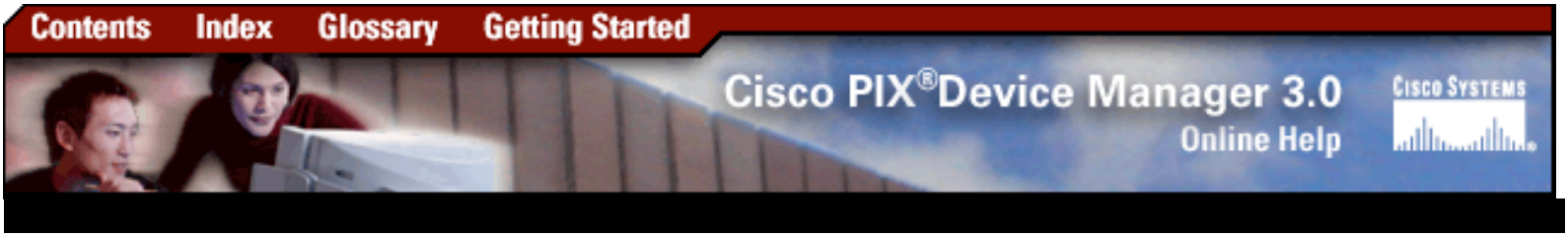
Exporting Graph Data

To export Graph or Table data in a comma-separated value format, use the following steps:

1. From the Graph Window, select **Export**.
2. Similar to printing, if there is more than one Graph in the Graph window, the **Export Graph Data** dialog will appear. Select one or more of the graphs listed by checking the box next to the Graph name. (More than one selection will be stored in a single file.)
3. Click **Export** at the bottom of the dialog box.
4. When the operating system standard File dialog box appears, enter a filename for the data.

Note: Similar to printing, if PDM is running in Netscape Navigator, it may bring up a security dialog requesting additional privileges be granted. Click the **Grant** button to continue.

Copyright © 2001-2004, Cisco Systems, Inc.



IDS

Monitoring>Miscellaneous Graphs>IDS

The **Monitoring>Miscellaneous Graphs>IDS** (Intrusion Detection System) panel lets you monitor Intrusion Detection statistics, including packet counts for each Intrusion Detection System IDS signature supported by the firewall. These graphs may be bookmarked for quick opening by your browser, printed, and the data may also be exported to other applications.

The following sections are included in this Help topic:

- Important Notes
- IDS Graph Types

- Building a New Graph Window
- Displaying a New Graph Window
  - Bookmarking Graphs
  - Printing Graphs
  - Exporting Data

Important Notes

IDS statistics are tracked by the firewall, thus available for graphing, only when one or more IDS Policies are enabled using the **Configuration>System Properties>Intrusion>IDS Policy** and **Configuration>System Properties>Intrusion>IDS Signatures** panels.

▲

IDS Graph Types

The IDS graphs represent the complete collection of IDS signatures supported by the firewall, categorized into subsets with one graph per subset. Each graph contains one to five IDS informational or attack signatures, with packet counts representing hits for each signature since the IDS statistics were last cleared or the firewall rebooted.

- IP Options
- IP Route Options
- IP Attacks
- ICMP Requests

- ICMP Responses
- ICMP Replies
- ICMP Attacks
- TCP Attacks
- UDP Attacks
- DNS Attacks
- FTP Attacks
- RPC Requests to Target Hosts
- YP Daemon Portmap Requests
- Miscellaneous Portmap Requests
- Miscellaneous RPC Calls
- RPC Attacks

Copyright © 2001-2004, Cisco Systems, Inc.

Connection Graphs

Monitoring>Connection Graphs

The **Connection Graphs** panel lets you monitor a wide variety of performance statistics for features of the firewall, including statistics for xlates, connections, AAA, fixups, URL filtering and TCP Intercept. These graphs may be bookmarked for quick opening by your browser, printed, and the data may also be exported to other applications.

The following sections are included in this Help topic:

- Connection Graph Types
- Building a New Graph Window
- Displaying a New Graph Window
  - Bookmarking Graphs
  - Printing Graphs
  - Exporting Data

Connection Graph Types

The following graph types and their associated graphs are available:

Note: The Connection graphs use a default time interval (**View**) of 120 seconds over which the packets per second, connections per second, and transactions per second are calculated. This interval may be changed using the 'perfmon interval' command via the **Tools>Command Line Interface** panel.

- **Xlates**:
  - **Xlate Utilization** - Displays the number of xlates per second during the last interval. An xlate, also referred to as a translation entry, represents a mapping of one IP address to another, or a mapping of one IP address/port pair to another.
- **Perfmon**:
  - **AAA Perfmon**—Displays the number of Authentication, Authorization and Accounting requests sent to a AAA server per second during the last interval.
  - **Fixup Perfmon**—Displays the number of packets per second for traffic that was processed by the HTTP, FTP or TCP fixup routines during the last interval.
  - **Web Perfmon**—Displays the number of URL requests per second processed by the firewall, and the

number of Websense requests per second made by the firewall during the last interval. Note that the number of Websense requests does not include any URL filtering decisions made using the internal URL cache of the firewall.

- **Connections Perfmon**—Displays the number of total connections, TCP connections, UDP connections and TCP Intercepts per second processed by the firewall during the last interval.

Copyright © 2001-2004, Cisco Systems, Inc.

System Graphs

Monitoring>System Graphs

The **System Graphs** panel lets you build a New Graph window, which monitors the system resources of the firewall, including block utilization, CPU utilization, failover statistics, and memory utilization. These graphs may be bookmarked for quick opening by your browser, printed, and the data may also be exported to other applications.

The following sections are included in this Help topic:

- System Graph Types
  - Blocks
  - CPU
  - Failover
  - Memory
- Building a New Graph Window
- Displaying a New Graph Window
  - Bookmarking Graphs
  - Printing Graphs
  - Exporting Data

System Graph Types

The following graph types and their associated graphs are available:

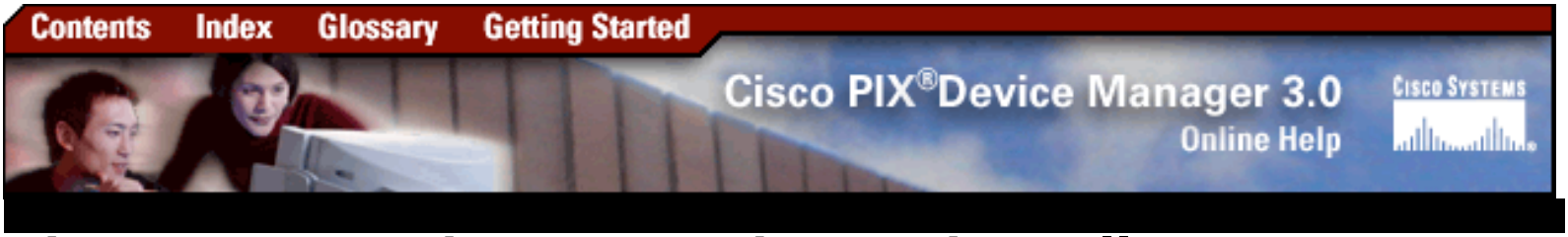
- **Blocks**:
  - **Blocks Used**—Displays the number of used blocks for each preallocated Firewall block size.
  - **Blocks Free**—Displays the number of available blocks for each preallocated Firewall block size.
- **CPU**:
  - **CPU Utilization**—Displays the firewall CPU utilization (percent). Each data point represents an instantaneous snapshot of the firewall CPU utilization at that moment in time.
- **Failover**:
  - **Translation Information**—Displays the number of xlate state update packets sent by the firewall to its failover partner, and received from its failover partner, since failover was enabled or the firewall rebooted.

- **TCP Connection Information**—Displays the number of TCP connection state update packets sent by the firewall to its failover partner, and received from its failover partner, since failover was enabled or the firewall rebooted.
- **UDP Connection Information**—Displays the number of UDP connection state update packets sent by the firewall to its failover partner, and received from its failover partner, since failover was enabled or the firewall rebooted.
- **Xmit Queue**—Displays the current depth, in packets, of the failover update queue used by the firewall to send state update packets to its failover partner. Also displays the maximum queue depth and total number of packets queued since failover was enabled or the firewall rebooted.
- **Receive Queue**—Displays the current depth, in packets, of the failover update queue used by the firewall to receive state update packets from its failover partner. Also displays the maximum queue depth and total number of packets queued since failover was enabled or the firewall rebooted.

  Note: If failover is not enabled using the Failover panel under System Properties, no failover graphs will be available for viewing.

- **Memory**:
  - **Memory Utilization**—Displays the number of physical memory bytes free and bytes used.

Copyright © 2001-2004, Cisco Systems, Inc.



Show Unparsed Commands on Firewall

Options>Show Unparsed Commands on Firewall

The **Show Unparsed Command on Firewall** panel lists commands that are ignored by PDM.

PDM does not fully support the complete firewall software command set. There are different types of unsupported commands. Some commands that PDM can parse cannot be edited within PDM. Others can be parsed, but cause PDM to enter the Monitor Only mode. Some commands can be used by themselves, but become unsupported in combination with another command.

Commands that appear in the Unparsed Commands list, are commands that PDM cannot parse and are ignored. These commands stay in the configuration and their values cannot be changed within PDM.

The **Unparsed Commands** panel displays the following explanation:

```
The Cisco PDM did not understand the following commands while parsing the
running configuration of your firewall. PDM does not support the complete
firewall command set. PDM will ignore the command(s) which appear below.
They will not be removed from or changed in the running firewall
configuration.
```

This message is followed by a list of the commands that are not parsed for that version of PDM.

For more information and possible corrections, refer to the *Cisco PIX Device Manager Installation Guide* or release notes for your version of PDM software.

Note: For more information about the CLI commands used by each PDM screen, see **CLI Commands Used by PDM Screens**.

Field Descriptions

The Unparsed Commands panel provides the following fields:

- **Unparsed Command(s)**—A list of the commands that could not be parsed when the configuration was applied to the firewall unit, after clicking **Apply**. For example, an access list that was not applied to an

interface is ignored and displays:

```
access-list for_example permit ip 10.1.3.0 255.255.255.0 10.1.2.0 255.255.255.0
```

- **OK**—Accepts changes and returns to the previous panel.
- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

Add/Edit Host/Network Group

Configuration>Hosts/Networks Groups>Add/Edit>Add/Edit Host/Network Group

The **Add/Edit Host/Network Group** dialog box appears when you click **Add** or **Edit** on the **Groups** region of the **Configuration>Hosts/Networks** tab. You can use the **Add/Edit Host/Network Group** dialog box to define groups of hosts or subnetworks. After creating a Host/Network group, you can apply a single rule to all the members of the Host/Network group.

The following sections are included in this Help topic:

- Introduction
  - Object Groups
  - Network Groups
- Important Notes
- Field Descriptions
  - Interface
  - Group Name
  - Description
- Adding Members to a Group
- Removing Members from a Group

Introduction

Firewall Object Groups

PIX Firewall object groups allow multiple objects, such as networks or services, to be associated and given a name. To simplify configuration, a name may then be used in place of a list in PDM Rules or VPN configuration.

PIX Firewall Version 6.2 and higher supports 4 types of named object groups:

- **`host/network (network)`**
- **`protocol`**
- **`icmp-type`**
- **`service`**

Object Group Names—The **Name** of any object group must be unique to all 4 types. For example, a **`service`** group and a **`network`** group may not share the same name.

Host/Network and **Service Types**—PDM uses Host/Network and Service type objects. You may add, edit or delete **`network`** type object groups in Configuration>Hosts/Networks Groups>Add/Edit> Add/Edit Host/Network Group and **`service`** type object groups in **Tools>Service Groups**, **Configuration>VPN**, and **Configuration>Access Rules**. For more information, see Network Groups and Manage Service Groups

ICMP and Protocol Types—The object group types **`icmp-type`** and **`protocol`** are not created in PDM and may not be renamed in PDM. However, PDM does support editing and deleting object groups using **Tools->CLI** (Command Line Interface).

Hierarchical/Nested Service Groups—Manage Service Groups lets you associate multiple TCP or UDP services (ports) in a named group. You can also add service object groups to a service object group. You may find this useful when the use of groups is hierarchical or to reuse existing service groups. You can then use the nested service group like any other group in an access rule, a conduit, or for IPSec rules. Nested **network** groups are not supported by PDM.

Network Groups

Host/Network groups are associated with an interface. Host and network IP addresses can be associated in a group to simplify management in complex or large configurations.

When a PDM user adds/edits/deletes a Host/Network PDM updates the groups appropriately.

When a PDM user edits/deletes a Translation Rule of a host/network used as a member in a network object group, PDM updates the reference groups appropriately.

When a network group used in a security rule is modified or deleted PDM modifies/deletes these rules respectively.

PDM may not be used to create nested or hierarchical network object-groups. Nested means that the group that has other groups has its members. If a nested group is configured using the CLI or otherwise, and it is used in an access-list or conduit, PDM will parse it, and show it in the rule table. However, it cannot be edited within PDM.

Important Notes about Network Object Groups

1. **Group members and Names**
   - Once a new group is created and named, it must always have at least one member.
   - Host/Network group names must be unique within all Host/Network groups and a Host/Network group may not share the same name as a service/port group.

2. **Nesting**—Nested or hierarchical network object grouping is not supported.

3. **Legacy PIX syntax**—Network object grouping in not supported with Filter Rules, Outbounds (rules that use

outbound keyword) and AAA rules using legacy PIX syntax with **include/exclude** in rules.

4. **Real** and **Reference Groups**—PDM sends the appropriate **object-group/network-object** commands to create real and reference groups.
   - **real_group_name** - name of an object group which contains real IP addresses
   - **associated_intf_name** - name of the interface to which the specified object group is associated. The name must have been defined by the 'nameif' command.
   - **ref_group_name** - name of an object group which contains NAT'd IP addresses of the object group specified by <**real_group_name**>
   - **ref_intf_name** - name of the interface from which the destination IP address of inbound traffic is NAT'd. The name must have been defined by the **nameif** command.
   - **reference** - keyword to associate the object group which contains real IP addresses and the object group which contains the NAT'd IP addresses.

     A **pdm group** command without the **reference** keyword allows PDM to associate a **network object-group** to an **interface**.

     A **pdm group** command with the **reference** keyword allows PDM to associate a **network object-group** which contains real IP addresses to its corresponding **network object-group** which contains NAT'd IP addresses.

5. **NAT**—For all **inbound** access rules, such as outside to inside access rules, the real IP address of the inside hosts is used to specify the destination IP address. PDM locates the NAT'd IP addresses for these inside hosts and then applies them to the PIX **access-list** CLI commands used by rules because the PIX **access-list** command expects the NAT'd IP addresses.

   This requires PDM to maintain the relationship between the real IP address and the NAT'd IP address. Using **network** object groups, PDM translates by maintaining the relationship between the object group containing the real IP addresses and the object group containing the NAT'd IP addresses. NAT'd IP addresses include static and dynamic NAT rules as defined in the Translation Rules table in PDM.

   This is achieved by these two CLI commands that PDM sends to PIX:

   - **pdm group <real_group_name> <associated_intf_name>**
   - **pdm group <ref_group_name> <ref_intf_name> reference <real_group_name>**

Field Descriptions

- **Interface**—The name of the interface associated with this group.
- **Group Name**—Enter a mandatory group name in this field to uniquely identify the group. See Important Notes, Group Members and Names.
- **Description**—Enter an optional group description in this field to provide an explanation of how membership in the group is determined or how the group is used in your security policy.

Adding Members to a Host/Network Group

Follow these steps to add members to a group:

1. In the **Add/Edit Host/Network Group** dialog box, select the host or network address from **Members not in the group**.
2. Click **Add>** to copy the host or network address to **Members in group.**
3. Click **OK**.

Removing Members from a Host/Network Group

Follow these steps to remove members from a group:

1. In the **Add/Edit Host/Network Group** dialog box, select the host or network address from **Members in group**
2. Click **<Remove** to move the selected host or network address back to **Members not in group.**
3. Click **OK**.

Copyright © 2001-2004, Cisco Systems, Inc.

Service Groups

Tools>Service Groups

The **Manage Service Groups** panel lets you associate multiple TCP or UDP services (ports) in a named group. You can then use the service group in an access or IPSec rule, a conduit, or other functions within PDM and the CLI.

The following sections are included in this Help topic:

- Introduction
  - Firewall Object Groups
  - Manage Service Groups
- Field Descriptions
  - TCP
  - UDP
  - TCP-UDP
  - Service Group
  - Description
- Adding a Service Group
- Editing a Service Group
- Deleting a Service Group

Introduction

Firewall Object Groups

Object groups allow multiple objects, such as networks or services, to be associated with a given name. To simplify configuration, a name may then be used in place of a list in PDM rules or VPN configuration.

PIX Firewall Version 6.2 and higher support four types of named object groups:

- host/network (network)
- protocol
- icmp-type
- service

Object Group Names—The **Name** of any object group must be unique to all four types. For example, a **service**

group and a **network group** may not share the same name.

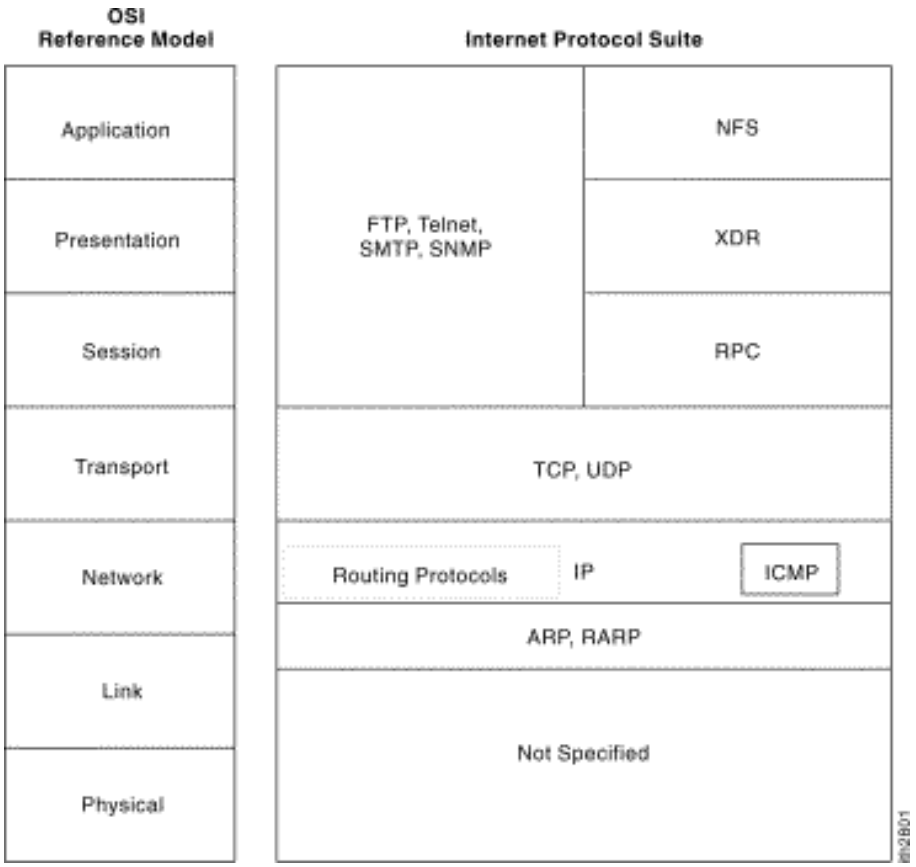
Host/Network and **Service Types**—PDM uses Host/Network and service type objects. You can add, edit or delete **network** type object groups in Configuration>Hosts/Networks>Group and **service** type object groups in Tools>Service Groups, Configuration>VPN, and Configuration>Access Rules.

ICMP and Protocol Types—The object group types **icmp-type** and **protocol** are not created in PDM and, therefore, cannot be renamed in PDM. However, PDM does support editing and deleting object groups using Tools>Command Line Interface.

Hierarchical/Nested Service Groups—Manage Service Groups lets you associate multiple TCP or UDP services (ports) in a named group. You can also add service object groups to a service object group. You might find this useful when the use of groups is hierarchical or to reuse existing service groups. You can then use the nested service group like any other group in an access rule, a conduit, or for IPSec rules. Nested **network** groups are not supported by PDM.

Manage Service Groups

The term, *service* refers to higher layer protocols associated with application level services having "well known" port numbers and "literal" names, such as **ftp**, **telnet**, and **smtp**.



PIX Firewall permits the following TCP literal names:

`bgp, chargen, cmd, daytime, discard, domain, echo, exec, finger, ftp, ftp-data, gopher, h323, hostname, http, ident, irc, klogin, kshell, lpd, nntp, pop2, pop3, pptp, rpc, smtp, sqlnet, sunrpc, tacacs, talk, telnet, time, uucp, whois, www.`

The **Manage Service Groups** panel lets you add, edit and delete service groups for use in Configuration>Access Rules and Configuration>VPN. It can be opened from the following locations within PDM:

- **Tools>Service Groups**
- **Configuration>Access Rules>Add>Manage Service Groups**
- **Configuration>Access Rules>Edit>Manage Service Groups**
- **Configuration>VPN>IPSec>IPSec Rules>Add Rule>Manage Service Groups**
- **Configuration>VPN>IPSec>IPSec Rules>Edit>Manage Service Groups**

The **Name** of a service group must be unique to all four types of object groups. For example, a **service** group and a **network** group may not share the same name.

Multiple service groups can be nested into a "group of groups" and used the same as a single group. When a service object group is deleted, it is removed from all service object groups where it is used.

If a service group is used in an access rule, do not remove it. A service group used in an access rule cannot be made empty.

Field Descriptions

- **TCP**—Select this option to add TCP services or port numbers to an object group.
- **UDP**—Select this option to add UDP services or port numbers to an object group
- **TCP-UDP**—Select this option to add services or port numbers that are common to TCP and UDP to an object group.
- **Service Group**—This table contains a descriptive name for each service object group. To modify or delete a group on this list, select the group and click **Edit** or **Delete**. To add a new group to this list, click **Add**.
- **Description**—Enter an optional group description in this box to provide an explanation of how membership in the group is determined or how the group is used in your security policy.

Adding a Service Group

Follow these steps to create a new service group:

1. Select the type of service you want to add to the current group (TCP, UDP, or TCP-UDP).
2. Click **Add**.
3. In the **Add Service Group** dialog box that appears, select the services or enter a specific port or port range. The name must be unique for all object groups. A service group cannot share a name with a network group.
4. Click **OK** to close the **Add Service Group** dialog box.
5. Click **OK** to close the **Manage Service Groups** dialog box.

Editing a Service Group

Follow these steps to change an existing service group:

1. Select an existing service group from the list.
2. Click **Edit**.
3. In the **Edit Service Group** dialog box that appears, change the selected services or port numbers, as required. The name must be unique for all object groups. A service group cannot share a name with a network group.
4. Click **OK** to close the **Edit Service Group** dialog box.
5. Click **OK** to close the **Manage Service Groups** dialog box.

Deleting a Service Group

Follow these steps to delete an existing service group:

1. Select an existing service group from the table in **Manage Service Groups**
2. Click **Delete**.

Note: **Deleting Service Groups**

- When a service object group is deleted, it is removed from all service object groups where it is used.
- If a service group is used in an access rule, do not remove it. A service group used in an access rule cannot be made empty.

Copyright © 2001-2004, Cisco Systems, Inc.

Turbo Access Rules

Configuration>System Properties>Advanced>Turbo Access Rules

The **Turbo Access Rules** panel lets you speed up processing of large access rules by allocating additional memory to any access rule with 19 or more entries. The **Configuration>Access Rules** tab, **Configuration>Translation Rules** tab, and other areas in PDM use access rules.

An access rule typically consists of multiple access rule entries, organized internally by the firewall as a linked list. When a packet is subjected to access rule control, the firewall searches this linked list linearly to find a matching element. The matching element is then examined to determine if the packet is to be transmitted or dropped. With a linear search, the average search time increases proportional to the size of the list.

Turbo Access Rules is a feature that improves the average search time for access rules containing a large number of entries. The Turbo Access Rules feature causes the firewall to compile tables for access rules and this improves searching of long rule lists.

For a firewall with 18 or less entries, Turbo Access Rules do not improve performance. For this reason, even when enabled, the Turbo Access Rules feature is only applied to a firewall with nineteen or more entries.

The TurboACL feature requires significant amounts of memory and is most appropriate for high-end firewall models, such as the PIX 525 or PIX 535. The minimum memory required for TurboACL is 2.1 MB and approximately 1 MB of memory is required for every 2000 ACL elements.

Note: Turbo ACL is not supported for the PIX 501.

More information about Turbo Access Rules are available in the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

Important Notes

- Enabling Turbo Access Rule Searches for a particular access list is not supported in PDM.
- This feature will have no effect if your firewall is configured to use only conduits.
- This feature is not available on the PIX 501.
- Turbo Access Rules can be memory intensive, depending on the number of access-lists configured. For performance reasons, do not enable this feature at peak usage hours.

Field Descriptions

This **Turbo Access Rule** panel displays the following fields:

- **Enable Turbo Access Rule Searches**—Select this check box to use this feature.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

DHCP Server

Configuration>System Properties>DHCP Server

The **DHCP Server** panel lets you configure the firewall as a DHCP server for hosts connected to the firewall interfaces. You can configure up to one DHCP server on each firewall interface.

Note: You cannot configure the DHCP server if the firewall is already configured as a DHCP relay agent. For more information about DHCP relay, refer to the DHCP relay Help topic.

The following sections are included in this Help topic:

- Field Descriptions
- Configuring the DHCP Server
- Configuring DHCP Server Autoconfiguration
- Configuring DHCP Server Options 150 and 66
- Viewing DHCP Server Statistics

Field Descriptions

The **DHCP** panel displays the following fields:

- **Edit**—Lets you access configuration parameters used to enable DHCP on the firewall interfaces and assign the range of IP addresses for the DHCP server pool.
  - **Enable DHCP**—Select this check box to turn on DHCP for the firewall on the selected interface.
  - **DHCP Address Pool**—Enter the range of IP addresses, from lowest to highest, for the DHCP server pool; for example, 10.0.1.101–10.0.1.110. The range of IP addresses must be on the same subnet as the interface on which the DHCP server is configured, but must not include the IP address of the DHCP server interface itself.

    Note: DHCP-assigned IP addresses—The PIX 501 with the 10-user license supports 32 DHCP-assigned IP addresses, 128 with the 50-user license, and 256 with the unlimited user license. All other platforms support 256 DHCP-assigned IP addresses.
- **Lease Length (seconds)**—Enter the amount of time (in seconds) the client can use its allocated IP address before the lease expires. The default value is 3600 seconds (1 hour).
- **Ping Timeout (milliseconds)**—Enter the number of milliseconds the firewall should wait before declaring timeout on a Ping. To verify the status of its DHCP leases, the firewall uses Ping to dynamically determine if an IP address is still in use by a client. The default value is 750 milliseconds.
- **Advanced**—Allows configuration of DHCP option 150 and option 66. DCHP option 150 and DHCP option 66 are used to provide the TFTP server address and name values of Cisco IP Phones on the inside network.

    - **Option 150**
        - **TFTP Server 1 IP**—Enter the IP address of the TFTP server to use for option 150.
        - **TFTP Server 2 IP**—Enter the IP address of the alternate TFTP server to use for option 150.
    - **Option 66**
        - **TFTP Server 1 IP**—Enter the IP address or the host name of the TFTP server for option 66.
- **Other DHCP Options**
    - **Enable autoconfiguration**—Instructs the DHCP server to configure the domain name, DNS, and WINS information.
    - **DNS Server 1**—Enter the IP address of the DNS server to use to automatically configure DNS.
    - **DNS Server 2**—Enter the IP address of the alternate DNS server to use to automatically configure DNS.
    - **Domain Name**—Enter the domain name of the DNS server to use to automatically configure DNS.
    - **Primary WINS Server**—Enter the IP address of the WINS (Windows Internet Naming Service) server to use to automatically configure DNS.
    - **Secondary WINS Server**—Enter the IP address of the alternate WINS server to use to automatically configure DNS.

Configuring the DHCP Server

Follow these steps to configure DHCP on an interface:

1. Highlight the interface on which to configure DHCP.
2. Click **Edit**.
3. Select the **Enable DHCP** check box.
4. Enter the range of IP addresses, from lowest to highest, that the DHCP server will use in the **DHCP Address Pool** box; for example, 10.0.1.101–10.0.1.110. The range of IP addresses must be on the same subnet as the interface on which the DHCP server is configured, but must not include the IP address of the DHCP server interface itself.
5. Click **OK**.
6. (Optional) Enter the amount of time (in seconds) the client can use its allocated IP address before the lease expires in the **Lease Length** box. The default value is 3600 seconds (1 hour).
7. (Optional) Enter the number of milliseconds the firewall should wait before declaring timeout on a Ping in the **Ping Timeout** box.

Configuring DHCP Server Autoconfiguration

Enabling autoconfiguration on the outside interface lets the DHCP server automatically configure DNS servers, the DNS default domain name, and WINS. To enable autoconfiguration, select the **Enable Autoconfiguration** check box.

The following steps are optional and override the DHCP autoconfigured values:

1. Enter the DNS domain name in the **Domain Name** box.
2. Enter the IP address(es) of the DNS server(s) the client will use in the **Server 1** and **Server 2** boxes. You can enter up to two DNS servers.
3. Enter the IP address(es) of the WINS server(s) the client will use in the **Server 1** and **Server 2** boxes. You can specify up to two WINS servers.

Configuring DHCP Server Options 150 and 66

DHCP requests are broadcast to the subnet. When enabled as a DHCP server, the firewall responds to DHCP requests. PIX Firewall Version 6.2 and higher support responding to DHCP requests with options 150 and 66.

DHCP option 150 provides for a DHCP server to supply a list of site-specific IP addresses for applications such as IP telephony.

DHCP option 66 is defined in RFC 2132 (DHCP options and BOOTP Vendor Extensions.) It gives the IP address or the host name of a single TFTP server [8].

IP phones may also include DHCP option 3 in their requests. The DHCP server in PIX Firewall Version 6.0(1) has already supported this option, which lists the IP addresses of default routers.

IP phones may include other DHCP options in their requests. Refer to the IP phone software documentation for additional information.

A typical IP telephony implementation for an Enterprise with small branch offices, such as Cisco AVVID, features remote sites with Cisco IP Phones connected to Cisco CallManager at the central office through a firewall protecting the branch office. This allows centralized call processing, reduces the equipment required & eliminates the administration of additional Cisco CallManager and application servers (for example, TFTP server & DNS server) at the branch offices.

PIX Firewall support for DHCP options 150 and 66 allows a Cisco IP Phone which does not have a statically defined IP address to register with the Cisco CallManager after the PIX Firewalls at the branch and central office have been properly configured to permit the voice signal traffic.

Before a Cisco IP Phone connects to Cisco CallManager, it needs to download its own configuration file from a designated TFTP server. When an Cisco IP Phone starts, if it does not have both the IP address and TFTP server IP address preconfigured, it sends a request with option 150 or 66 to the DHCP server for this information.

If the Cisco IP Phone has a statically defined IP address, Cisco IP Phones require configuration of the TFTP server locally on the phone, so that it can communicate with the TFTP server directly.

If the Cisco IP Phone requests an IP address from DHCP server, but has a statically defined TFTP server IP address, it may include options 150 or 66 in the DHCP server request. In this case, the PIX Firewall DHCP server responds with the TFTP server IP address(es) designated for Cisco IP Phones.

It is possible for Cisco IP Phones to include both options 150 and 66 in a single request. In this case, the PIX Firewall will provide values for both options in the response and let Cisco IP Phones decide which one it will use.

Follow these steps to configure DHCP options 150 and 66:

1. Click **Advanced**.
2. In the DHCP option 150 panel, enter the IP address of the first TFTP server to use for option 150 in the **TFTP Server 1 IP** box.
3. (Optional) Enter the IP address of an alternate TFTP server to use for option 150 in the **TFTP Server 2 IP** box, should the first TFTP server become unavailable.
4. In the DHCP option 66 panel, enter the host name or IP address of the TFTP server to use for option 66.
5. Click **OK**.

Viewing DHCP Server Statistics

To see DHCP statistics, click **Tools>Command Line Interface**, and then enter the **show dhcpd statistics** and **show dhcpd binding** commands. PDM does not provide statistics for the DHCP server.

Copyright © 2001-2004, Cisco Systems, Inc.

DHCP Relay

Configuration>System Properties>DHCP Relay

The **DHCP Relay** panel lets you configure the firewall as a DHCP relay agent. When configured as a DHCP relay agent, the firewall uses external DHCP servers, on the interfaces you specify, to assign IP addresses dynamically to clients on the Ethernet interfaces of the firewall. When the firewall receives a request from a client on one interface, the request is forwarded to a DHCP server on another interface.

Note:You cannot configure the DHCP relay agent if a DHCP server is enabled on the firewall. The DHCP relay agent works only with external DHCP servers.

The following sections are included in this Help topic:

- Field Descriptions
- Configuring DHCP Relay
- Adding/Editing the DHCP Server
- Editing the DHCP Relay Agent

Field Descriptions

The **DHCP Relay Servers** panel displays the following fields:

- **Timeout**—Specifies the number of seconds allowed for DHCP relay address negotiation. The default is 60 seconds.
- **Server—**Specifies the IP address of the DHCP server to which DHCP requests are relayed by the firewall.
- **Interface—**Specifies the interface on which DHCP requests are relayed to the DHCP server.

The **DHCP Relay Agent** panel displays the following fields:

- **Interface**—Specifies the interface on which DHCP requests are received from clients. By default, the DHCP relay agent is disabled.
- **DHCP Relay Enabled—**Specifies if DHCP relay is enabled on the interface.
- **Set Route—**Configures the DHCP relay agent to change the default route address, in the packet sent from the DHCP server, to the interface on which the DHCP relay agent is configured. When selected, this option sets a default route from the client to the firewall.

Configuring DHCP Relay

Follow these steps to configure DHCP relay:

1. Configure the DHCP server.
2. Configure the DHCP relay agent.

Note: You should configure the external DHCP server before configuring the DHCP relay agent on a firewall interface.

Adding/Editing the DHCP Server

Follow these steps to add/edit the DHCP server:

1. Enter the IP address of the server to relay DHCP requests to in the **DHCP Server** box.
2. Select the name of the interface from the **Interface** list.
3. Click **OK**.
4. Repeat Steps 1 through 3 to configure additional DHCP servers. You can configure up to four external DHCP servers on additional interfaces.

See also Configuring DHCP Relay.

Editing DHCP Relay Agent

Follow these steps to edit the DHCP relay agent:

1. Select the **Enable DHCP Relay Agent on the** *interface* **interface** check box to enable DHCP relay on the interface you selected.
2. Select the **Set Route** check box to change the default route address to the address of the interface on which the DHCP relay agent is configured. When selected, this option sets a default route from the client to the firewall. Leave the check box clear to keep the default route address unchanged.
3. Click **OK**.
4. Repeat Steps 1 through 3 to configure a DHCP relay agent on additional interfaces. You can configure a DHCP relay agent on multiple interfaces.

See also Configuring DHCP Relay.

Copyright © 2001-2004, Cisco Systems, Inc.

URL Filtering

Configuration>System Properties>URL Filtering

The **URL Filtering** panel lets you prevent internal users from accessing external World Wide Web URLs (HTTP, HTTPS, or FTP) that you designate using the Websense or N2H2 URL filtering server.

After you define your URL filtering server(s) and related parameters on this panel, use the **Filter Rules** panel to define the rules that are used to enforce URL filtering.

The following sections are included in this Help topic:

- Important Notes
- Websense Overview
- N2H2 Overview
- Field Descriptions
- Configuring Advanced URL Filtering
- Adding or Editing a URL Filtering Server
- Deleting a URL Filtering Server
- Resetting to Last Applied Settings

Important Notes

- The URL filtering feature is available only if you have the Websense or N2H2 third-party application, available from http://www.websense.com or http://www.N2H2.com.
- A total of 16 URL servers can be configured. The primary filtering server is the first server in the list. The firewall can be configured to use either N2H2 or Websense, but not both. For example, If you configure the firewall to use two Websense servers, and then you select N2H2, a warning appears asking you to click **OK** or **Cancel**. If you click **OK**, then all the previously configured Websense servers are removed, and the new N2H2 server is added. This action also takes place when switching from N2H2 to Websense.
- HTTPS and FTP filtering are not supported for the N2H2 filtering server.
- If you change policy settings within the Websense server application, you must disable then reenable the Websense cache to ensure the cached information does not conflict with any new policy settings.

Websense Overview

For HTTP, when a user issues an HTTP request to a website, the firewall sends the request to the website and to the Websense server at the same time. If the Websense server permits the connection, the firewall allows the reply from the website to reach the user who issued the original request. If the Websense server denies the connection, the firewall redirects the user to a block page, indicating that access was denied.

For HTTPS, the firewall prevents the completion of SSL connection negotiation. The browser displays an error message such as "The Page or the content cannot be displayed." Because HTTPS content is encrypted, the firewall sends the URL to the Websense server without directory and filename information.

For FTP, when a user issues an FTP **get** request to a server, the firewall sends the request to the FTP server and to the Websense server at the same time. If the Websense server permits the connection, the firewall allows the successful FTP return code to reach the user unchanged (for example, a successful return code is 250: CWD command successful). If the Websense server denies the connection, the firewall alters the FTP return code to show that the connection was denied (for example, the firewall changes code 250 to code 550: Directory not found). Websense only filters FTP **get** commands (and not **put** commands).

See http://www.websense.com for more information.

N2H2 Overview

N2H2's URL filtering software, Filtering by N2H2, can filter HTTP requests based on destination host name, destination IP address, username, and password. Filtering by N2H2 relies on N2H2's sophisticated URL database, which includes more than 15 million sites organized into over 40 content categories.

Note: HTTPS and FTP filtering are not supported for the N2H2 filtering server.

The firewall and the N2H2 server use N2H2's Internet Filtering Protocol (IFP) to communicate with each other over TCP or UDP. When the firewall receives an HTTP request, it sends an IFP request to the N2H2 server along with the requested URL. The N2H2 server processes the request and returns an IFP response. Based on the IFP response, the firewall either blocks the HTTP request by redirecting the requesting browser to a block page, or allows normal HTTP processing to continue. The N2H2 server also logs IFP responses; this log can be used for reporting and auditing.

For more information about Filtering by N2H2, see N2H2's website at http://www.n2h2.com

Field Descriptions

The **URL Filtering Server** area includes the following items:

- **Websense** radio button—Selects Websense URL filtering. You can only include one type of server (Websense or N2H2, but not both).
- **N2H2** radio button—Selects N2H2 URL filtering. You can only include one type of server (Websense or N2H2, but not both).
- **N2H2 Port** field—If you click the N2H2 radio button, enter the N2H2 URL filtering port. The default is 4005.
- **URL Filtering Server** table—This table shows the servers in prioritized order. The server at the top of the list is the only one used unless it fails. If the first server fails, the firewall goes down the list until it finds an active server.
    - **Interface**—The name of the network interface on which the URL server resides.
    - **IP Address**—The IP address of the server that runs the URL filtering application.
    - **Timeout**—The timeout value, in seconds, before the firewall tries to access the next URL server.
    - **Protocol**—The protocol version selected for the URL server. See Adding or Editing a URL Filtering Server for more information.
- **Insert Before** button—Adds a new server above the selected one.
- **Insert After** button—Adds a new server below the selected one.
- **Add** button—Adds a server at the end of the list.
- **Edit** button—Edits the selected URL server.
- **Delete** button—Deletes the selected URL server.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.
- **Advanced** button—Opens the **Advanced URL Filtering** dialog box.

Configuring Advanced URL Filtering

Follow these steps to set advanced URL filtering options. These options apply to all servers.

1. On the **Configuration>System Properties>URL Filtering** page, click **Advanced**.

   The **Advanced URL Filtering** dialog box opens.

2. Set the following options:

- **URL Cache Size** area—Specifies the size of the cache that is used to cache the URL access privileges in the memory of the firewall.
    - **Enable caching based on** check box—Enables caching based address pairs:
        - **Destination Address** radio button—Selects caching based on **Destination Address**. Select if all users share the same URL filtering policy on the URL Filtering server.
        - **Source/Destination Address** radio button—Selects caching based on **Source/Destination Address** pairs. Select if users do not share the same URL filtering policy on the URL Filtering server.
    - **Cache Size** field—Amount of memory in KB allocated for caching.

Note: Access to the URL cache does not update the Websense accounting logs. Before using this feature, let Websense run to accumulate logs to let you view Websense accounting information. After you get a usage profile that meets your security needs, enable this feature to increase throughput.

- **URL Buffer Size** area—Sets buffering options.
  - **Enable buffering** check box—Enables buffering and buffers the response from the web server in cases where the URL filter response from the URL server has not been received.
  - **Number of 1550-byte buffers** field—Number of 1550-byte buffers to allocate for URL buffering. 1-128 blocks.
- **Long URL Support** area—By default, the firewall considers a URL to be a long URL if it is greater than 1159 characters. The maximum size of the long URL can be set in this area. If the URL exceeds the maximum size, then it is by default dropped. You can configure the action taken for each filter rule on the Access Rules tab: drop, block, or truncate.
  - **Use Long URL** check box—Enables the Long URL feature. If the Long URL feature is enabled, you may not add/switch to N2H2 or add/switch to a Websense server with the UDP Protocol. Long URL support is limited to Websense servers using TCP, and not N2H2 servers.
  - **Maximum Long URL Size** field—The maximum size of the Long URL from 2 to 4 KB. The default is 2 KB.
  - **Memory Allocated for Long URL** field—The memory allocated for the Long URL from 2 to 1024 KB. The number of Long URLs that can be used at any particular time depends on the size of the Long URL and the memory available.

3. Click **OK**.

Adding or Editing a URL Filtering Server

Follow these steps to add or edit a URL server:

1. In the **URL Filtering** panel, click one of the following buttons:

- **Add** if there are no entries in the table.
- **Insert Before** if you want to insert a URL server before an existing one.
- **Insert After** if you want to insert a URL server after an existing one.
- **Edit** if you want to edit an existing server.

The Add/Edit parameters for URL Filtering dialog box appears.

2. Set the following options:

- **Interface** drop-down list—The name of the network interface on which the URL server resides. The default is the **inside** interface.
- **IP Address** field—The IP address of the server that runs the URL filtering application.
- **Timeout** field—The timeout value, in seconds, before the firewall tries to access the next URL server. The default is **5 seconds**.
- **Protocol** area—The protocol version selected for the URL server.
  - For a Websense server:

        - **TCP 1** radio button—(Default) Uses TCP 1.
        - **TCP 4** radio button—Uses TCP 4. Version 4 provides functionality beyond Version 1. Specifically, when the firewall AAA filtering is enabled to perform user authentication, the username information is passed to the Websense server so that it can perform URL filtering and log URL activity by username.
        - **UDP 4** radio button—Uses UDP 4. If you use UDP, you cannot use the Long URL feature.
    - For an N2H2 server:
        - **TCP** radio button—(Default) Uses TCP.
        - **UDP** radio button—Uses UDP.

3. Click **Apply**.

Deleting a URL Filtering Server

Follow these steps to delete a URL server:

1. In the **URL Filtering** panel, select the server you want to delete from the **URL Filter Server** table.
2. Click **Delete**.
3. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Filter Rules

Configuration>Access Rules>Filter Rules

Access Rules shows your entire network security policy expressed in rules. This tab includes a panel for Filter Rules, as well as for Access Rules and AAA Rules. This topic describes Filter Rules.

When you click the **Filter Rules** option button, this tab lets you filter outbound traffic for HTTP, HTTPS, and FTP, as well as ActiveX and Java. ActiveX objects and Java applets are security risks for outbound connections because they can contain code intended to attack hosts and servers. You can disable ActiveX objects and remove Java applets with a filter rule. To remove URLs or FTP servers you deem inappropriate for use at your site, you can use the HTTP, HTTPS, and FTP filter rules in conjunction with a URL filtering server such as Websense or N2H2 (N2H2 only supports HTTP filtering).

Note: Identify the URL filtering servers you want to use on the System Properties>URL Filtering page.

Note: Review **Important Notes about Object Groups** regarding the naming of Service and Network Groups**.**

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- How Filter Rules are Organized
- Adding or Inserting a New Filter Rule
- Editing an Existing Filter Rule
- Copying and Pasting a Filter Rule
- Deleting a Filter Rule
- Applying Your Changes
- Resetting to Last Applied Settings
- Print

Important Notes

You cannot define any filter rules until you configure NAT for the hosts or networks on which you want to permit or deny traffic. See the Translation Rules tab.

Field Descriptions

This section includes the following tables:

- Button Descriptions
- Table Column Descriptions

The **Access Rules>Filter Rules** panel includes the following buttons:

Button	Description	
Show Detail/ Show Summary (toggle)	This button toggles between the following values:	
	Show Detail	Shows the hosts that are capable of communication with other hosts using protocols and services.
	Show Summary	Shows rules in a format similar to the CLI, which is similar to the information entered in the dialog boxes.
Apply	Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See **More** Configuration Changes.	
Reset	Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.	
Advanced	There are no advanced features for filter rules, and this button is disabled.	

The **Access Rules>Filter Rules** table displays the following columns:

Note: You can adjust the table column widths by moving your cursor over a column line until it turns into a double arrow. Click and drag the column line to the desired size.

Column	Description
#	A number indicating order of evaluation for the rule.
Action	The action that applies to the given rule type. Options are **filter ActiveX**, **do not filter ActiveX**, **filter Java applet**, **do not filter Java applet**, **filter HTTP (URL)**, **do not filter HTTP (URL)**, **filter HTTPS, do not filter HTTPS**, **filter FTP**, and **do not filter FTP**. See Access Rules>Filter Rules>Add, Edit, Insert or Paste Rule for more information.

Source Host/ Network	The IP addresses and names of hosts that have filtering operations performed when connecting to hosts listed in the **Destination Host/Network** column.
Destination Host/ Network	The IP addresses and names of hosts that have filtering operations performed when connecting to hosts listed in the **Source Host/Network** column.
Service	The service on which filtering will be performed, for example, http/tcp for an HTTP filter, or, if you changed the default filtering ports, (*port-port*)/tcp.
Options	Filtering options. See Access Rules>Filter Rules>Add, Edit, Insert or Paste Rule for information about the options available for each filter. For example, HTTP options include "Block when URL server is down," and "Truncate long URLs."

How Filter Rules are Organized

The firewall evaluates each filter rule in the order specified. Unlike ACLs, PDM does not create a set based on the source interface; instead, the filter rules reside in a global list, and the firewall evaluates all outbound traffic against the list.

Adding or Inserting a Filter Rule

Follow these steps to add a new rule:

1. If you have not defined any rules or want to add a rule to the end of the list, right-click anywhere in the table body, and choose **Add** from the drop-down menu.

   Alternatively, click the **Add** icon on the PDM toolbar; or from the **Rules** menu, choose **Add**.

   The Add Rule dialog box appears.

2. If you want to insert a rule above or below a rule, right-click the rule, and choose **Insert Before** or **Insert After** from the drop-down menu.

   Alternatively, select the rule and then click the **Insert Before** or **Insert After** icon on the PDM toolbar; or from the Rules menu, choose **Insert Before** or **Insert After**.

   The Insert Rule Before/After dialog box appears.

3. See the Editing a Filter Rule topic to complete adding the rule.

Editing an Existing Filter Rule

Follow these steps to edit an existing rule:

1. Double-click the rule.

   Alternatively, right-click the rule, and choose **Edit** from the drop-down list; or select the rule and then click the **Edit** icon on the PDM toolbar; or from the **Rules** menu, choose **Edit**.

   The Edit Rule dialog box appears.

2. See the Editing a Filter Rule topic to complete editing the rule.

Copying and Pasting a Filter Rule

Follow these steps to copy (or cut) and paste a rule:

1. Right-click the rule, and choose **Cut** or **Copy** from the drop-down menu.

   Alternatively, select the rule and then click the **Cut** or **Copy** icon on the toolbar; or from the **Rules** menu, choose **Cut** or **Copy**.

2. If you want to paste the rule at the end of the list, right-click anywhere in the table body, and choose Paste from the drop-down menu.

   Alternatively, click the **Paste** icon on the PDM toolbar; or from the **Rules** menu, choose **Paste**.

   The Paste Rule dialog box appears.

3. If you want to paste the rule above or below an existing rule, right-click the existing rule, and choose **Paste Before** or **Paste After** from the drop-down menu.

   Alternatively, select the rule and then click the **Paste Before** or **Paste After** icon on the PDM toolbar, or from the Rules menu, choose **Paste Before** or **Paste After**.

   The Paste Rule Before/After dialog box appears.

4. See the Editing a Filter Rule topic to complete adding the rule.

Deleting a Rule

The following step describes how to delete a rule permanently from PDM. To cut and paste a rule, see Copying and

Pasting a Filter Rule. Follow these steps to delete an existing rule:

- Right-click the rule you want to delete, and choose delete from the drop-down menu.

  Alternatively, select the rule and then click the **Delete** icon on the PDM toolbar; or from the **Rules** menu. choose **Delete**.

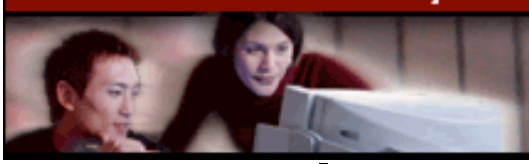
Applying Your Changes

To apply your changes, click the **Apply** button. If you click a different tab or selection before you apply your changes, you are prompted to apply or discard the changes.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.



Access Rules

Configuration>Access Rules>Access Rules

The **Access Rules** tab shows your entire network security policy expressed in rules. This tab includes a panel for Access Rules, as well as for AAA Rules and Filter Rules. This topic describes Access Rules.

When you click the **Access Rules** option button, this tab lets you define access control lists (ACLs) to control the access of a specific host or network to another host/network, including the protocol or port that can be used.

By default on the PIX Firewall, traffic from a higher security level (i.e. inside) can access a lower security level (i.e. outside): there is an implicit access list on the inside interface allowing all outbound IP traffic from the inside network. (The firewall denies traffic destined for the inside network from the outside network using the Adaptive Security Algorithm (ASA). ASA is a stateful approach to security. Every inbound packet is checked against the ASA and against connection state information in memory.) The implicit access list appears in PDM, but you cannot edit it. To limit outbound traffic, you can add an ACL (in which case, the implicit access list is removed).

By default on the FWSM, no traffic can pass through the firewall unless you add an ACL to allow it.

To allow traffic that is normally denied by the ASA, you can add an ACL; for example, you can allow public access to a web server on a DMZ network by adding an ACL to the outside interface.

The following sections are included in this Help topic:

- Prerequisites
- Important Notes
- Field Descriptions
- Organization of ACLs
- Null Rules
- Example Rule
- Adding or Inserting an Access Rule
- Editing an Existing Access Rule
- Copying and Pasting an Access Rule
- Deleting a Rule
- Applying Your Changes
- Resetting to Last Applied Settings
- Print

Prerequisites

1. Define each host or server in the **Hosts/Networks** tab.
2. If desired, create network groups in the **Hosts/Networks** tab.
3. Configure NAT in the **Translation Rules** tab.

Important Notes

- The firewall supports only an inbound ACL on an interface.
- At the end of each ACL, there is an implicit, unwritten rule that denies all traffic that is not permitted. If traffic is not explicitly permitted by an access control entry (ACE), it will be denied. ACEs are referred to as rules in this topic.

Field Descriptions

This section includes the following tables:

- Button Descriptions
- Table Column Descriptions

The **Access Rules>Access Rules** panel includes the following buttons:

Button	Description	
Show Detail/ Show Summary (toggle)	This button toggles between the following values:	
	Show Detail	Shows the hosts that are capable of communication with other hosts using protocols and services. This setting shows translated addresses in square brackets. See the **Destination Host/Network** column for more information. Example.
	Show Summary	Shows rules in a format similar to the CLI, which is similar to the information entered in the dialog boxes. IP addresses in summary mode are the untranslated addresses, even though the actual **access-list** command on the firewall includes the translated addresses where appropriate. Use the **Show Detail** button for translated addresses. Example.

Apply	Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See **More** Configuration Changes.
Reset	Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.
Advanced	This button allows you to set advanced log options for ACLs on which you enabled logging: the maximum number of deny flows and the alert interval (shown in the **Log Level Interval** table column). See **Advanced Access Rule Configuration** for more information.

The **Access Rules>Access Rules** table includes the following columns:

Note: You can adjust the table column widths by moving your cursor over a column line until it turns into a double arrow. Click and drag the column line to the desired size.

Column	Description
#	A number indicating order of evaluation for the rule. **Note**: Implicit rules are not numbered, but are represented by a hyphen.
Action	The action that applies to the rule, either **Permit** or **Deny**.
Source Host/ Network	The IP addresses that are permitted or denied to send traffic to the IP addresses listed in the **Destination Host/Network** column. In detail mode (see the **Show Detail** button), an address column might contain an interface name with the word **any**, such as **inside:any**. **any** means that any host on the inside interface is affected by the rule.
Destination Host/ Network	The IP addresses that are permitted or denied to send traffic to the IP addresses listed in the **Source Host/Network** column. In detail mode (see the **Show Detail** button), an address column might contain an interface name with the word **any**, such as **outside:any**. **any** means that any host on the outside interface is affected by the rule. Also in detail mode, an address column might contain IP addresses in square brackets, for example, [209.165.201.1-209.165.201.30]. These addresses are translated addresses. When an inside host makes a connection to an outside host, the firewall maps the inside host's address to an address from the pool. After a host creates an outbound connection, the firewall maintains this address mapping. This address mapping structure is called an xlate, and remains in memory for a period of time. During this time, outside hosts can initiate connections to the inside host using the translated address from the pool, if allowed by the ACL. Normally, outside-to-inside connections require a static translation so that the inside host always uses the same IP address.
Interface	Specifies the interface to which you apply the rule. An interface column may contain the following information:

	Interface	The rule is applied to inbound traffic on this interface (going into the firewall).
	Interface**(outbound)**	This text is shown for the implicit rule permitting outbound traffic from an inside interface.
	Interface**(inbound)**	(Conduit only) For example, "dmz(inbound)," which means the rule is applied to traffic that the firewall receives from interface "dmz" and is destined to a higher security interface. For example, traffic from "dmz" to "inside."
	(inbound)	(Conduit only) No interface name is listed, which means the rule is applied to traffic the firewall receives from multiple interfaces, as long as the traffic direction is from a lower security interface to a higher security interface. For example, this rule may be applied for traffic from outside to inside, and from dmz to inside.
Service	The service and protocol specified by the rule.	
Log Level Interval	If you enable logging for the ACL, this column shows the logging level and the interval in seconds between log messages. To set logging options, including enabling or disabling logging, right-click this column, and choose **Edit Log Option**. The **Log Options** screen appears.	
Description	The description you typed when you added the rule. An implicit rule includes the following description: "Implicit outbound rule." To edit the description, right-click this column, and choose **Edit Description**.	

▲

▲

Organization of ACLs

ACL rules are grouped by the interface on which they are applied. You can only apply one ACL to an interface, but an ACL can be made up of many rules. In all ACLs, there is an implicit rule at the end denying all other traffic.

In the following table, there are two ACLs, one for each interface:

#	Action	Source Host/ Network	Destination Host/Network	Interface	Service	Log Level Interval	Description
1	✓	any	any	inside	ftp/tcp	informational 300	
2	✗	any	any	inside	http/tcp	informational 300	

1	✓	any	any	dmz	http/tcp	informational 300	
2	✓	any	any	dmz	dns/udp	informational 300	
3	✗	any	any	dmz	ftp/tcp	informational 300	

In this table, the first two rules are in an ACL applied to the inside interface.

The third, fourth, and fifth rules are in an ACL that is applied to the interface named dmz. The numbering starts over because these rules are part of a new ACL and are evaluated by the firewall separately from the ACL that is applied to the inside interface.

▲

▲

Null Rules

A null rule indicates that an access rule was configured for a host that is not visible on another interface. This rule is null because no traffic can flow between these two hosts even though the access rule would permit it. For example:

#	Action	Source Host/ Network	Destination Host/Network	Interface	Service	Log Level Interval	Description
1	✓	(Null Rule)	(Null Rule)	[inbound]	tcp	alerts 300	

This situation can happen when PDM reads an existing configuration with one of the following characteristics:

- Inbound rules without a static translation.
- Outbound rules without NAT.
- No hosts or networks defined for either source or destination.

Perform one of the following tasks to make the host visible:

- Make sure the host is defined in PDM (see **Hosts/Networks>Add**).
- Add a NAT rule making the hosts visible on the appropriate interfaces to allow traffic to pass between the two hosts (see **Translation Rules**).

Alternatively, you can delete the rule. If you leave the rule in the configuration, there is no real harm except processing overhead.

Example Rule

The following ACL permits ICMP echo-reply messages into the inside interface. You must allow all other traffic with the last rule. This ACL permits hosts on the inside to ping hosts on other remote networks. The following example is the summary view of this rule.

#	Action	Source Host/ Network	Destination Host/Network	Interface	Service	Log Level Interval	Description
1	✔	any	any	inside	echo-reply/ icmp	alerts 300	
2	✔	any	any	inside	ip	alerts 300	

The following example shows the detailed view of the same ACL. It shows the source and destination interface names and IP addresses.

#	Action	Source Host/ Network	Destination Host/Network	Interface	Service	Log Level Interval	Description
1	✔	inside:any	[209.165.200.224]	inside	echo-reply/ icmp	alerts 300	
2	✔	inside:any	[209.165.200.224]	inside	ip	alerts 300	

Adding or Inserting an Access Rule

Follow these steps to add a new rule:

1. If you have not defined any rules or want to add a rule to the end of an access list, right-click anywhere in the table body, and choose **Add** from the drop-down menu.

   Alternatively, click the **Add** icon on the PDM toolbar; or from the **Rules** menu, choose **Add**.

The Add Rule dialog box appears.

2. If you want to insert a rule above or below a rule, right-click the rule, and choose **Insert Before** or **Insert After** from the drop-down menu.

   Alternatively, select the rule and then click the **Insert Before** or **Insert After** icon on the PDM toolbar; or from the Rules menu, choose **Insert Before** or **Insert After**.

   The Insert Rule Before/After dialog box appears.

   Note: You must apply the rule to the same interface as the rule you are inserting before or after. If you choose another interface in the Add dialog box, you receive an error message and cannot add the rule.

   Note: If you insert before or after an outbound rule, PDM may put the rule into a location you may not expect. This is because PDM sorts outbound rules into the order that firewall will apply them to traffic.
3. See the Editing an Access Rule topic to complete adding the rule.

▲

Editing an Existing Access Rule

Follow these steps to edit an existing rule:

1. Double-click the rule.

   Alternatively, right-click the rule, and choose **Edit** from the drop-down list; or select the rule and then click the **Edit** icon on the PDM toolbar; or from the **Rules** menu, choose **Edit**.

   The Edit Rule dialog box appears.

2. See the Editing a Rule topic to complete editing the rule.

▲

Copying and Pasting an Access Rule

Follow these steps to copy (or cut) and paste a rule:

1. Right-click the rule, and choose **Cut** or **Copy** from the drop-down menu.

   Alternatively, select the rule and then click the **Cut** or **Copy** icon on the toolbar; or from the **Rules** menu, choose **Cut** or **Copy**.

2. If you want to paste the rule at the end of the list, right-click anywhere in the table body, and choose Paste from the drop-down menu.

Alternatively, click the **Paste** icon on the PDM toolbar; or from the **Rules** menu, choose **Paste**.

The Paste Rule dialog box appears.

3. If you want to paste the rule above or below an existing rule, right-click the existing rule, and choose **Paste Before** or **Paste After** from the drop-down menu.

   Alternatively, select the rule and then click the **Paste Before** or **Paste After** icon on the PDM toolbar, or from the Rules menu, choose **Paste Before** or **Paste After**.

   The Paste Rule Before/After dialog box appears.

   Note: You must apply the rule to the same interface as the rule you are pasting before or after. If you choose another interface in the Paste dialog box, you receive an error message and cannot add the rule.

   Note: If you paste before or after an outbound rule, PDM may put the rule into a location you may not expect. This is because PDM sorts outbound rules into the order that firewall will apply them to traffic.

4. See the Editing a Rule topic to complete adding the rule.

Deleting a AAA Rule

The following step describes how to delete a rule permanently from PDM. To cut and paste a rule, see Copying and Pasting an Access Rule. Follow these steps to delete an existing rule:

- Right-click the rule you want to delete, and choose delete from the drop-down menu.

  Alternatively, select the rule and then click the **Delete** icon on the PDM toolbar; or from the **Rules** menu. choose **Delete**.

Applying Your Changes

To apply your changes, click the **Apply** button. If you click a different tab or selection before you apply your changes, you are prompted to apply or discard the changes.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

AAA Rules

Configuration>Access Rules>AAA Rules

Access Rules shows your network security policy expressed in rules. This tab includes a panel for AAA Rules, as well as for Access Rules and Filter Rules. This topic describes AAA Rules.

When you click the **AAA Rules** option button, you can define authentication, authorization, or accounting (AAA) rules. AAA is used to tell the firewall who the user is, what the user can do, and what the user did. You can use authentication alone, or with authorization. Authorization always requires authentication. For example, if you authenticate outside users who access any server on the inside network, then authentication alone is adequate. However, if you want to limit the inside servers that a particular user accesses, you can configure an authorization server to specify which servers and services are allowed.

AAA provides an extra level of protection and control for user access than using ACLs alone. For example, you can create an ACL allowing all outside users to access a server on the DMZ network. But if you only want registered users to Telnet to the server, you can enable AAA to allow only authenticated and/or authorized users to make it past the firewall. If the server also has its own authentication and authorization, the user enters a second set of user name and password (in the case of FTP, the user must enter both usernames and passwords separated by an at sign (@)).

The firewall uses a special feature called "cut-through proxy" that significantly speeds up performance compared to a traditional proxy server. The performance of a traditional proxy server suffers because it analyzes every packet at the application layer of the Open System Interconnection (OSI) model. The PIX Firewall and FWSM cut-through proxy, on the other hand, challenges a user initially at the application layer, then authenticates against standard RADIUS, TACACS+, or local databases. After the firewall checks the policy, the firewall shifts the session flow, and all traffic flows directly and quickly between the two parties while maintaining session state information.

Each AAA rule identifies the following characteristics for matching traffic:

- The source and destination network
- The action (authentication, authorization, or accounting; a rule can also exempt a MAC address from AAA)
- The AAA server group (RADIUS, TACACS+, or the local database)
- The service type (for example, Telnet or FTP)

The following sections are included in this Help topic:

- Prerequisites
- Important Notes
- Field Descriptions

- How AAA Rules are Organized
- Adding a New AAA Rule
- Editing a AAA Rule
- Pasting AAA Rules
- Deleting a AAA Rule
- Applying Your Changes
- Resetting to Last Applied Settings

Prerequisites

1. Define each host or server in the **Hosts/Networks** tab.
2. If desired, create network groups in the **Hosts/Networks** tab.
3. Configure NAT using the **Translation Rules** tab. If outside users need to access inside servers, be sure to set up a static translation.
4. Add users to the local database (see **System Properties>Administration>User Accounts**) or add AAA server(s) to server groups (**System Properties>AAA>AAA Server Groups** and **AAA Servers**).
5. Be sure that users can access the specified network (by an ACL if required).

Important Notes

- PDM does not support a mixed configuration of AAA rules that:

  - Specify the source and destination addresses
  - Match ACLs for the source and destination addresses

  If your configuration already contains AAA rules, then you can only add AAA rules of the same kind. If you have not configured any AAA rules, then PDM only allows you to add rules that match ACLs. To convert your rules to match ACLs, you must delete all of your AAA rules in PDM, then re-add them (with no rules configured, PDM defaults to ACL mode). In PDM, the configuration of AAA rules is the same in both modes.
- For FTP authentication, the user must enter the name and password in the following format:

  firewall_name@ftp_name
  firewall_password@ftp_password

  The firewall forwards the FTP name and password to the FTP server after successful authentication on the firewall. Other services such as Telnet and HTTP (if configured for authentication) require you to enter a second name and password at the destination server prompt.

- Some services are not reliably authenticated, such as mail or SMTP. If you specify that *all* services need to be authenticated, then the user must first authenticate with Telnet, FTP, HTTP, or HTTPS (or another service that reliably provides an authentication prompt), and then use the other services.

- AAA authorization rules support TACACS+ servers, but not RADIUS servers or the local database. However, you can use the local database to authorize users for firewall commands. See the **System Properties>Administration>Authentication/Authorization** screen to create this kind of rule.

- AAA accounting rules are not supported using the local database as the **AAA Server Group**.

Field Descriptions

This section includes the following tables:

- Button Descriptions
- Table Column Descriptions

The **Access Rules>AAA Rules** panel includes the following buttons:

Button	Description	
Show Detail/ Show Summary (toggle)	This button toggles between the following values:	
	Show Detail	Shows the hosts to which the AAA rule applies. This setting shows translated addresses in square brackets. See the **Destination Host/Network** column for more information.
	Show Summary	Shows rules in a format similar to the CLI, which is similar to the information entered in the dialog boxes. IP addresses in summary mode are the untranslated addresses, even though the actual **aaa** command on the firewall includes the translated addresses where appropriate. Use the **Show Detail** button for translated addresses.
Apply	Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See More Configuration Changes.	
Reset	Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.	
Advanced	Lets you enable Secure HTTP and Proxy Limit features. See **Advanced AAA Configuration** for more information.	

The **Access Rules>AAA Rules** table includes the following columns:

Note: You can adjust the table column widths by moving your cursor over a column line until it turns into a double arrow. Click and drag the column line to the desired size.

Column	Description
#	A number indicating order of evaluation for the rule. See **How AAA Rules are Organized** for more information.
Action	The type of AAA rule: • **authenticate** • **do not authenticate** • **authorize** • **do not authorize** • **account** • **do not account** • **exempt MAC** • **do not exempt MAC**
Source Host/ Network	The IP addresses that are subject to AAA when traffic is sent to the IP addresses listed in the **Destination Host/Network** column. In detail mode (see the **Show Detail** button), an address column might contain an interface name with the word **any**, such as **inside:any**. **any** means that any host on the inside interface is affected by the rule.
Destination Host/ Network	The IP addresses that are subject to AAA when traffic is sent from the IP addresses listed in the **Source Host/Network** column. In detail mode (see the **Show Detail** button), an address column might contain an interface name with the word **any**, such as **outside:any**. **any** means that any host on the outside interface is affected by the rule. Also in detail mode, an address column might contain IP addresses in square brackets, for example, [209.165.201.1-209.165.201.30]. These addresses are translated addresses. When an inside host makes a connection to an outside host, the firewall maps the inside host's address to an address from the pool. After a host creates an outbound connection, the firewall maintains this address mapping. This address mapping structure is called an xlate, and remains in memory for a period of time.
Interface	Specifies the interface on which a AAA rule is configured and enforced. This column always contains the name of an interface on your firewall, such as "inside," which means this AAA rule is applied to traffic the firewall receives from the inside interface.
Service	The service and protocol specified by the rule.
Server Group	Specifies the AAA Server Group tag. Options are TACACS+, RADIUS, LOCAL, or a predefined AAA Server Group defined in **System Properties>AAA>AAA Server Groups**. To create new AAA rules, a server group must exist and have one or more servers in it. You can define servers in **System Properties>AAA>AAA Servers** and assign them to the appropriate server group. Note that AAA accounting rules are not supported using the local database as the **AAA Server Group**.
Description	The description you typed when you added the rule. To edit the description, right-click this column, and choose **Edit Description**.

How AAA Rules are Organized

AAA Rules are ordered by the interface on which they are configured and enforced. Within each group, rules are shown by type, with authentication rules first, authorization rules second, and accounting rules third. AAA rules are further ordered by server group if you are using multiple server groups to implement your AAA policies.

The firewall evaluates rules of each type and interface in order.

#	Action	Source Host/ Network	Destination Host/Network	Interface	Service	Server Group
1	Authenticate	any	any	inside	http/tcp	portal
2	Authenticate	any	any	inside	telnet/tcp	portal
3	Authenticate	any	any	inside	ftp/tcp	portal
1	Authenticate	any	any	inside	http/tcp	TACACS+
2	Authenticate	any	any	inside	telnet/tcp	TACACS+
1	Authorize	any	any	inside	http/tcp	portal
2	Authorize	any	any	inside	telnet/tcp	portal
1	Account	any	any	inside	http/tcp	portal
1	Account	any	any	inside	http/tcp	TACACS+

The first three rules are authentication rules using the authentication server group named **portal**. The fourth and fifth are authentication rules using **TACACS+** as the authentication server group. The sixth and seventh rules are authorization rules, and the last two are accounting rules.

Note: If you **Insert/Paste Before** or **Insert/Paste After** a rule, you can only create a rule of the same type as the selected rule.

Adding or Inserting a AAA Rule

Follow these steps to add a new rule:

1. If you have not defined any rules or want to add a rule to the end of an access list, right-click anywhere in the table body, and choose **Add** from the drop-down menu.

   Alternatively, click the **Add** icon on the PDM toolbar; or from the **Rules** menu, choose **Add**.

   The Add Rule dialog box appears.

2. If you want to insert a rule above or below a rule, right-click the rule, and choose **Insert Before** or **Insert After** from the drop-down menu.

   Alternatively, select the rule and then click the **Insert Before** or **Insert After** icon on the PDM toolbar; or from the Rules menu, choose **Insert Before** or **Insert After**.

   The Insert Rule Before/After dialog box appears.

   Note: You can only create a rule of the same type as the selected rule.
3. See the Editing a AAA Rule topic to complete adding the rule.

Editing an Existing AAA Rule

Follow these steps to edit an existing rule:

1. Double-click the rule.

   Alternatively, right-click the rule, and choose **Edit** from the drop-down list; or select the rule and then click the **Edit** icon on the PDM toolbar; or from the **Rules** menu, choose **Edit**.

   The Edit Rule dialog box appears.

2. See the Editing a Rule topic to complete editing the rule.

Copying and Pasting a AAA Rule

Follow these steps to copy (or cut) and paste a rule:

1. Right-click the rule, and choose **Cut** or **Copy** from the drop-down menu.

   Alternatively, select the rule and then click the **Cut** or **Copy** icon on the toolbar; or from the **Rules** menu,

choose **Cut** or **Copy**.

2. If you want to paste the rule at the end of the list, right-click anywhere in the table body, and choose Paste from the drop-down menu.

   Alternatively, click the **Paste** icon on the PDM toolbar; or from the **Rules** menu, choose **Paste**.

   The Paste Rule dialog box appears.

3. If you want to paste the rule above or below an existing rule, right-click the existing rule, and choose **Paste Before** or **Paste After** from the drop-down menu.

   Alternatively, select the rule and then click the **Paste Before** or **Paste After** icon on the PDM toolbar, or from the Rules menu, choose **Paste Before** or **Paste After**.

   The Paste Rule Before/After dialog box appears.

   Note: You can only create a rule of the same type as the selected rule.

4. See the Editing a Rule topic to complete adding the rule.

Deleting a AAA Rule

The following step describes how to delete a rule permanently from PDM. To cut and paste a rule, see Copying and Pasting a AAA Rule. Follow these steps to delete an existing rule:

- Right-click the rule you want to delete, and choose delete from the drop-down menu.

  Alternatively, select the rule and then click the **Delete** icon on the PDM toolbar; or from the **Rules** menu. choose **Delete**.

Applying Your Changes

To apply your changes, click the **Apply** button. If you click a different tab or selection before you apply your changes, you are prompted to apply or discard the changes.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time

Refresh was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Translation Rules

Configuration>Translation Rules

The **Translation Rules** tab lets you view all the address translation rules or Network Address Translation (NAT) exemption rules applied to your network.

The Firewall supports both the Network Address Translation (NAT) feature, which provides a globally unique address for each outbound host session, and the Port Address Translation (PAT) feature, which provides a single, unique global address for up to 64,000 simultaneous outbound or inbound host sessions. The global addresses used for NAT come from a pool of addresses to be used specifically for address translation. The unique global address that is used for PAT can either be one global address or the IP address of a given interface.

The Firewall can perform NAT or PAT in both inbound and outbound connections. This ability to translate inbound addresses is called **Outside NAT**, because addresses on the outside, or less secure interface are translated to an inside, usable IP address. Outside NAT gives you the option to translate an outside host or network to an inside host or network, and it is sometimes referred to as bi-directional NAT. Just as when you translate outbound traffic with NAT, you may choose dynamic NAT, static NAT, dynamic PAT and static PAT. If necessary, you may use outside NAT together with inside NAT to translate the both source and destination IP addresses of a packet.

From the Translation Rules tab you can also create a **Translation Exemption Rule**, which lets you specify traffic that is exempt from being translated or encrypted. The Exemption Rules are grouped by interface in the table, and then by direction. If you have a group of IP addresses that will be translated, you can exempt certain addresses from being translated using the Exemption Rules. If you have an previously configured an access-list, you can use that to define your exemption rule. PDM will write to the Command Line Interface (CLI) a **nat 0** command. You can resort the view of your exemption by clicking on the column heading. See Configuration>Translation Rules>Translation Exemption Rule.

Related Topics: More Static NAT , More Dynamic NAT, Troubleshooting NAT.

The following sections are included in this Help topic:

- How to Use Translation Rules
- How PDM Handles Redundant or Overlapping Translation Rules
- Important Notes
- Field Descriptions
  - Manage Pools
  - Translation Rules

    - Translation Exemption Rules
- Printing

How to Use Translation Rules

Using Translation Rules

- Adding a New Translation Rule
- Editing a New Translation Rule
- Move using Cut and Paste Commands
- Adding Translation Rules Using Copy and Paste Commands
- Deleting Translation Rules Using Copy and Paste Commands
- Resetting to Last Applied Settings

Using Exemption Rules

- Adding a New Exemption Rule
- Editing a New Exemption Rule
- Move using Cut and Paste Commands
- Adding Exemption Rules Using Copy and Paste Commands
- Deleting Translation Rules Using Copy and Paste Commands
- Resetting to Last Applied Settings

Examples

- Dynamic
- Static NAT
- Static PAT
- Overlapping Translation Rules

Important Notes

- Before you can designate access and translation rules for your network, you must first define each host or server for which a rule will apply. To do this, click the **Hosts/Networks** tab to define hosts and networks.

Caution: Review **Important Notes about Object Groups** regarding the naming of Network and Service Groups**.**

- When you are working in either the **Access Rules** or the **Translation Rules** tabs, you can access the task menu three ways: From the PDM toolbar, the **Rules** menu, or by right-clicking anywhere in the Rules table.

  You cannot use unavailable translation commands until you define networks or hosts. Unavailable commands appear dimmed on the menu.

- It is important to note that the order in which you apply translation rules can affect the way the rules operate. PDM will list the static translations first and then the dynamic translations. When processing NAT the firewall will first translate the static translations in the order they are configured. You can use the Insert Before or Insert After command on the **Rules** menu to determine the order in which static translations are processed. Because dynamically translated rules are processed on a best match basis, the option to insert a rule before or after a dynamic translation is disabled.
- It is necessary to run NAT even if you have routable IP addresses on your secure networks. This is a unique

feature of PIX Firewall. You can do this by translating the IP address to itself on the outside. See Example Static Rule.

- A packet sourced on the more secure (inside) interface destined for an intermediate (DMZ) interface, could not have the same translated address when it is outbound on a less secure (outside) interface. However, if one dynamic rule is deleted on either of the outbound interfaces, all outbound dynamic rules for translations originating on the same interface will be deleted.
- It is possible to create an Exemption Rule for traffic that is not to be encrypted and sent out to the Internet or a less secure interface. This makes it possible to allow certain traffic between hosts or networks to remain unencrypted. This can be useful in a scenario where you want to encrypt some traffic to another remote VPN network, but would like traffic destined to anywhere else to be unencrypted.

Field Descriptions

Translation Rules and **Translation Exemption Rules**—Lets you select which type of rules will be displayed in the **Rules** table. Click the **Select Translation Rules** option to display traffic that will be translated, and the **Translation Exemption Rules** option to display traffic that will be exempted from translation or encryption.

Manage Pools

Manage Pools—Lets you manage the Global address NAT pools, which are used for dynamic NAT configuration. These are the IP addresses the firewall will present to the outside or less secure interface for which they are configured. See Managing Pools for more information.

Translation Rules

When **Translation Rules** is selected, the **Translation Rules** tab displays the following fields:

- **Manage Pools**—Lets you manage the Global address NAT pools, which are used for dynamic NAT configuration. These are the IP addresses the firewall will present to the outside or less secure interface for which they are configured. See Managing Pools for more information.
- **Rules Table**
  - **Rule Type**—Displays the translation rule type applied to the given row, which can either be **dynamic** or **static**.
    - **Dynamic**—Internal IP addresses are dynamically translated using IP addresses from a pool of global addresses or, in the case of PAT, a single address. These rules translate addresses of hosts on a higher security level interface to addresses selected from a pool of addresses for traffic sent to a lower security level interface. Dynamic translations are often used to map local, RFC 1918 IP addresses to addresses that are Internet-routable addresses. They are represented with the dynamic icon .
    - **Static**—Internal IP addresses are permanently mapped to a global IP address. These rules map a host address on a lower security level interface to a global address on a higher security level interface. For example, a static rule would be used for mapping the local address of a web server on a perimeter network to a global address that hosts on the outside interface would use to access the web server. They are represented with the static icon .

- **Original**—Displays the original address with its associated interface before network translation is applied.
  - **Interface**—The interface on which the original addresses reside.
  - **Address**—The original addresses to be translated.
- **Translated**—Displays the translated addresses with its associated interface after network translation is applied.
  - **Interface**—The interface on which the translated addresses reside.
  - **Address**—The translated addresses.

Translation Exemption Rules

When **Translation Exemption Rules** is selected, the **Translation Rules** tab displays the following fields:

- **Manage Pools**—Lets you manage the Global address NAT pools, which are used for dynamic NAT configuration. These are the IP addresses the firewall will present to the outside or less secure interface for which they are configured. See Managing Pools for more information.
- **Rules Table**
  - #—Displays the number of a rule within a group.
  - **Action**—Displays whether a rule is Exempt or Not Exempt from NAT.
  - **Interface**—Displays the interface on which the rule is applied, and in parentheses, the direction the rule is applied.
  - **Host/Network Exempted From NAT**—Displays the source addresses of the host or network associated interface that is exempt from being translated or encrypted. See Configuration>Translation Rules>Translation Exemption Rule.
  - **When Connecting to Host/Network**—Displays the destination addresses of the host or network with its associated interface after network translation is applied.
  - **Description**—If a description of the rule is available, it is displayed in this column.
  - **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
  - **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Note: To create or modify a translation rule, you must first click the **Translation Rules** option above the **Rules** table.

▲

Using Translation Rules

Adding a New Translation Rule

Follow these steps to add a new address translation rule:

1. On the PDM toolbar, click **Translation Rules**, and click **Add a new rule**.

2. In the **Add Address Translation Rule** dialog box, configure the translation rule and click **OK** to return to the **Translation Rules** tab.
3. Click **Apply**.

Editing a New Translation Rule

Follow these steps to edit an existing address translation rule:

1. On the **Translation Rules** tab, select the rule you want to edit.
2. Click **Rules>Edit** on the PDM toolbar. The **Edit Address Translation Rule** dialog box appears. You can also double-click the rule to edit it.
3. In the **Edit Address Translation Rule** dialog box, edit the translation rule and click **OK** to return to the **Translation Rules** table.
4. Click **Apply**.

It is not possible to change the type of rule (static or dynamic) in the **Edit Address Translation Rule** dialog box. To change a static rule to a dynamic rule or a dynamic rule to a static rule, cut the rule and paste it back into the **Translation Rules** table, and then change the rule type.

Moving Translation Rules Using Cut and Paste Commands

Follow these steps to move an address translation rule using cut and paste:

1. On on the **Translation Rules** tab, select the rule to move.
2. Click **Cut Rule** on the toolbar. The translation rule is cut from the tab.
3. Select the translation rule you want the cut rule to be positioned immediately before.
4. On the **Rules** menu, click **Paste**. Note that if this is a static rule you can click **Paste Before** or **Paste After**. The **Paste Address Translation Rule** dialog box appears.
5. In the **Paste Address Translation Rule** dialog box, modify the translation rule if needed, and click **OK** to return to the **Translation Rules** tab.
6. Click **Apply**.

Adding Translation Rules Using the Copy and Paste Commands

Follow these steps to modify an address translation rule using the **Copy** and **Paste** commands.

1. On the **Translation Rules** tab, select the rule you want to copy.
2. Click **Copy Rule** on the PDM toolbar. The rule is copied from the tab.
3. Select the rule that you want the cut rule to be positioned immediately before.
4. On the **Rules** menu, click **Paste**. Note that if this is a static rule you can click **Paste Before** of **Paste After**. The **Paste Address Translation Rule** dialog box appears.
5. In the **Paste Address Translation Rule** dialog box, modify the translation rule if needed, and click **OK** to return to the **Translation Rules** tab.
6. Click **Apply**.

Inserting Translation Rules

Follow these steps to insert a translation rule before or after a static translation. See the Important Notes section that explains why these rules can only be inserted before or after static rules.

1. Select a static rule from the **Rules** table.
2. On the **Rules** menu, click **Insert Before** or **Insert After**.
3. Create the rule that you would like to insert.
4. Click **Apply**.

Deleting Translation Rules

Follow these steps to delete an address translation rule:

1. On the **Translation Rules** tab, select the rule you want to delete.
2. Click **Delete**.
3. Click **Apply**.

Note: To create or modify an exemption rule, you must first click the **Translation Exemption Rules** option.

▲

Using Translation Exemption Rules

Adding a New Exemption Rule

Follow these steps to add a new address translation exemption rule:

1. On the PDM toolbar, click the **Translation Exemption Rules** option and click **Add a new rule**.
2. In the **Add Address Exemption Rule** dialog box, configure the exemption rule and click **OK** to return to the **Translation Exemption Rules** tab.
3. Click **Apply**.

Editing a New Exemption Rule

Follow these steps to edit an existing address translation rule:

1. On the **Translation Exemption Rules** tab, select the rule you want to edit.
2. Click **Rules>Edit** on the PDM toolbar. The **Edit Address Exemption Rule** dialog box appears. You can also double-click the rule to edit it.
3. In the **Edit Address Exemption Rule** dialog box, edit the translation rule and click **OK** to return to the **Translation Exemption Rules**.
4. Click **Apply**.

Moving Exemption Rules Using Cut and Paste Commands

Follow these steps to move an address translation rule using cut and paste:

1. On on the **Translation Exemption Rules** tab, select the rule to move.
2. Click **Cut Rule** on the toolbar. The exemption rule is cut from the tab.
3. Select the Exemption rule you want the cut rule to be immediately before.
4. On the **Rules** menu, click **Paste**. Note that if this is a static rule you can click **Paste Before** or **Paste After**. The **Paste Address Exemption Rule** dialog box appears.
5. In the **Paste Address Exemption Rule** dialog box, modify the exemption rule if needed, and click **OK** to return to the **Exemption Rules** tab.
6. Click **Apply**.

Adding Exemption Rules Using the Copy and Paste Commands

Follow these steps to modify an address translation rule using the **Copy** and **Paste** commands.

1. In the **Exemption Rules** tab, select the rule you want to move.
2. Click **Copy Rule**. The rule is copied from the tab.
3. Select the rule that you want the cut rule to be immediately before.
4. On the **Rules** menu, click **Paste**. Note that if this is a static rule you can click **Paste Before** of **Paste After**. The **Paste Address Exemption Rule** dialog box appears.
5. In the **Paste Address Exemption Rule** dialog box, modify the exemption rule if needed, and click **OK** to return to the **Translation Exemption Rules** tab.
6. Click **Apply**.

Inserting Exemption Rules

1. On the **Rules** menu, click **Insert Before** or **Insert After**.
2. Create the rule that you would like to insert.
3. Click **Apply**.

Deleting Exemption Rules

Follow these steps to delete an exemption rule:

1. In the **Translation Exemption Rules** tab, select the rule you want to delete.
2. Click **Delete**.
3. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Examples

Example of a Dynamic Rule

In this example translation rule, the outside interface has an address of 209.165.200.225. Before you begin, you must configure your address pool for PAT in the **Manage Global Address Pools** dialog box. For an example of how to configure this rule, see Translation Rules properties.

The completed translation rule would appear on the **Translation Rules** tab as follows:

Rule	Original		Translated	
Type	Interface	Address	Interface	Address
	inside	inside:any / 0.0.0.0	outside	209.165.200.225(interface PAT)

The **Rule Type** column lists whether the rule type is Static or Dynamic. A dynamic translation shows the dynamic icon.

The **Original** column lists where the translation originates, including what interface and IP addresses are translated.

The **Translated** column lists the interface where the translation occurs, and what IP addresses are presented to connections on that interface. In this example, all outbound connections are presented as 209.165.200.225, using PAT.

Example of a Static NAT Rule

In this example of a Static translation, the address on the inside interface is routable on the Internet, but because the firewall requires an entry for NAT, it is translated as itself.

Rule	Original		Translated	
Type	Interface	Address	Interface	Address
	inside	209.165.201.1	outside	209.165.201.1
	inside	Company_LAN 209.165.201.0 / 255.255.255.0	outside	209.165.201.0 / 255.255.255.0

The **Rule Type** column lists whether the rule type is Static or Dynamic. A static translation shows the static icon.

The **Original** column lists where the translation originates, including what interface and IP addresses are translated.

The **Translated** column lists the interface where the translation occurs, and what IP addresses are presented to connections on that interface.

In the first row, the static address 209.165.201.1 is presented to connections on the outside interface as 209.165.201.1.

The second row shows an entire subnet called "Company_LAN." These connections are presented on the outside interface as their own IP addresses—in this case the 209.165.201.0 subnet.

Example of a Static PAT Rule

The NAT table displays all static PAT rules first, followed by the normal static NAT rules, and then the dynamic NAT rules. No new column is introduced in the table. The contents of "Original Address" and "Translated Address" columns are extended to show service mapping for static PAT rules.

Rule	Original		Translated	
Type	Interface	Address	Interface	Address
	inside	209.165.201.1 Port 8000/tcp	outside	Interface IP Port 80/tcp

The **Rule Type** column lists whether the rule type is Static or Dynamic. A static translation shows the static icon.

The **Original** column lists where the translation originates, including what interface, IP addresses, port number/ protocol are translated.

The **Translated** column lists the interface where the translation occurs, and what IP addresses, Port number/ protocol are presented to connections on that interface.

How PDM Handles Redundant or Overlapping Translation Rules

Definition of terms:

Redundant: If there exist two or more NAT rules in a configuration to translate an IP address, and the resulted translations are identical, the rules are called "redundant" to each other, for example:

1. static (in,out) 1.1.1.0 1.1.1.0
2. static (in,out) 1.1.1.1 1.1.1.1

For address 1.1.1.1, both rules will translate it to 1.1.1.1. However, translation may not be exactly identical, for example:

1. static (in,out) 1.1.1.0 1.1.1.0 0 0

2. static (in,out) 1.1.1.1 1.1.1.1 100 100 norandomseq

Overlap: If there exists two or more NAT rules in a configuration to translate an address and the resulted translations are different, the rules are overlapping each other, for example:

1. static (in,out) 1.1.1.0 1.1.1.0
2. static (in,out) 1.1.1.5 1.1.1.1

PDM builds NAT rules in two cases: when PDM reads your current configuration and when you use PDM to add/ edit a NAT rule. PDM checks for NAT overlapping/redundancy only in the second case. If you use the CLI to configure NAT, it is up to you to avoid overlapping/redundancy.

The following is a list of possible NAT overlapping/redundancy scenarios that will help you understand how PDM behaves and why it does it this way. As you will see, some cases are not so obvious. One needs to understand how PIX Firewall translates packets using the NAT configuration and the runtime xlate database to see why a particular combination will fail at runtime, and thus should be prevented or warned when being configured.

I. Between same pair of local/global interfaces.

A. Static NAT

A-1 overlap between siblings

static (inside,outside) 1.1.1.1 1.1.1.1 netmask 255.255.255.255
static (inside,outside) 1.1.1.1 1.1.1.2 netmask 255.255.255.255

PIX: reject
PDM: reject

A-2 redundant/overlap between child and parent

A-2-1 redundant, child first

static (inside,outside) 1.1.1.1 1.1.1.1 netmask 255.255.255.255
static (inside,outside) 1.1.1.0 1.1.1.0 netmask 255.255.255.0

PIX: warn
PDM: warn

A-2-2 redundant, parent first

static (inside,outside) 1.1.1.0 1.1.1.0 netmask 255.255.255.0
static (inside,outside) 1.1.1.1 1.1.1.1 netmask 255.255.255.255

PIX: warn
PDM: warn

A-2-3 overlap, child first

static (inside,outside) 2.2.3.3 1.1.1.1 netmask 255.255.255.255
or
static (inside,outside) 3.3.1.1 1.1.1.1 netmask 255.255.255.255

static (inside,outside) 2.2.0.0 1.1.0.0 netmask 255.255.0.0

PIX: warn
PDM: warn

A-2-4 overlap, parent first

static (inside,outside) 2.2.0.0 1.1.0.0 netmask 255.255.0.0

static (inside,outside) 2.2.3.3 1.1.1.1 netmask 255.255.255.255
or
static (inside,outside) 3.3.1.1 1.1.1.1 netmask 255.255.255.255

PIX: warn
PDM: warn

A-3 overlap between unrelated hosts/networks

static (inside,outside) 3.3.1.1 1.1.1.1 netmask 255.255.255.255 0 0
static (inside,outside) 3.3.0.0 2.2.0.0 netmask 255.255.0.0 0 0

PIX: accept
PDM: warn

A-4 overlap with interface address

ip address outside 192.168.1.1 255.255.255.0
static (inside,outside) 192.168.1.0 1.1.1.0 netmask 255.255.255.0

PIX: accept
PDM: accept

A-5 overlap with global pool

global (outside) 1 192.168.1.1-192.168.1.10
static (inside,outside) 192.168.1.2 1.1.1.2 netmask 255.255.255.255

PIX: accept
PDM: accept

B. Static PAT

B-1 PAT overlap between siblings

static (inside,outside) tcp 1.1.1.1 80 1.1.1.1 8080 netmask 255.255.255.255
static (inside,outside) tcp 1.1.1.1 80 2.2.2.1 80 netmask 255.255.255.255

or

static (inside,outside) tcp 1.1.1.1 80 1.1.1.1 8080 netmask 255.255.255.255
static (inside,outside) tcp 2.2.2.1 80 1.1.1.1 8080 netmask 255.255.255.255

PIX: reject
PDM: reject

B-2 redundant/overlap between children and parent
B-2-1 redundant, child first

static (inside,outside) tcp 1.1.1.1 80 1.1.1.1 8080 netmask 255.255.255.255
static (inside,outside) tcp 1.1.1.0 80 1.1.1.0 8080 netmask 255.255.255.0

PIX: accept
PDM: warn

B-2-2 redundant, parent first

static (inside,outside) tcp 1.1.1.0 80 1.1.1.0 8080 netmask 255.255.255.0
static (inside,outside) tcp 1.1.1.1 80 1.1.1.1 8080 netmask 255.255.255.255

PIX: accept
PDM: warn

B-2-3 overlap, child first

static (inside,outside) tcp 1.1.1.1 80 1.1.1.1 8080 netmask 255.255.255.255
static (inside,outside) tcp 1.1.1.0 80 1.1.1.0 80 netmask 255.255.255.0

PIX: accept
PDM: warn

B-2-4 overlap, parent first

static (inside,outside) tcp 1.1.1.0 80 1.1.1.0 80 netmask 255.255.255.0
static (inside,outside) tcp 1.1.1.1 80 1.1.1.1 8080 netmask 255.255.255.255

PIX: accept
PDM: warn

B-3 overlap with interface IP

ip address outside 192.168.1.1 255.255.255.0
static (inside,outside) tcp 192.168.1.0 80 1.1.1.0 8080 netmask 255.255.255.0

PIX: accept
PDM: accept

B-4 overlap with global pool

global (outside) 1 192.168.1.1-192.168.1.10
static (inside,outside) tcp 192.168.1.2 80 1.1.1.2 8080 netmask 255.255.255.255

PIX: accept
PDM: accept

C. Static PAT and NAT

Combinations of all cases mentioned in scenarios **A** and **B**. Overlapping between static NAT and PAT is bad because it creates unpredictable address translation on the firewall. Listed are some possible misconfigurations you may encounter.

C-1 static and PAT for single address

C-1-1 static first

static (inside,outside) 1.1.1.1 1.1.1.1 netmask 255.255.255.255
static (inside,outside) tcp 1.1.1.1 80 1.1.1.1 8080 netmask 255.255.255.255

PIX: reject
PDM: reject

C-1-2 PAT first

static (inside,outside) tcp 1.1.1.1 80 1.1.1.1 8080 netmask 255.255.255.255
static (inside,outside) 1.1.1.1 1.1.1.1 netmask 255.255.255.255

PIX: accept
PDM: reject

C-2 general static, with exception of PAT for a single address

C-2-1 static first

static (inside,outside) 1.1.1.0 1.1.1.0 netmask 255.255.255.0
static (inside,outside) tcp 1.1.1.1 80 1.1.1.1 8080 netmask 255.255.255.255

PIX: warn
PDM: warn

C-2-2 PAT first

static (inside,outside) tcp 1.1.1.1 80 1.1.1.1 8080 netmask 255.255.255.255
static (inside,outside) 1.1.1.0 1.1.1.0 netmask 255.255.255.0

PIX: accept
PDM: warn

D. Static PAT and dynamic NAT. Similar to scenario **C**, overlapping between static PAT and dynamic NAT creates unpredictable address translation on the firewall, although overlapping between normal static and dynamic NAT is fine and causes no problem.

D-1 overlap with nat 0

nat (inside) 0 0 0

static (inside,outside) tcp 2.2.2.1 80 1.1.1.1 8080 netmask 255.255.255.255
or
static (inside,outside) tcp 1.1.1.1 80 1.1.1.1 8080 netmask 255.255.255.255

PIX: accept
PDM: warn

D-2 overlap with dynamic nat

nat (inside) 1 0 0
global (outside) 1 2.2.2.1-2.2.2.100
static (inside,outside) tcp 2.2.2.101 80 1.1.1.1 8080 netmask 255.255.255.255

PIX: accept
PDM: warn

E. Between different pairs of local/global interfaces.

static (inside,outside) 3.3.3.1 3.3.3.1 netmask 255.255.255.255 0 0
static (intf2,outside) 3.3.3.1 2.2.2.1 netmask 255.255.255.255 0 0

PIX: accept
PDM: reject

Copyright © 2001-2004, Cisco Systems, Inc.

Translation Exemption Rule

Configuration>Translation Rules>Translation Exemption Rule

The **Add**, **Edit** and **Paste Exemption Rule** dialog box lets you add, edit, and paste Network Address Translation (NAT) exemption rules for your firewall, which are viewed in the Translation Rules table of the **Configuration>Translation Rules** tab. Depending upon which command you selected in the Translation Rules menu, the title for this dialog box will appear as **Add Address Exemption Rule**, **Edit Address Exemption Rule**, or **Paste Address Exemption Rule**.

The following sections are included in this Help topic:

- Field Descriptions
  - Action
  - Host/Network Exempted From NAT
  - When Connecting To
- Adding Address Translation Exemption Rules

Note: Review **Important Notes about Object Groups** regarding the naming of Network and Service Groups**.** See also Hosts/Network>Add/Edit Network Groups.

Field Descriptions

The **Add**, **Edit** and **Paste Address Exemption Rule** dialog boxes display the following fields:

Action

The Action group box allows you to select the action, exempt or do not exempt, that this exemption rule will take if the host/network meets the criteria defined.

The **Select an action** list options are as follows:

- **Exempt**—Specifies that the traffic defined will be exempted from NAT.
- **Do Not Exempt**—Specifies that the traffic defined will not be exempted from NAT.

Host/Network Exempted From NAT

The Host/Network Exempted From NAT group box allows you to define the criteria which must be met for the Action to be performed. The criteria my be defined by selecting an IP address, Name, Group, or by browsing a previously defined list of hosts/networks.

IP Address—Selects the criteria of testing the IP address of the source host or network to determine if the Action of the exemption rule will be applied. Selecting this option displays the following fields:

- **Interface**—Selects the firewall network interface name on which the original host or network resides.
- **IP address**—Specifies the IP address of the host or network to which you would like to apply a rule.
- **Mask**—Select the network mask (netmask) for the address.

Name—Selects the criteria of testing the name of the source host or network to determine if the Action of the exemption rule will be applied. Selecting this option displays the following fields:

- **Name**—Lets you select a previously defined name of a host or network to which you would like to apply the rule. Note: The firewall also automatically generates a host name for each interface by using the interface name, such as `inside` or `outside`.

Group—Selects the criteria of testing a group of the source host or network to determine if the Action of the exemption rule will be applied. Selecting this option displays the following fields:

- **Interface**—Interface—Selects the firewall network interface name on which the original host or network resides.
- **Group**— Selects the group of the host or network to which you would like to apply the rule.

Browse—Lets you select the correct IP address and mask from the Hosts/Networks tree from a predefined host or network.

When Connecting To

IP address—Specifies the IP address of the destination host or network to which you would like to apply the exemption rule.

- **Interface**—Selects the firewall network interface name on which the original host or network resides.
- **IP address**—Specifies the IP address of the host or network to which you would like to apply

a rule.

- **Mask**—Select the network mask (netmask) for the address.

Name—Selects the criteria of testing the name of the source host or network to determine if the Action of the exemption rule will be applied. Selecting this option displays the following fields:

- **Name**—Lets you select a previously defined name of a host or network to which you would like to apply the rule. Note: The firewall also automatically generates a host name for each interface by using the interface name, such as `inside` or `outside`.

Group—Selects the criteria of testing a group of the source host or network to determine if the Action of the exemption rule will be applied. Selecting this option displays the following fields:

- **Interface**—Interface—Selects the firewall network interface name on which the original host or network resides.
- **Group**— Selects the group of the host or network to which you would like to apply the rule.

Browse... —Lets you select the correct IP address and mask from the Hosts/Networks tree from a predefined host or network.

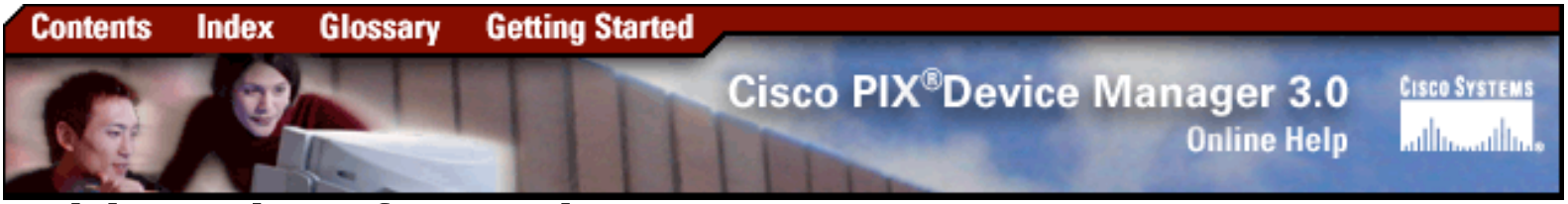
- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Adding Address Translation Exemption Rules

Follow these steps to create a new exemption rule:

1. From the **Configuration>Translation Rules** tab, add a new rule by one of these methods:
   - Select **Translation Exemption Rules**.
   - On the **Rules** menu, click **Add**.
   - Click **Add a new Rule** on the PDM toolbar.
   - Using the right mouse button (right-click), click **Add**.
2. Create the new translation rule by filling in the appropriate fields.
3. Click **OK**, then **Apply** on the **Configuration>Translations Rules** tab.

Copyright © 2001-2004, Cisco Systems, Inc.



Add Basic Information

Configuration>Hosts/Networks>Add>Create host/network>Basic Information

In the **Create host/network>Basic Information** dialog box, you specify values for the IP address, netmask, interface, and name of a host or network. This information provides the basic identification information for that host or network. PIX Device Manager uses the name and IP address/netmask pair to resolve references to this host or network in the source and destination conditions of access rules and in translation rules. PIX Device Manager uses the interface value to apply access and translation rules that reference this host or network to the correct interface. The interface delivers network packets to the host or network, and therefore, it enforces the rules that reference that host or network.

The following sections are included in this Help topic:

- Field Descriptions
- Defining Basic Information

Field Descriptions

The **Create host/network>Basic Information** dialog box displays the following fields:

- **IP Address**—Identifies the IP address of the host or network you want to add.
- **Mask**—(address mask) Identifies the bits of the IP address to treat as wildcard. When you define a host, this value must be 255.255.255.255. For example, to define a Class B network, with an address space between 192.168.0.0 and 192.168.255.255, you would specify an IP address value of 192.168.0.0 and a mask value of 255.255.0.0. To define the host, 192.168.1.1, on this network, you would specify an IP address value of 192.168.1.1 and a mask value of 255.255.255.255.
- **Interface**—Identifies the interface in the firewall unit from which this host or network is reachable. The host or network must either be directly connected to this interface or reside behind a gateway that is reachable from this interface.
- **Name [Recommended]**—Identifies the name used when referencing this host or network in access and translation rules. This name may include up to 16 characters. Valid characters are a to z, A to Z, 0 to 9, period ("."), and an underscore ("_"). The name must start with an alphabetic character. We recommend that you name all hosts and networks.
- **Next**—Continues to the **Create host/network>Static Route** dialog box.
- **Cancel**—Clears any changes you may have made and returns to the **Configuration>Hosts/Networks** tab.
- **Help**—Provides more information.

Defining Basic Information

Follow these steps to specify the basic identification information for the host or network:

1. To define a host or network, click **Add** on the **Configuration>Hosts/Networks** tab. The **Create host/network>Basic Information** dialog box appears.
2. To specify the address used to reach the host or network, enter the address in the **IP Address** box.
3. To specify the mask value that corresponds to the network or host that you are defining, click the desired value in the **Mask** list. If you are defining a host, you must click the 255.255.255.255 value.
4. If the selected interface does not correspond to the interface from which the host or network is directly reachable, click the correct interface name in the **Interface** list. By default, this value is the interface selected on the **Configuration>Hosts/Networks** tab.
5. To specify the name used when referencing this host or network within access or translation rules, enter the name in the **Name (Recommended)** box. While this value is optional, it is recommended.
6. To define the static routing rule for this host or network, click **Next**. If the selected interface is not the inside interface, the **Create host/network>Static Route** dialog box appears. Otherwise, the **Create host/network>NAT (Network Address Translation)** dialog box appears.

Copyright © 2001-2004, Cisco Systems, Inc.

Understanding Static NAT

Static NAT refers to persistent one-to-one address mapping translation. In contrast to dynamic NAT, the static address translation does not vary over time. For inbound access to the internal local hosts, you should use static NAT rules. A static NAT rule maps an external IP address to a specific internal host's internal IP address. An internal IP address may be assigned to different external addresses on different interfaces.

Caution: If you expose your internal DNS servers using a static NAT rule, you do not benefit from the address hiding feature provided by translation rules. External users can simply request information about your trusted networks from the DNS servers that you expose.

Example Use Scenario

Scenario: We can define a static NAT rule that maps from the external IP address 192.168.7.130 (translated address) to the internal file server 192.168.1.3 (real address).

For this scenario, PDM generates a rule similar to the following:
static (inside, outside) 192.168.7.130 192.168.1.3 netmask 255.255.255.255 0 0

Description: When the firewall unit receives a session request where the source address matches the IP address of the internal file server, it changes the source address to the external IP address before placing the packet onto the network of which the external address is a member. Likewise, when the firewall unit receives a network packet destined for the translated address, it changes the destination address to the address of the internal file server and places the new packet onto the network to which the internal file server belongs. Thus, the internal file server processes the packet as though it were originally destined for the file server. In both cases, all packets that are part of a valid session are remapped according to the translation rule (assuming that the active security policy permits the communication). If the active security policy does not permit a specific communication, the session request is rejected and the translation never occurs.

Copyright © 2001-2004, Cisco Systems, Inc.

Understanding Dynamic NAT

Dynamic NAT, commonly referred to as Network Address Translation (NAT), is the process of converting between IP addresses used within an intranet or other private network (called a subdomain) and Internet IP addresses (or external IP addresses on a Cisco firewall unit). This approach makes it possible to use a large number of addresses within the subdomain without depleting the limited number of available numeric Internet IP addresses.

In addition to conserving IP addresses, dynamic NAT provides additional security features for your network by hiding its internal structure and allowing logical mappings to users who compose the different groups and departments within your company. While some users may not need to use dynamic NAT, you should keep this feature in mind as your network continues to grow.

The following sections describe what problems address hiding solves and how it works to solve these problems.

- Why You Should Use Dynamic NAT
- How Dynamic NAT Works
- How Session Awareness and Port Mapping Affect Dynamic NAT

Why You Should Use Dynamic NAT

An address hiding translator, such as the software module that provides this feature for a Cisco firewall unit, provides several benefits for your network:

- Enhances network security by hiding your network's internal structure from external users and enables you to logically group your users according to security domains.
- Permits an almost unlimited number of users for one Class C network address because valid external addresses are required only when a user is connected to the Internet.
- When you attach your existing IP networks to the Internet, you do not need to replace the IP address of each computer on your internal subnets with a valid, registered IP address from the Internet Network Information Center (the American Registry for Internet Numbers [ARIN]).
- As these benefits indicate, NAT overcomes several limitations associated with the current IP addressing scheme. A discussion of these limitations follows.

Conceals Internal IP Addresses from Internet Users. As the network administrator, you may wish to conceal internal network addresses from the Internet, which prevents them from being disclosed to possibly malicious users. An address hiding translator dynamically assigns a valid external IP address to an internal IP address by mapping the internal address to an external address. Because this mapping between the external and internal IP addresses is temporary (it lasts only for the duration of a session or until the user-configured idle time-out value is exceeded), your internal IP addresses are concealed from the Internet. Only the external addresses appear in the packets that are distributed across the Internet.

Requires Fewer Registered IP Addresses. To connect to the Internet, a company must purchase IP addresses from the American Registry for Internet Numbers (ARIN), which is the organization responsible for registering and assigning IP addresses to those who wish to connect to the Internet. Currently, IP addresses are allocated based on the size of the company that is requesting IP addresses. To prevent depletion of IP addresses on the Internet, small and medium organizations receive fewer IP addresses, regardless of plans for future expansion. An address hiding translator bypasses this limitation and ensures that you can continue to grow your network without acquiring additional addresses. Because an address hiding translator distributes the control and allocation of valid external IP addresses, it provides full connectivity and access to the Internet regardless of the size of your network or the number of users that you support.

Use of Invalid Internal Addresses. Because many companies use invalid IP addresses within their intranets, computers using those addresses cannot legally access the Internet. From the perspective of the routers, these addresses appear to belong to a network that is different from the Internet. If you have used such addresses, you may find that it is impractical to change them to valid internal addresses. The address hiding translator maintains the integrity of your internal addressing schemes by mapping registered IP addresses to all internal addresses, including invalid addresses.

Note: Invalid IP addresses are also referred to as reserved addresses, which are IP addresses restricted to special purposes, such as internal domain or Internet service provider network usage.

How Dynamic NAT Works

For information to be routed correctly, each connected computer must have a globally unique transport address that is identifiable by the routers that exist within the network of your Internet service provider, as well as those routers that compose the Internet backbone. If the IP addresses are not unique, these routers cannot route network packets. Those users who have duplicate IP addresses cannot be reached and cannot establish application sessions.

Network Address Translation solves these problems by temporarily reassigning a registered IP address to an internal computer that requests services across the Internet (or another external network). When residing on a firewall unit, the address hiding translator acts as a buffer between the global Internet and the local IP networks called subnets. The internal subnets only require IP addresses that are unique to that subnet level. When a computer on one of these subnets sends traffic out over the Internet (thus traversing the firewall), the address hiding translator strips the internal IP address (unique for that subnet) from the network packets and replaces that address with a unique external address that is registered and assigned to that subnet or site.

Often, the address hiding translator contains a pool of external IP addresses, which enables more than one internal computer to connect to the Internet at the same time. The pool contains those IP addresses that are registered with the American Registry for Internet Numbers (ARIN), http://www.arin.net. When you allocate IP addresses for your subnets, you must verify that those addresses do not conflict with the external IP addresses. Doing so ensures that the external IP addresses remain unique, enabling the address hiding translator to distinguish among computers. When a network packet is routed across the firewall, the address hiding translator replaces the internal corporate address with a temporary external address. As soon as the application session is over (or the idle time-out value is exceeded), the external address is returned to the pool, where it can be reassigned during a new session request.

How Session Awareness and Port Mapping Affect Dynamic NAT

In addition to the one-to-one address translation, the firewall also provides many-to-one address translation. The many-to-one mapping is called Port Address Translation (PAT). With PAT, the translation uses the port in addition to the IP address. By using the port, up to 65,535 local hosts can concurrently share a single IP address. Because PAT automatically maps multiple sessions to the same registered IP address, you do not need as many registered IP addresses. This feature also ensures that you can dynamically grow your network.

Note: Because PAT requires port information, only TCP, UDP, and ICMP echo/echo-reply operate with PAT.

Copyright © 2001-2004, Cisco Systems, Inc.

Hosts/Networks

Configuration>Hosts/Networks

The **Configuration>Hosts/Networks** tab, lets you view, edit, add to, or delete from the list of hosts and networks defined for the selected interface defined previously in Configuration>System Properties>Interfaces. The PIX Device Manager requires that you define any host or network that you intend to use in access rules and translation rules. These hosts or networks are organized below the interface from which they are reachable.

Access rules reference these hosts or networks in the source and destination conditions of a rule, while translation rules reference them in the original address condition of a rule. When defining either type of rule, you can reference a host or network by clicking **Browse** in the appropriate add or edit rule dialog box. Additionally, you can reference the host or network by name if a name is defined for that host or network. We recommend that you name all hosts and networks.

In addition to defining the basic information for these hosts or networks, you can define route settings and Network Address Translation (NAT) rules for any host or network. You can also configure route settings in the **Routing>Static Route** panel on the **Configuration>System Properties** tab and translation rules on the **Configuration>Translation Rules** tab. These different configuration options accomplish the same results. The **Configuration>Hosts/Networks** tab provides another view to modify these settings on a per host/network basis

The following sections are included in this Help topic:

Introduction

- Important Notes
- Important Notes about Object Groups
- Field Descriptions

Hosts/Networks

- Select Interface
- Adding Hosts or Networks
- Editing Hosts or Networks
- Deleting Hosts or Networks

Groups

- Adding Groups
- Editing Groups

- Deleting Groups

Important Notes

Consider the following information before defining the hosts and networks associated with the selected interface:

- You should define a host or network under an interface when it is connected either directly to that interface or indirectly through one or more gateways. PDM assumes a host or network can connect to only one Firewall interface. If, for some reason, you have a host or network that is reachable by multiple interfaces in the firewall unit, you must create an instance of that host or network for each such interface.
- If you attempt to define an access or translation rule using a host or network not previously defined on the **Configuration>Hosts/Networks** tab, you are presented with a shortcut to access the add or edit settings provided by this tab.

Important Notes about Object Groups

Object groups allow multiple objects, such as networks or services, to be associated and given a name. To simplify configuration, a name may then be used in place of a list in Rules or VPN configuration.

PIX Firewall Version 6.2 and higher support 4 types of named object groups:

- **`network`**
- **`service`**
- **`protocol`**
- **`icmp-type`**

The **Name** of any object group must be unique to all 4 types. For example, a **`service`** group and a **`network`** group may not share the same name.

The object group types **`icmp-type`** and **`protocol`** are not created in PDM and may not be renamed in PDM. However, PDM does support editing and deleting object groups using **Tools>CLI** (Command Line Interface). You may also edit or delete **`network`** type object groups under the Hosts/Networks tab and **`service`** type object groups in **Tools>Service Groups**.

Field Descriptions

The **Hosts/Networks** tab displays the following fields:

- **Select Interface**—Displays a list of hosts and networks defined for the interface selected. You can select any enabled interface previously defined on the **Configuration>System Properties** tab.
- **Groups**—Displays a list of Groups associated with the selected interface. Additional Gorups may be added, edited, or deleted.

- **Add**—Opens the **Add** dialog box.
- **Edit**—Opens the **Edit** dialog box.
- **Delete**—Deletes the selected item.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Select Interface

Use this list to select the firewall interface on which you wish to manage networks, hosts, or groups.

Adding Hosts or Networks

Follow these steps to add a host or network:

1. Click **Add** in the **Hosts/Networks** region of the **Configuration>Hosts/Networks** tab.
2. Complete the series of screens displayed by the **Create host/network** wizard.
3. Click **Apply**.

Editing Hosts or Networks

Follow these steps to change information about an existing host or network:

1. Select a host or network from the tree in the **Hosts/Networks** region of the **Configuration> Hosts/Networks** tab.
2. Click **Edit**.
3. Complete the **Edit host/network** dialog box that appears.
4. Click **OK** on the **Edit host/network** screen.
5. Click **Apply**.

Deleting Hosts or Networks

Follow these steps to delete an existing host or network:

1. On the **Configuration>Hosts/Network** tab, select the name of the interface from which you want to delete a host or network in the **Interface** box.

   In the tree, select the host or network you want to delete.If necessary, expand the tree to view the children of a specific node. You cannot delete an interface.

   Note: When you delete a host or network, PIX Device Manager deletes all access and translation rules and static routes defined for this host or network.

   ---

2. Click **Delete**.A message box appears prompting you to verify the delete operation.
3. To delete the selected host or network from the selected interface, click **OK**.

Adding Groups

Follow these steps to create a group of hosts or networks:

1. Click **Add** in the **Groups** region of the **Configuration>Hosts/Networks** tab.
2. Select the networks or hosts you want to add to a group on the **Add Host/Network Group** dialog box that appears.
3. Click **OK** on the **Add Host/Network Group** dialog box.
4. Click **Apply**.

Editing Groups

Follow these steps to change a group of hosts or networks:

1. Select an existing group from the tree in the **Groups** region of the **Configuration>Hosts/Networks** tab.
2. Click **Edit**.
3. Change the networks or hosts in the selected group on the **Edit Host/Network Group** dialog box that appears.
4. Click **OK** on the **Edit Host/Network Group** dialog box.
5. Click **Apply**.

Deleting Groups

Follow these steps to delete a group of hosts or networks:

1. Select a group from the tree in the **Groups** region of the **Configuration>Hosts/Networks** tab.
2. Click **Delete**. You cannot delete a host or network that is currently in use.
3. Click **Apply**

Copyright © 2001-2004, Cisco Systems, Inc.

Add/Edit Address Translation Rule

Configuration>Translation Rules>Add/Edit Address Translation Rule

The **Add, Edit** and **Paste Translation Rule Properties** dialog box lets you add, edit, and paste translation rules for your firewall, which are viewed in the **Translation Rules** table. Depending upon which command you selected from the **Rules** menu, the title for this dialog box will appear as **Add Address Translation Rule**, **Edit Address Translation Rule**, or **Paste Address Translation Rule**.

The following sections are included in this Help topic:

- Field Descriptions
- Adding Address Translation Rules
- Example
- Printing

Note: Review **Important Notes about Object Groups** regarding the naming of Network and Service Groups**.**

Field Descriptions

The **Add**, **Edit** and **Paste Address Translation Rule** dialog boxes display the following fields:

- Original Host/Network
  - **Interface**—Selects the firewall network interface on which the original host or network resides.
  - **IP address**—Specifies the IP address of the host or network to which you would like to apply a rule.
  - **Mask**—Select the network mask (netmask) for the address.
  - **Browse**—Lets you select the correct IP address and mask from the Hosts/Networks tree from a predefined host or network.
  - **Translate address on less secured interface**—Selects the firewall interface to which you want to provide access. For example, if you are configuring a translation of an inside address, you would select the outside interface, because that is where the translation occurs.
  - **Static**—Specifies that the address translation is a static, one-to-one translation of an IP address from a private (non-valid) IP address to a global (valid) IP address. Static or Dynamic can be selected, but not both.
  - **IP address**—The global IP address on the lower security level interface you are accessing.

    - **Advanced**—Lets you configure the **DNS Rewrite, Maximum Connections**, **Embryonic Limit** and **Randomize Sequence Number**.
        - **DNS Rewrite**—Lets the firewall rewrite the DNS record so that an outside client can resolve name of an inside host using an inside DNS server, or vice versa. For example, assume an inside web server www.example.com has IP 192.168.1.1, it is translated to 10.1.1.1 on the outside interface. An outside client sends a DNS request to an inside DNS server, which will resolve www.example.com to 192.168.1.1. When the reply comes to the firewall with DNS Rewrite enabled, the firewall will translate the IP address in the payload to 10.1.1.1, so that the outside client will get the correct IP address.
        - **Maximum Connection**—The maximum number of connections that are allowed to connect to the statically translated IP Address. Valid options are 0 through 65,535. If this value is set to zero, the number of connections are unlimited.
        - **Embryonic Limit**—The number of embryonic connections allowed to form before the firewall begins to deny these connections. Set this limit to prevent attack by a flood of embryonic connections. An embryonic connection is one that has has been started but has not yet established, such as a three-way TCP handshake state. Valid values are 0 through 65,535. If this value is set to zero, the number of connections is unlimited. A positive number enables the TCP Intercept feature.
        - **Randomize Sequence Number**—With this check box selected, the firewall will randomize the sequence number of TCP packets. Disable this feature only if another inline firewall is also randomizing sequence numbers and the result is scrambling the data. Use of this option opens a security hole in the firewall. The default is selected.

    - **Redirect port**—Enables static Port Address Translation (PAT). This check box can only be selected if Static is selected.
        - **TCP** —Selects a TCP port to be specified in the **Original Port** and **Translated Port** boxes.
        - **UDP**—Selects a UDP port to be specified in the **Original Port** and **Translated Port** boxes.
        - **Original Port**—The port number supplied by the host/network.
        - **Translated Port**—The port number to which the original port number will be translated.
- **Dynamic**—Lets you specify either a predefined pool of IP addresses, or perform PAT on a global IP address or the less secure interface for multiple hosts on the more secure interface. This is set up through either **Advanced** or **Manage Pools**. For example, if your inside network has multiple hosts, you can permit outbound access through a pool or a PAT address by using Dynamic NAT to dynamically assign an global IP address for each host requesting an outbound connection. Static or Dynamic can be selected, but not both.
    - **Address pool**—Select the pool of addresses used for Dynamic NAT.
    - **Advanced**—Lets you create, edit, and manage global IP address pools for Dynamic NAT.
    - **Manage Pools**—Lets you create, edit, and manage global IP address pools for Dynamic NAT.
    - **Address pool** table—Lists the pools and addresses used for Dynamic NAT.
        - **Pool ID**—The pool ID is a number that identifies the pool of addresses used for Dynamic NAT. This is a positive number between 1 and 2,147,483,647.
        - **Address**—Lists the address or range of addresses used for Dynamic NAT or PAT.
- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Adding Address Translation Rules

Follow these steps to create a new translation rule:

1. From the **Configuration>Translation Rules** tab, add a new rule using one of the following methods:
    - On the **Rules** menu, click **Add**.
    - Click **Add a new Rule** on the PDM toolbar.
    - Using the right mouse button (right-click), click **Add**.
2. Create the new translation rule by filling in the appropriate fields. See the example that follows.
3. Click **OK**, then **Apply** on the **Configuration>Translations Rules** tab.

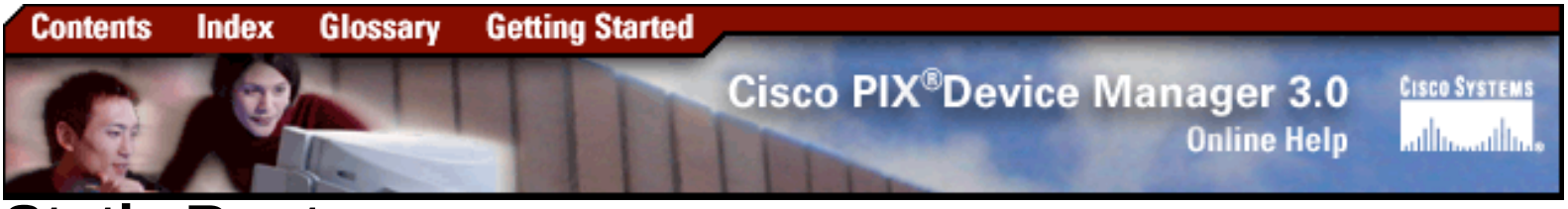
Example

To create a dynamic rule for all outbound connections to access the Internet on a PIX Firewall that already has a properly configured outside interface, you would complete the following steps. In this example, the private network is on the Inside interface on the 192.168.1.0 255.255.255.0 network, with 192.168.1.1 as the address of the Inside interface. The outside interface has an address of 209.165.200.225, and the default gateway has been set to 209.165.200.226. Before you begin this, you must configure your address pool for PAT using the **Manage Global Address Pools** dialog box.

1. From the **Configuration>Translation Rules** tab, add a new rule using one of the following methods:
    1. On the **Rules** menu, click **Add**.
    2. Click the **Add a new Rule** on the PDM toolbar.
    3. Using the right mouse button (right-click), click **Add**.
2. In the **Original Host/Network** region of the **Add Address Translation Rule** dialog box, set the Interface to **(inside)**, the IP address to **0.0.0.0**, and the Mask to **0.0.0.0**. This permits all outbound connections to be translated.
3. In the **Translate address on less secured interface** list, select **outside**. This specifies connections that start on the inside interface that go through the outside interface will be translated.
4. In the **Translate Address to** region of the **Add Address Translation Rule** dialog box, click **Dynamic**. Select the address pool you created using the **Manage Pools** button, which specifies you are using PAT on the outside interface.
5. Click **OK**, then **Apply** on the **Configuration>Translations Rule** tab.

To see an example of what this completed Translation Rule would look like, see the Translation Rules help.

Copyright © 2001-2004, Cisco Systems, Inc.



Static Route

Configuration>System Properties>Routing>Static Route

The **Static Route** panel lets you enter a static route for a specified interface.

The following sections are included in this Help topic:

- Screen Element Descriptions
- Adding static routes
- Editing static routes
- Deleting static routes
- Applying Changes

The **Static Route** panel lets you create static routes that will access networks connected to a router on any interface. To enter a default route, set the IP address and mask to 0.0.0.0, or the shortened form of 0.

If an IP address from one of the firewall unit's interfaces is used as the gateway IP address, the firewall will ARP the designated IP address in the packet instead of ARPing the gateway IP address.

Leave the **Metric** to the default of 1 unless you are sure of the number of hops to the gateway router.

Screen Element Descriptions

The **Static Table** panel provides the following fields:

- **Interface Name**—Lists the internal or external network interface name enabled in **Configuration>System Properties>Interfaces**.
- **IP Address**—Lists the internal or external network IP address. Use **0.0.0.0** to specify a default route. The **0.0.0.0** IP address can be abbreviated as **0**.
- **Netmask**—Lists the network mask address that applies to the IP address. Use **0.0.0.0** to specify a default route. The **0.0.0.0** netmask can be abbreviated as **0**.
- **Gateway IP**—Lists the IP address of the **gateway router** which is the next hop address for this router.
- **Metric**—Lists the number of **hops** to the gateway IP. The default is **1** if a metric is not specified.
- **Add**—Opens the **Add** dialog box.
- **Edit**—Opens the **Edit** dialog box.
- **Delete**—Deletes the selected item.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use

the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Adding Static Routes

Follow these steps to add static routes:

1. Click **Add** to open the **Add Static Route** dialog box.
2. Choose the **interface** name.
3. Choose the **mast IP address** associated with the interface name you have chosen.
4. Enter the IP address of the gateway router in **Gateway IP.**
5. Enter in the number of hops to the gateway IP address in **Metric.**
6. To return to the previous panel click:
   - **OK**—Accepts changes and returns to the previous panel.
   - **Cancel**—Discards changes and returns to the previous panel.
   - **Help**—Provides more information.
7. Changes will actually be made to the firewall configuration when you click **Apply**.

Editing Static Routes

Follow these steps to edit static routes:

1. Select an static route from the **Static Route** table.
2. Click **Edit** to open **Edit Static Route**.
3. Choose the **interface** name.
4. Choose the **mast IP address** associated with the interface name you have chosen.
5. Enter the IP address of the gateway router in **Gateway IP.**
6. Enter in the number of hops to the gateway IP address in **Metric.**
7. To return to the previous panel click:
   - **OK**—Accepts changes and returns to the previous panel.
   - **Cancel**—Discards changes and returns to the previous panel.
   - **Help**—Provides more information.
8. Changes will actually be made to the firewall configuration when you click **Apply**.

Deleting Static Routes

Follow these steps to delete a static route:

1. Select a static route from the **Static Route Table**.
2. Click **Delete**.

Applying Changes

Changes to the table made by **Add**, **Edit**, or **Delete** are not immediately applied to the running configuration. You must click on one of the following buttons to apply or discard changes:

1. **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
2. **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Manage Global Address Pools

Configuration>Hosts/Networks>Add>Create host/network>NAT>Manage Pools

The **Manage Global Address Pools** dialog box lets you view, define new, or delete existing global address pools used in dynamic NAT rules. For more information on dynamic NAT rules and its uses, refer to Understanding Dynamic NAT.

The following sections are included in this Help topic:

- Field Descriptions
- Adding Address Pools
- Deleting Address Pools

Field Descriptions

The **Manage Global Address Pools** dialog box displays the following fields:

- **Global Address Pools** table
  - **Interface**—Identifies the interface name associated with the address pool used for dynamic address translation.
  - **Pool ID**—Identifies the ID number of the address pool.
  - **IP Address(es)**—Identifies the type and value of the address(es) for the pool. It can identify one of the following types:
    - A range of addresses
    - A **PAT** address
    - A PAT address associated with an interface
- **Add**—Opens **Add/Edit Global Pool Item**, from which you can define the settings for a new global address pool.
- **Edit**—Opens **Add/Edit Global Pool Item** for the selected pool.
- **Delete**—Deletes the selected global address pool.
- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Adding Address Pools

Follow these steps to add a global address pool:

1. To open the **Add Global Pool Item** dialog box, click **Add** in the **Manage Global Address Pools** dialog box.
2. To specify the interface name to associate with with the new address pool, select that name in the **Interface** list.
3. To specify the ID number that dynamic NAT rules use to reference this address pool, enter the number in the **Pool ID** box.
4. Click the option that identifies the type of address pool that you want to define:
   - **Range**—Select this option to specify that a range of IP addresses be used with the new address pool. If you select this option, specify the following values:
     a. Enter the start and end addresses used by the range in the **IP Address** boxes.
     These addresses are the addresses to which the original addresses will be translated. If the firewall is exposing the host or network to users on the Internet, these IP addresses must be valid IP addresses that are registered with the American Registry for Internet Numbers (ARIN).
     b. Enter the mask in the **Network Mask (optional)** box.
     This value identifies the mask of the network on which translated IP addresses are members.
   - **Port Address Translation (PAT)**—Click this option to specify that an IP address be used for Port Address Translation (PAT). If you select this option, specify the following value:
     - Enter the IP address used for PAT in the **IP Address** box.
     This value is the specific translated IP address to which you want to translate the original addresses of the translated host or network. If the firewall is exposing the host or network to users on the Internet, this IP address must be a valid IP address that is registered with ARIN.
   - **Port Address Translation (PAT) using the IP address of the interface**—Select this option to specify that the IP address assigned to the interface selected in the **Interface** list be used as the translated address for PAT.
5. To accept your changes and close the **Add Global Pool Item** dialog box, click **OK**.

Deleting Address Pools

Follow these steps to delete a global address pool:

1. Select an address pool from the **Global Address Pools** table in the **Manage Global Address Pools** dialog box.
2. Click **Delete**.
3. To accept your changes and close the **Manage Global Address Pools** dialog box, click **Done**.

Copyright © 2001-2004, Cisco Systems, Inc.

Add, Edit, Insert or Paste Filter Rule

Configuration>Access Rules>Filter Rules>Add, Edit, Insert or Paste Rule

The **Add, Edit, Insert,** or **Paste Rule** dialog boxes let you create a new rule, or modify an existing rule.

Note: Identify the URL filtering servers you want to use on the System Properties>URL Filtering page.

The following sections are included in this Help topic:

- Field Descriptions
- Editing a Rule
- ActiveX Filtering
- Do Not Filter ActiveX
- Java Applet Filtering
- Do Not Filter Java
- HTTP (URL) Filtering
- Do not filter HTTP (URL)
- HTTPS Filtering
- Do not filter HTTPS
- FTP Filtering
- Do Not Filter FTP

Field Descriptions

The **Add, Edit, Insert,** or **Paste Rule** dialog boxes display the following areas and fields:

Area	Description and Fields

<table>
<tr><td>Action</td><td colspan="3">Action area—Determines the action type of the new rule. Choose the type of action from the list:

• Filter ActiveX
• Do Not Filter ActiveX
• Filter Java Applet
• Do Not Filter Java
• Filter HTTP (URL)
• Do not filter HTTP (URL)
• Filter HTTPS
• Do not filter HTTPS
• Filter FTP
• Do Not Filter FTP</td></tr>
<tr><td rowspan="6">Source and Destination Host/ Network</td><td colspan="3">Defines the source and destination host or network of the rule.</td></tr>
<tr><td rowspan="5">IP Address option button</td><td colspan="2">Click this option button to identify the networks by IP address.</td></tr>
<tr><td>Interface</td><td>The interface on which the host or network resides.</td></tr>
<tr><td>IP address</td><td>The IP address of the host or network.</td></tr>
<tr><td>Mask</td><td>The netmask of the host or network.</td></tr>
<tr><td>Browse</td><td>Lets you select an existing host or network by clicking the options under the Select Host/ Network panel to populate the Name, Interface, IP address, and Mask boxes with the properties of the selected host or network.</td></tr>
<tr><td rowspan="2">Name option button</td><td colspan="2">Click this option button to identify the networks by name.</td></tr>
<tr><td>Name</td><td>The name of the host or network. If you choose this option, and reopen the rule to edit it, the option button selection reverts to IP Address, and the named host/network IP address information appears in the fields</td></tr>
<tr><td>Action Filtering Option</td><td colspan="3">Each action type includes custom options. See the following action types for field descriptions for this area:

• Filter ActiveX
• Do Not Filter ActiveX
• Filter Java Applet
• Do Not Filter Java
• Filter HTTP (URL)
• Do not filter HTTP (URL)
• Filter HTTPS
• Do not filter HTTPS
• Filter FTP
• Do Not Filter FTP</td></tr>
</table>

Editing a Rule

Follow these steps to add a new rule or to modify an existing rule:

1. From the **Action** list, choose an action:
    - Filter ActiveX
    - Do Not Filter ActiveX
    - Filter Java Applet
    - Do Not Filter Java
    - Filter HTTP (URL)
    - Do not filter HTTP (URL)
    - Filter HTTPS
    - Do not filter HTTPS
    - Filter FTP
    - Do Not Filter FTP
2. Define the source and destination hosts or networks. Filters only apply to outgoing traffic, from a higher security network to a lower security network (for example, inside to outside). You cannot filter traffic from outside to inside.

- By IP Address—If you select this option, you can specify a particular network or host behind an interface, or you can use wildcards to specify any network behind the interface. By default, the IP address and mask are 0.0.0.0, the wildcard notation signifying any address.
    - To browse to an IP address:
        a. Click the **IP Address** option button.
        b. Click the **Browse** button.
        The Select Host/Network dialog box appears.
        c. From the list, choose the interface in front of the host/network.
        All the hosts and networks behind the interface are displayed.
        d. Select the host/network, and click **OK**.
        The interface, IP address, and subnet mask boxes are automatically filled.
    - To type an IP address:
        a. Click the **IP Address** option button.
        b. From the **Interface** list, select an interface name.
        c. In the **IP address** box, enter the IP address of the host or network.
        d. In the **Mask** box, enter the netmask of the source host or network, or select a netmask from the list.
- By Name—If you select this option, the firewall filters the specific network identified by name. By default, the networks directly connected to the firewall are named after the firewall interfaces; however, only the directly connected network is specified. If you want to filter all networks behind an interface, use the IP Address option (above).
        a. Click the **Name** option button.
        b. In the **Name** box, type the name of the source host or network; or click the **down arrow** and choose a name from the list.

3. Define the additional parameters associated with the action type you selected in Step 1. The options area that displays at the bottom of the dialog box depends on the type of action selected.

4. Click **OK** to finish editing the rule, or **Cancel** to discard your changes.

ActiveX Filtering

ActiveX objects are security risks for outbound connections because they can contain code intended to attack hosts and servers. You can disable ActiveX objects by choosing the **Filter ActiveX** action.

ActiveX Filtering Option Area Field

Field	Description
Filter Java ActiveX on the following ports	Enter a port number range on which to filter ActiveX (*n*—*n*). To filter a single port, enter the port number in the first box (or in both boxes). By default, the port number is 80 (HTTP).

Do Not Filter ActiveX

Do Not Filter ActiveX allows you specify hosts or networks that should not be filtered. For example, if the host or network you specify is included in a Filter ActiveX rule, then you can create a Do Not Filter ActiveX rule to create an exception. You can place this do not filter rule in any order (before or after the filter rule).

There are no options for this action.

Java Filtering

Java applets are security risks for outbound connections because they can contain code intended to attack hosts and servers. You can remove Java applets by choosing the **Filter Java** action.

Java Filtering Option Area Field

Field	Description

Filter Java applet on the following port(s)	Enter a port number range on which to filter ActiveX (*n*—*n*). To filter a single port, enter the port number in the first box (or in both boxes). By default, the port number is 80 (HTTP).

Do Not Filter Java

Do Not Filter Java allows you specify hosts or networks that should not be filtered. For example, if the host or network you specify is included in a Filter Java rule, then you can create a Do Not Filter Java rule to create an exception. You can place this do not filter rule in any order (before or after the filter rule).

There are no options for this action.

HTTP (URL) Filtering

The Filter HTTP (URL) action lets you designate the web traffic that is to be filtered by a Websense server or N2H2 server. When a user issues an HTTP request to a site, the firewall sends the request to the server and to the filtering server at the same time. If the filtering server permits the connection, the firewall allows the reply from the site to reach the user who issued the original request. If the filtering server denies the connection, the firewall redirects the user to a block page, indicating that access was denied.

Note: Identify the servers you want to use on the System Properties>URL Filtering page.

Note: URL filtering can considerably increase access times to websites when the filtering server is remote from the firewall.

HTTP Filtering Option Area Fields

Field	Description	
Filter HTTP on Port (s) box	Enter a port number range on which to filter HTTP (*n*—*n*). To filter a single port, enter the port number in the first box (or in both boxes). By default, the port number is 80 (HTTP).	
Long URL area	This area lets you define what action the firewall takes when the URL is longer than the maximum length permitted. The Firewall supports a maximum URL length of 1159 bytes for the N2H2 filtering server. Filtering of URLs up to 6 KB is supported for the Websense filtering server. Click one of the following option buttons to perform an action when the URL is longer than the maximum length permitted:	
	Drop	The firewall drops the packet.
	Truncate	The firewall sends only the hostname or IP address portion of the URL for evaluation to the filtering server.

	Block	The firewall denies access to the URL.
Allow Outbound Traffic if URL Server is Not Available check box	Outbound HTTP connections are not filtered if the URL server is unavailable. Otherwise, no outbound HTTP traffic is allowed until the server returns.	
Truncate CGI Requests by Removing the CGI Parameters check box	Truncates CGI URLs to include only the CGI script location and the script name (but not parameters). Many long HTTP requests are CGI requests. If the parameters list is very long, waiting and sending the complete CGI request including the parameter list can waste memory resources and impact firewall performance.	

Do Not Filter HTTP (URL)

The Do Not Filter HTTP (URL) action allows you specify hosts or networks that should not be filtered. For example, if the host or network you specify is included in a Filter HTTP (URL) rule, then you can create a Do Not Filter HTTP (URL) rule to create an exception. You can place this do not filter rule in any order (before or after the filter rule).

There are no options for this action.

HTTPS Filtering

The Filter HTTPS action lets you designate the secure web traffic that is to be filtered by a Websense server. HTTPS filtering is not supported on N2H2 servers. The firewall prevents the completion of SSL connection negotiation if the site is not allowed. The browser displays an error message such as "The Page or the content cannot be displayed." Because HTTPS content is encrypted, the firewall sends the URL lookup without directory and filename information.

Note: Identify the servers you want to use on the System Properties>URL Filtering page.

Note: URL filtering can considerably increase access times to websites when the filtering server is remote from the firewall.

HTTPS Filtering Option Area Fields

Field	Description
Filter HTTPS on Port (s) boxes	Enter a port number range on which to filter HTTPS (*n*—*n*). To filter a single port, enter the port number in the first box (or both boxes). By default, the port number is 443 (HTTPS).

Allow Outbound Traffic if URL Server is Not Available check box	Outbound HTTPS connections are not filtered if the URL server is unavailable. Otherwise, no outbound HTTPS traffic is allowed until the server returns.

Do Not Filter HTTPS

Do Not Filter HTTPS allows you specify hosts or networks that should not be filtered. For example, if the host or network you specify is included in a Filter HTTPS rule, then you can create a Do Not Filter HTTPS rule to create an exception. You can place this do not filter rule in any order (before or after the filter rule).

There are no options for this action.

▲

FTP Filtering

The Filter FTP action lets you designate the FTP traffic that is to be filtered by a Websense server. FTP filtering is not supported on N2H2 servers. When a user issues an FTP **get** request to a server, the firewall sends the request to the FTP server and to the Websense server at the same time. If the Websense server permits the connection, the firewall allows the successful FTP return code to reach the user unchanged (for example, a successful return code is 250: CWD command successful). If the Websense server denies the connection, the firewall alters the FTP return code to show that the connection was denied (for example, the firewall changes code 250 to code 550: Directory not found).

Websense only filters FTP **get** commands (and not **put** commands).

Note: Identify the servers you want to use on the System Properties>URL Filtering page.

Note: URL filtering can considerably increase access times to websites when the filtering server is remote from the firewall.

FTP Filtering Option Area Fields

Field	Description
Filter FTP on Port(s) boxes	Enter a port number range on which to filter FTP (*n*—*n*). To filter a single port, enter the port number in the first box (or both boxes). By default, the port number is 21 (FTP).
Allow Outbound Traffic if URL Server is Not Available check box	Outbound FTP connections are not filtered if the URL server is unavailable. Otherwise, no outbound FTP traffic is allowed until the server returns.

Block Outbound Traffic if Absolute FTP Path Is Not Provided check box	Prevents interactive FTP sessions that do not provide the entire directory path. An interactive FTP client is a non-browser client such as the **ftp** command from a DOS prompt or a UNIX shell prompt, or a stand alone FTP client. For example, when you use a web browser for FTP and you browse to a file, the URL for the file includes the entire path. When you use the **ftp** command at the command line, you can change directories without typing the entire path (**cd ./files** instead of **cd /public/files**), in which case the firewall cannot determine your exact location.

Do Not Filter FTP

Do Not Filter FTP allows you specify hosts or networks that should not be filtered. For example, if the host or network you specify is included in a Filter FTP rule, then you can create a Do Not Filter FTP rule to create an exception. You can place this do not filter rule in any order (before or after the filter rule).

There are no options for this action.

Copyright © 2001-2004, Cisco Systems, Inc.

AAA Server Groups

Configuration>System Properties>AAA>AAA Server Groups

The **AAA Server Groups** panel lets you specify up to 14 authentication, authorization, and accounting (AAA) server groups for your network.

Each AAA server group directs different types of traffic to the authentication servers in its group. If the first authentication server listed in the group fails, the firewall seeks authentication from the next server in the group. You can have up to 16 groups and each group can have up to 16 AAA servers for a total of up to 256 AAA servers.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Adding a Server Group
- Deleting a Server Group
- Resetting to Last Applied Settings

Important Notes

- Use the **AAA Servers** panel in the **Configuration>System Properties** tab to add AAA servers to the server groups you define with this panel.
- PIX Firewall listens for RADIUS on ports 1645 and 1646. If your RADIUS server uses ports 1812 and 1813, you will need to reconfigure it to listen on ports 1645 and 1646.

▲

Field Descriptions

The **AAA Server Groups** panel displays the following fields:

- **AAA Server Groups table**
  - **Server Group**—Displays default and user-defined AAA server groups.
  - **Authentication Protocol**—Displays the associated authentication protocol for the group.
- **Add**—Opens the **Add AAA Server Group** dialog box, where you can define a new AAA server group and assign it an authentication protocol.
- **Delete**—Deletes the highlighted AAA server group.
- **RADIUS Server Only**
  - **Ignore authenticator key**—Select this check box to prevent a retransmit caveat message.

    - **Authentication Port**—Enter the port to be used for authentication information.
    - **Accounting Port**—Enter the port to be used for accounting information.
- **Apply**—Applies changes you have made to the firewall.
- **Reset**—Discards any changes without applying them.

Adding a Server Group

Follow these steps to add a server group:

1. In the **AAA Server Groups** panel, click **Add**. The **Add AAA Server Group** dialog box appears.
2. Enter the desired server group name in the **Server Group** box and click TACACS+ or RADIUS.
3. Click **OK** to create the server group.
4. Click **Apply**.

Deleting a Server Group

Follow these steps to delete a server group:

1. In the **AAA Server Groups** panel, select the server group you want to delete in the AAA Server Group table.
2. Click **Delete**. The group is deleted.
3. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

AAA Servers

Configuration>System Properties>AAA>AAA Servers

The **AAA Servers** panel lets you specify which servers handle the authentication, authorization, and accounting (AAA) services for your network. The **AAA Servers** panel displays a list of current AAA servers.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Adding an AAA Server
- Editing an AAA Server
- Deleting an AAA Server
- Resetting to Last Applied Settings

Important Notes

- Before adding an AAA server to a server group, you must first create one or more AAA server groups for your network. Use the **AAA Server Groups** panel in the **Configuration>System Properties** tab to create AAA server groups.

Field Descriptions

The **AAA Server** panel displays the following fields:

- **AAA Server(s) table**
  - **Server Group**—Displays the server group to which the AAA server belongs.
  - **Interface Name**—Displays the interface on which the AAA server resides.
  - **Server IP Address**—Displays the IP address of each AAA server.
  - **Key**—Displays the encryption key for each AAA server. The key is a case-sensitive, alphanumeric keyword of up to 127 characters that is the same value as the key on the TACACS+ server. The key is used between the firewall and server for encrypting data between them. The key must be the same on both the PIX and server systems. Spaces are not permitted in the key, but other special characters are.
  - **Timeout**—Displays the time in seconds that the firewall retries access before choosing the next AAA server. The default is 5 seconds. The maximum time is 30 seconds.
- **Add**—Opens the **Add** dialog box.
- **Edit**—Opens the **Edit** dialog box.

- **Delete**—Deletes the selected item.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Adding an AAA Server

Follow these steps to add an AAA Server:

1. Click **Add**. The **Add AAA Server** dialog box appears.
2. Enter the desired server group, interface name, IP address, key, and timeout value for the new server.
3. Click **OK** to add the server.
4. Click **Apply**.

Editing an AAA Server

Follow these steps to edit an AAA Server:

1. In the **AAA Servers** panel, select the server you want to edit from the AAA Servers table.
2. Click **Edit**. The **Edit AAA Server** dialog box appears.
3. Make the desired changes to the selected server.
4. Click **OK** to modify the server.
5. Click **Apply**.

Deleting an AAA Server

Follow these steps to delete an AAA Server:

1. In the **AAA Servers** panel, select the server you want to delete in the AAA Servers table.
2. Click **Delete**. The server is deleted. Note that you cannot delete the last remaining server in a defined server group.
3. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Advanced AAA Configuration

Configuration>Access Rules>AAA Rules>Advanced AAA Configuration

The **Advanced AAA Configuration** dialog box lets you enable Secure HTTP and the Proxy Limit.

When Secure HTTP is enabled, the firewall authenticates with the HTTP client, such as a browser, using HTTP over SSL (HTTPS), thereby making the password secure. Otherwise, the password is sent in clear text.

When Proxy Limit is enabled, the user authentication session limit is set by specifying the maximum number of concurrent proxy connections.

The following sections are included in this Help topic:

- Field Descriptions
- Enabling Secure HTTP
- Setting the Proxy Limit

Field Descriptions

The **Advanced AAA Configuration** dialog box displays the following fields:

- **Enable Secure HTTP**—Enable this feature to have the firewall authenticate with the HTTP client, such as a web browser, using HTTP over SSL (HTTPS). If you do not enable this feature, the firewall uses HTTP and passwords will be in clear text. This feature is disabled by default.
- **Enable Proxy Limit**—Enable this feature to limit the number of concurrent proxy connections allowed per user. If you disable this feature, no limit is imposed. This feature is enabled by default.
- **Proxy Limit**—When Proxy Limit is enabled, this field specifies the number of concurrent proxy connections allowed. If Proxy Limit is disabled, no limit is used. Values range from 1 to 128. The default value is 16.
- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Enabling Secure HTTP

This feature is disabled by default. Follow these steps to enable HTTP over SSL:

1. In the **Advanced AAA Configuration** dialog box, select the **Enable Secure HTTP** check box.
2. Click **OK**.
3. Click **Apply**.

Note: No data will be encrypted when this feature is enabled if HTTP is not configured.

Setting the Proxy Limit

This feature is enabled by default. Follow these steps to set the Proxy Limit or to disable the feature:

1. To set the Proxy Limit, in the **Advanced AAA Configuration** dialog box **Proxy Limit** connections box, enter a value between 1 and 128.
2. To disable the Proxy Limit, clear the **Enable Proxy Limit** check box. When this feature is disabled, the **Proxy Limit** connections box is also disabled.
3. Click **OK**.
4. Click **Apply**.

Copyright © 2001-2004, Cisco Systems, Inc.

Advanced Access Rule Configuration

Configuration>Access Rules>Access Rules>Advanced Access Rule Configuration

This dialog box allows you to set global ACL logging options. These settings only apply if you enable the newer logging mechanism for the access control entry (ACE, also known as a rule) for the ACL. See **Log Options** for more information.

When you enable logging, if a packet matches the ACE, the firewall creates a flow entry to track the number of packets received within a specific interval (see **Log Options**). The firewall generates a syslog message at the first hit and at the end of each interval, identifying the total number of hits during the interval. At the end of each interval, the firewall resets the hit count to 0. If no packets match the ACE during an interval, the firewall deletes the flow entry.

A large number of flows can exist concurrently at any point of time. To prevent unlimited consumption of memory and CPU resources, the firewall places a limit on the number of concurrent deny flows; the limit is placed only on deny flows (and not permit flows) because they can indicate an attack. When the limit is reached, the firewall does not create a new deny flow until the existing flows expire. If someone initiates a denial of service (DoS) attack, the firewall can create a very large number of deny flows in a very short period of time. Restricting the number of deny-flows prevents unlimited consumption of memory and CPU resources.

Field Descriptions

The **Access Rules>Access Rules>Advanced Access Rule Configuration** dialog box displays the following fields:

Fields	Description
Maximum Deny Flows	The maximum number of deny flows permitted before the firewall stops logging, between 1 and the default value. The default is either 4096, 1024, or 256 depending on the memory of your firewall (> 64 MB, > 16 MB, and <= 16 MB respectively).
Alert Interval	The amount of time (1-3600 seconds) between syslog messages (number 106101) that identify that the maximum number of deny flows was reached. The default is 300 seconds.

Copyright © 2001-2004, Cisco Systems, Inc.

Log Options

Configuration>Access Rules>Access Rules>Log Options

The **Configuration>Access Rules>Access Rules>Log Options** dialog box lets you set logging options for each access control entry (ACE, also called a rule) for an access control list (ACL). Conduits and outbound lists do not support logging. See **Advanced Access Rule Configuration** to set global logging options.

This dialog box lets you use the older logging mechanism (only denied traffic is logged), to use the newer logging mechanism (permitted and denied traffic is logged, along with additional information such as how many packet hits), or to disable logging.

Field Descriptions

The **Configuration>Access Rules>Access Rules>Log Options** dialog box displays the following fields:

Radio Buttons and Buttons	Description
Restore to default logging behavior	Uses the older ACL logging mechanism: the firewall logs syslog message number 106023 when a packet is denied. If you selected the **Enable Logging** checkbox from the **Edit Rule** dialog box, click this radio button to return to the default setting.
Disable logging for the rule	Disables all logging for the ACE.
Enable logging for the rule	Enables the newer ACL logging mechanism: the firewall logs syslog message number 106100 when a packet matches the ACE (either permit or deny). If a packet matches the ACE, the firewall creates a flow entry to track the number of packets received within a specific interval (see the Logging Interval box that follows). The firewall generates a syslog message at the first hit and at the end of each interval, identifying the total number of hits during the interval. At the end of each interval, the firewall resets the hit count to 0. If no packets match the ACE during an interval, the firewall deletes the flow entry.

	Logging Level list	Select the level of logging messages to be sent to the syslog server from this list. Levels are defined as follows: • Emergency (level 0)—The firewall does not use this level. • Alert (level 1, immediate action needed) • Critical (level 2, critical condition) • Error (level 3, error condition) • Warning (level 4, warning condition) • Notification (level 5, normal but significant condition) • Informational (level 6, informational message only) • Debugging (level 7, appears during debugging only)
	Logging Interval box	Set the amount of time in seconds (1-600) the firewall waits before sending the flow statistics to the syslog. This setting also serves as the timeout value for deleting a flow if no packets match the ACE. The default is 300 seconds.
OK	Accepts changes and returns to the previous panel.	
Cancel	Discards changes and returns to the previous panel.	

Copyright © 2001-2004, Cisco Systems, Inc.

Fixup

Configuration>System Properties>Advanced>Fixup

The **Fixup** panel is an informational listing of the services, protocols, and port numbers to which firewall applies the Adaptive Security Algorithm (ASA). The ports listed by default, or those you specify, are the ports at which the firewall listens for each respective service. You can change the port value for each service (except RSH and SIP) by selecting the protocol you want to change from the tree on the left side of the panel.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

Important Notes

The firewall enables fixups based on the following default values:

- FTP (**ftp**) port 21
- H.323 H225 (**h323**) port 1720
- H.323 RAS (**h323**) port 1718-1719
- HTTP (**http**) port 80
- ILS/LDAP (**ILS**) port 389
- RSH (**rsh**) port 514
- RTSP (**rtsp**) port 554
- SIP (**sip**) port 5060
- Skinny (**skinny**) port 2000
- SMTP (**smtp**) port 25
- SNMP (**snmp**) port 161-162
- SQL*Net (**sqlnet**) port 1521
- TFPT (**tftp**) port 69

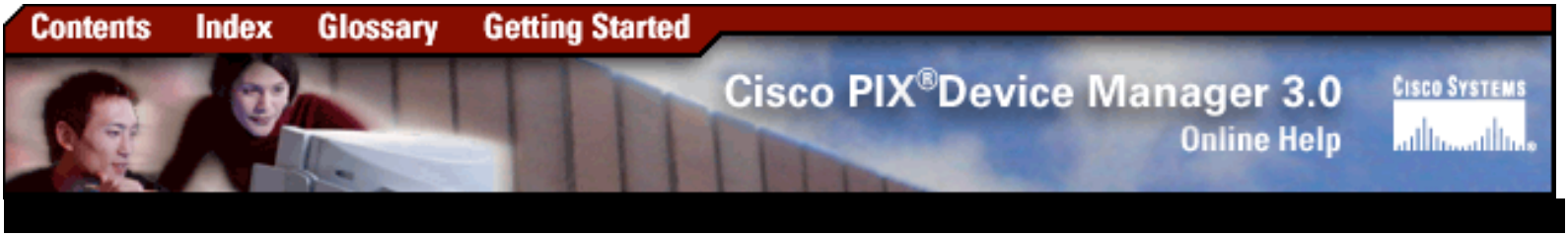
For more information about the protocols used in the **Fixup** panels, see Protocols and the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software. For a list of applications supported by firewalls managed by PDM, see Supported Applications.

Field Descriptions

The **Fixup Summary** panel displays the following fields:

- Fixup Summary table
  - **Protocol**—Displays the services or protocols assigned for fixup.
  - **Port Range**—Lists the lower and upper port number range (if applicable) for the service or protocol.

Copyright © 2001-2004, Cisco Systems, Inc.



FTP

Configuration>System Properties>Advanced>Fixup>FTP

The **FTP** panel lets you enable or disable the firewall to look into the payload of the FTP control channel and apply the Adaptive Security Algorithm (ASA). You can specify the port(s) at which the firewall listens for FTP traffic. FTP fixup is enabled on port 21 by default.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Disabling FTP Fixup
- Enabling FTP Fixup
- Changing the FTP Fixup Port Numbers
- Resetting to Last Applied Settings

Important Notes

The FTP port can be changed; however if you change the default of port 21 to something like 2021, all FTP clients must use port 2021 to send data, and FTP control connections on port 21 will no longer work.

If you disable FTP fixup, internal users can FTP to external servers only in passive mode.

For more information about the protocols used in the **Fixup** panels, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

Field Descriptions

The **FTP** panel displays the following fields:

- **FTP table**
  - **Low Port**—Displays the port number or lower port number range for the FTP fixup.
  - **High Port**—Displays the upper port number range (if applicable) for the FTP fixup.
  - **Strict**—Displays whether the "strict" option (see the **Strict** check box description) is in effect for this FTP fixup.
- **Add**—Opens the **Add** dialog box.
- **Low port**—Enter a port number or lower port number range for addition to the FTP table.

- **High port (optional)**—Enter an upper port number range for addition to the FTP table.
- **Strict**—Select the **Strict** check box to prevent web browsers from sending embedded commands in FTP requests. Each FTP command must be acknowledged before a new command is allowed. Clear the **Strict** check box to allow multiple embedded commands in FTP requests.
- **Delete**—Deletes the selected item.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Disabling FTP Fixup

This feature is enabled by default. Follow these steps to disable FTP fixup:

1. Select any row displayed in the FTP table.
2. Click **Delete**. The port or port range is deleted from the FTP table.
3. Click **Apply**.

Enabling FTP Fixup

Follow these steps to re-enable FTP fixup after it has been disabled:

1. Enter **21** or a lower port number range in the **Low port** box.
2. Enter an upper port number range (if applicable) in the **High port** box.
3. Click **Add**.
4. Repeat Steps 1 through 3 if necessary.
5. Click **Apply**.

Changing the FTP Fixup Port Numbers

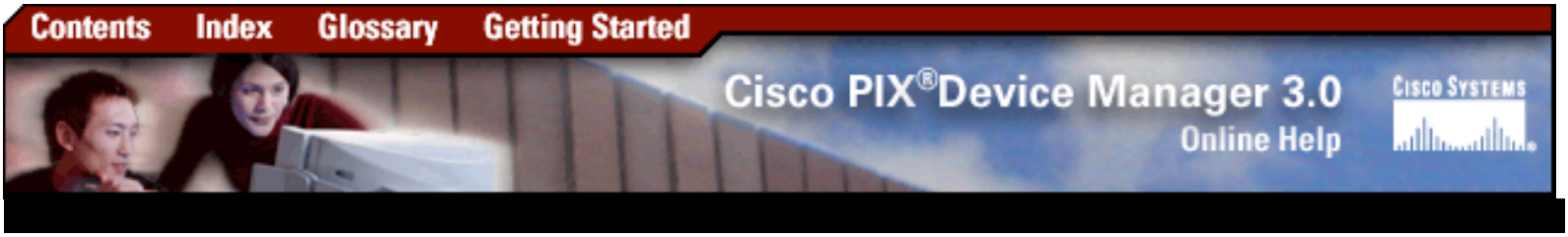
Follow these steps to change the FTP fixup ports:

1. Select the port or port range you want to change in the FTP table.
2. Click **Delete**.
3. Enter a port number or a lower port number range in the **Low port** box.
4. Enter an upper port number range (if applicable) in the **High port** box.
5. Click **Add**.
6. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.



H.323 H225

Configuration>System Properties>Advanced>Fixup>H.323 H225

The **H.323 H225** panel lets you enable or disable the firewall to look into the payload of H.323 signal channels and apply the Adaptive Security Algorithm (ASA). H.323 fixup is enabled for port 1720 by default.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Disabling H.323 Fixup
- Enabling H.323 Fixup
- Changing the H.323 Fixup Port Numbers
- Resetting to Last Applied Settings

Important Notes

H.323 is a suite of protocols defined by the International Telecommunication Union (ITU) for multimedia conferences over LANs. H.323 also supports VoIP gateways and VoIP gatekeepers. The firewall supports H.323 version 2. The H.323 fixup feature provides support for Intel InternetPhone, CU-SeeMe, CU-SeeMe Pro, MeetingPoint, and MS NetMeeting.

For more information about the protocols used in the **Fixup** panels, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

For a list of applications and protocols supported, see IP.

▲

Field Descriptions

The **H.323** panel displays the following fields:

- **H.323 table**
  - **Low Port**—Displays the port number or lower port number range for the H.323 fixups.
  - **High Port**—Displays the upper port number range (if applicable) for the H.323 fixups.
- **Add**—Copies the new entry into the H.323 table.
- **Low Port**—Lets you enter a port number or lower port number range for addition to the H.323 table.

- **High Port (optional)**— Lets you enter an upper port number range for addition to the H.323 table.
- **Delete**—Deletes the selected item.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Disabling H.323 Fixup

This feature is enabled by default. Follow these steps to disable H.323 fixup:

1. Select any row displayed in the H.323 table.
2. Click **Delete**. The port or port range is deleted from the H.323 table.
3. Click **Apply**.

Enabling H.323 Fixup

Follow these steps to re-enable H.323 fixup after it has been disabled:

1. Enter **1720** or a lower port number range in the **Low Port** box.
2. Enter an upper port number range (if applicable) in the **High Port** box.
3. Click **Add**.
4. Repeat steps 1 through 3 if necessary.
5. Click **Apply**.

Changing the H.323 Fixup Port Numbers

Follow these steps to change the H.323 fixup ports:

1. Select the port or port range you want to change in the H.323 table.
2. Click **Delete**.
3. Enter a port number or a lower port number range in the **Low Port** box.
4. Enter an upper port number range (if applicable) in the **High Port** box.
5. Click **Add**.
6. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

HTTP

Configuration>System Properties>Advanced>Fixup>HTTP

The **HTTP** panel lets you enable or disable the firewall to look into the payload of HTTP traffic and apply the Adaptive Security Algorithm (ASA). You can specify the port(s) at which the firewall listens for HTTP traffic. HTTP fixup is enabled for port 80 by default.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Disabling HTTP Fixup
- Enabling HTTP Fixup
- Changing the HTTP Fixup Port Number
- Resetting to Last Applied Settings

Important Notes

For more information about the protocols used in the **Fixup** panels, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

For a list of applications and protocols supported, see IP.

Field Descriptions

The **HTTP** panel displays the following fields:

- **HTTP table**
  - **Low Port**—Displays the port number or lower port number range for the HTTP fixups.
  - **High Port**—Displays the upper port number range (if applicable) for the HTTP fixups.

- **Add**—Copies the new entry into the HTTP table.
- **Low port**—Lets you enter a port number or lower port number range for addition to the HTTP table.
- **High port (optional)**— Lets you enter an upper port number range for addition to the HTTP table.
- **Delete**—Deletes the highlighted row from the HTTP table.

Note: If you disable HTTP fixup, the **filter url** CLI command does not work.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Disabling HTTP Fixup

This feature is enabled by default. Follow these steps to disable HTTP fixup:

1. Select any row displayed in the HTTP table.
2. Click **Delete**.
3. Click **Apply**.

Enabling HTTP Fixup

Follow these steps to re-enable HTTP fixup after it has been disabled:

1. Enter **80** or a lower port number range in the **Low port** box.
2. Enter an upper port number range (if applicable) into the **High port** box.
3. Click **Add**.
4. Repeat steps 1 through 3 if necessary.
5. Click **Apply**.

Changing the HTTP Fixup Port Numbers

Follow these steps to change the HTTP fixup ports:

1. Select the port or port range you want to change in the HTTP table.
2. Click **Delete**.
3. Enter a port number or a lower port number range into the **Low** box.
4. Enter an upper port number range (if applicable) into the **High** box.
5. Click **Add**. The port or port range appears in the HTTP table.
6. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

ILS

Configuration>System Properties>Advanced>Fixup>ILS

The **ILS** (Internet Locator Service) panel lets you enable or disable the firewall to look into the payload of LDAP/ILS traffic and apply the Adaptive Security Algorithm (ASA). You can specify the port(s) at which the firewall listens for ILS traffic. ILS fixup is enabled for port 389 by default.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Disabling ILS Fixup
- Enabling ILS Fixup
- Changing the ILS Fixup Port Number
- Resetting to Last Applied Settings

Important Notes

Internet Locator Service and ILS

The Internet Locator Service (ILS) is based on the Lightweight Directory Access Protocol (LDAP) and is ILSv2 compliant. ILS was developed by Microsoft for use with its NetMeeting, SiteServer, and Active Directory products. For a list of other applications supported by PIX Firewall, see Supported Applications.

You can use the fixup command to change the default port assignment for ILS/LDAP. The default port assignment from 389, but may be specified a a range of port numbers.

PIX Firewall version 6.2 introduces NAT support for ILS, which is used to register and locate endpoints in the ILS or SiteServer Directory. PAT cannot be supported because only IP addresses are stored by an ILS/LDAP database.

For Search Responses, when the ILS/LDAP server is located outside, NAT should be considered to allow internal peers to communicate locally while registered to external ILS servers. For such search responses, xlates will be searched first, and then DNAT entries to obtain the correct address. If both of these searches fail, then the address will not be changed. For sites using NAT 0 (no NAT) and not expecting DNAT interaction, we recommend that the fixup be turned off to provide better performance.

Additional configuration may be necessary when the ILSILS/LDAP server is located inside the firewall border. This would require a hole for outside clients to access the ILSILS/LDAP server on the specified port, typically TCP 389.

LDAP/ILS follows a client/server model with sessions handled over a single TCP connection. Depending on the client's actions, several of these sessions may be created.

During connection negotiation time, a BIND PDU is sent from the client to the server. Once a successful BIND RESPONSE from the server is received, other operational messages may be exchanged (such as ADD, DEL, SEARCH, or MODIFY) to perform operations on the ILS Directory. The ADD REQUEST and SEARCH RESPONSE PDUs may contain IP addresses of NetMeeting peers, used by H.323 (SETUP and CONNECT\messages) to establish the NetMeeting sessions. Microsoft NetMeeting v2.X & 3.X provides ILS support.

The ILS inspection performs the following operations:

- Decodes the LDAP REQUEST/RESPONSE PDUs using the BER decode functions
- Parses the LDAP/ILS packet
- Extracts IP addresses
- Translates IP addresses as necessary
- Encodes the PDU with translated addresses using BER encode functions
- Copies the newly encoded PDU back to the TCP packet
- Performs incremental TCP checksum and sequence number adjustment
- ILS inspection has the following limitations:
- Referral requests and responses are not supported.
- Users in multiple directories are not unified.
- Single users having multiple identities in multiple directories cannot be recognized by NAT

For more information about the protocols used in the fixups, see the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

Field Descriptions

The **ILS** panel displays the following fields:

- **ILS table**
  - **Low Port**—Displays the port number or lower port number range for the ILS fixups.
  - **High Port**—Displays the upper port number range (if applicable) for the ILS fixups.
- **Add**—Copies the new entry into the ILS table.
- **Low port**—Lets you enter a port number or lower port number range for addition to the ILS table.
- **High port (optional)**— Lets you enter an upper port number range for addition to the ILS table.
- **Delete**—Deletes the highlighted row from the ILS table.

Note: If you disable ILS fixup, the **filter url** CLI command does not work.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Disabling ILS Fixup

This feature is enabled by default. Follow these steps to disable ILS fixup:

1. Select any row displayed in the ILS table.
2. Click **Delete**.
3. Click **Apply**.

Enabling ILS Fixup

Follow these steps to re-enable ILS fixup after it has been disabled:

1. Enter **80** or a lower port number range in the **Low port** box.
2. Enter an upper port number range (if applicable) into the **High port** box.
3. Click **Add**.
4. Repeat steps 1 through 3 if necessary.
5. Click **Apply**.

Changing the ILS Fixup Port Numbers

Follow these steps to change the ILS fixup ports:

1. Select the port or port range you want to change in the ILS table.
2. Click **Delete**.
3. Enter a port number or a lower port number range into the **Low** box.
4. Enter an upper port number range (if applicable) into the **High** box.
5. Click **Add**. The port or port range appears in the ILS table.
6. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

RSH

Configuration>System Properties>Advanced>Fixup>RSH

The **RSH** panel lets you enable or disable use of the RSH protocol through the firewall, and specify the port at which the firewall listens for RSH traffic. RSH is enabled for port 514 in the firewall default configuration.

The **RSH** panel lets you enable or disable the firewall to look into the payload of RSH traffic and apply the Adaptive Security Algorithm (ASA). You can specify the port at which the firewall listens for RSH traffic. RSH fixup is enabled for port 514 by default.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Disabling RSH Fixup
- Enabling RSH Fixup
- Resetting to Last Applied Settings

Important Notes

For more information about the protocols used in the **Fixup** panels, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

For a list of applications and protocols supported, see IP.

Field Descriptions

The **RSH** panel displays the following fields:

- **Enable**—Enables RSH fixup for a Cisco firewall unit. Clearing this check box disables RSH fixup.
- **Port**—Specifies port 514 as the port at which the firewall listens for RSH traffic.

Note: The **rsh** port number cannot be changed.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Disabling RSH Fixup

This feature is enabled by default. Follow these steps to disable RSH fixup:

1. In the **RSH** panel, select the **Enable** check box.
2. Click **Apply**.

Enabling RSH Fixup

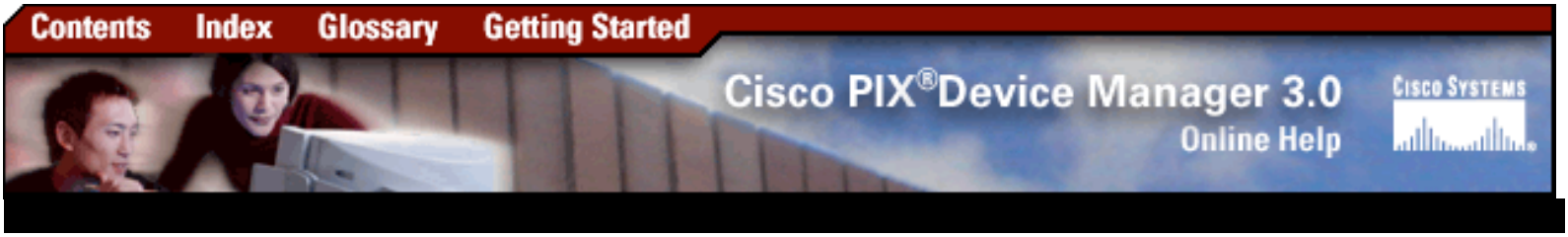
Follow these steps to re-enable RSH fixup after it has been disabled:

1. In the **RSH** panel, click the **Enable** check box.
2. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.



RTSP

Configuration>System Properties>Advanced>Fixup>RTSP

The **RTSP** panel lets you enable or disable the firewall to look into the payload of the Real Time Streaming Protocol (RTSP) signal channel and apply the Adaptive Security Algorithm (ASA). You can specify the port(s) at which the firewall listens for RTSP traffic. RTSP fixup is enabled for port 554 by default.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Disabling RTSP Fixup
- Enabling RTSP Fixup
- Changing the RTSP Fixup Port Number
- Resetting to Last Applied Settings

Important Notes

RTSP is used by RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer, and Cisco IP/TV connections. PIX Firewall does not support multicast RTSP. For a list of other applications and protocols supported, see **more IP**.

For more information about the protocols used in the **Fixup** panels, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

For a list of applications and protocols supported, see IP.

▲

Field Descriptions

The **RTSP** panel displays the following fields:

RTSP table

- **Low Port**—Displays the low port number for the RTSP fixup. 554 is the default value.
- **High Port**—Displays the high port number for the RTSP fixup.
- **Add**—Copies the specified port value into the RTSP table.
- **Port**—Lets you enter a port number for addition to the RTSP table.

- **Delete**—Deletes the highlighted row from the RTSP table.
- **Add parameters for URL Filtering**
- **Reset**—Discards any changes without applying them.

Disabling RTSP Fixup

This feature is enabled by default. Follow these steps to disable RTSP fixup:

1. Select the port number you want to disable in the RTSP table.
2. Click **Delete**.
3. Click **Apply**.

Enabling RTSP Fixup

Follow these steps to re-enable RTSP fixup after it has been disabled:

1. Enter a port number in the **High Port** or **Low Port**. 554 is the default.
2. Click **Add**. The port appears in the RTSP table.
3. Repeat Steps 1 and 2 if necessary.
4. Click **Apply**.

Changing the RTSP Fixup Port Numbers

Follow these steps to change the RTSP fixup ports:

1. Select the port number you want to change in the RTSP table.
2. Click **Delete**.
3. Enter a port number in the **High Port** or **Low Port**.
4. Click **Add**. The port appears in the RTSP table.
5. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

SIP

Configuration>System Properties>Advanced>Fixup>SIP

The **SIP** panel lets you add or delete port(s) on which the firewall listens for Session Initiation Protocol SIP over TCP traffic, and enable SIP on the UDP port. SIP over TCP fixup is enabled on port 5060 by default. For SIP over TCP, you can change the default or add additional ports to match the configuration of an end point device. With SIP over UDP enabled, the firewall processes packets originating from or destined to the SIP UDP port, and the packets are either dropped or accepted based on the configuration of this feature. The firewall uses SIP to support Voice over IP (VoIP) gateways and VoIP proxy servers.

Some applications require special handling by the firewall application inspection function, or "fixup." Applications that require special application inspection functions are those that embed IP address information in the user data packet or open secondary channels on dynamically assigned ports, or both.

To support SIP, SIP fixup inspects the signaling messages, NATs the appropriate embedded IP addresses, and opens the negotiated media connections. While the signaling is sent over a well-known destination port (UDP/TCP 5060), the media streams are allocated dynamically. SIP is a text-based protocol that embeds IP addresses throughout the text. The application inspection function works with NAT to locate and translate these embedded addresses.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Adding SIP Over TCP Ports
- Deleting SIP Over TCP Ports
- Enabling SIP Over UDP
- Disabling SIP Over UDP

Important Notes

For more information about the protocols used in the **Fixup** panels, refer to the *Cisco PIX Firewall and VPN Configuration Guide*.

For a list of applications and protocols supported, see IP.

Field Descriptions

The **SIP** panel displays the following fields:

SIP table

- **Low Port**—Specifies the lowest numbered port on which the firewall listens for SIP over TCP traffic.
- **High Port**—Specifies highest numbered port on which the firewall listens for SIP over TCP traffic.
- **Enable SIP over UDP**—Select to enable SIP over UDP.
- **Enable IP address privacy**—Select so SIP fixup will retain the outside IP addresses in the SIP header and SDP data of inbound SIP packets. Note that when this is enabled, outside NAT will not work.
- **Add**—Copies the specified port numbers into the SIP table.
- **Delete**—Deletes the highlighted row from the SIP table.

Adding SIP Over TCP Ports

Follow these steps:

1. Enter a low port number in the **Low Port** box.
2. Enter an optional high port number in the **High Port** box. The high port number must be greater than the number you entered in the **Low Port** box.
3. Click **Add**.

Deleting SIP Over TCP Ports

Follow these steps:

1. Select the port(s) to delete. You can select only one row at a time.
2. Click **Delete**.

Enabling SIP Over UDP

To enable the firewall to accept packets originating from or destined to the SIP UDP port (5060), select the **Enable SIP over UDP** check box.

Disabling SIP Over UDP

SIP over UDP fixup is enabled on port 5060 by default. Disable SIP over UDP fixup if the end points in your network do not use SIP or if port 5060 is already being used. To disable the firewall to accept packets originating from or destined to the SIP UDP port, clear the **Enable SIP over UDP** check box.

Copyright © 2001-2004, Cisco Systems, Inc.

Skinny

Configuration>System Properties>Advanced>Fixup>Skinny

The **Skinny** panel lets you enable or disable the firewall to look into the payload of Skinny signal channel and apply the Adaptive Security Algorithm (ASA). You can specify the port(s) at which the firewall listens for Skinny traffic. Skinny fixup is enabled for port 2000 by default.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Disabling Skinny Fixup
- Enabling Skinny Fixup
- Changing the Skinny Fixup Port Number
- Resetting to Last Applied Settings

Important Notes

For more information about the protocols used in the **Fixup** panels, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

For a list of applications and protocols supported, see IP.

Field Descriptions

The **Skinny** panel displays the following fields:

- **Skinny table**
  - **Low Port**—Displays the port number or lower port number range for the Skinny fixup. The default is **2000**.
  - **High Port**—Displays the upper port number range (if applicable) for the Skinny fixup.
- **Add**—Copies the **Low** and **High** port values into the Skinny table.
- **Low port**—Lets you enter a port number or lower port number range for addition to the Skinny table.
- **High port (optional)**—Lets you enter an upper port number range for addition to the Skinny table.
- **Delete**—Deletes the selected item.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use

the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Disabling Skinny Fixup

This feature is enabled by default. Follow these steps to disable Skinny fixup:

1. Select the row you want to delete in the Skinny table.
2. Click **Delete**.
3. Click **Apply**.

Enabling Skinny Fixup

Follow these steps to re-enable Skinny fixup after it has been disabled:

1. Enter **2000** or a lower port number range in the **Low port** box.
2. Enter an upper port number range (if applicable) in the **High port** box.
3. Click **Add**.
4. Repeat Steps 1 through 3 if necessary.
5. Click **Apply**.

Changing the SKINNY Fixup Port Numbers

Follow these steps to change the Skinny fixup ports:

1. Select the port or port range you want to change in the Skinny table.
2. Click **Delete**.
3. Enter a port number or a lower port number range in the **Low port** box.
4. Enter an upper port number range (if applicable) in the **High port** box.
5. Click **Add**. The port or port number range appears in the Skinny table.
6. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

SMTP

Configuration>System Properties>Fixup>SMTP

The **SMTP** panel lets you enable or disable the firewall to look into the payload of SMTP traffic and apply the Adaptive Security Algorithm (ASA). You can specify the port(s) at which the firewall listens for SMTP traffic. SMTP fixup is enabled for port 25 by default.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Disabling SMTP Fixups
- Enabling SMTP Fixups
- Changing the SMTP Fixup Port Number
- Resetting to Last Applied Settings

Important Notes

SMTP fixup enables the Mail Guard feature, which limits mail servers to the HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT commands. All other commands are rejected.

For more information about the protocols used in the **Fixup** panels, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

For a list of applications and protocols supported, see IP.

Field Descriptions

The **SMTP** panel displays the following fields:

- **SMTP table**
  - **Low Port**—Displays the port number or lower port number range for the SMTP fixup. The default is **25**.
  - **High Port**—Displays the upper port number range (if applicable) for the SMTP fixup.
- **Add**—Copies the new entry into the SMTP table.
- **Low**—Lets you enter a port number or lower port number range for addition to the SMTP table.

- **High**—(optional) Lets you enter an upper port number range for addition to the SMTP table.
- **Delete**—Deletes the selected item.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Disabling SMTP Fixup

This feature is enabled by default. Follow these steps to disable SMTP fixup:

1. Select the port number you want to disable in the SMTP table.
2. Click **Delete**.
3. Click **Apply**.

Enabling SMTP Fixup

Follow these steps to re-enable SMTP fixup after it has been disabled:

1. Enter **25** or a lower port number range into the **Low port** box.
2. Enter an upper port number range (if applicable) into the **High port** box.
3. Click **Add**.
4. Repeat Steps 1 through 3 if necessary.
5. Click **Apply**.

Changing the SMTP Fixup Port Numbers

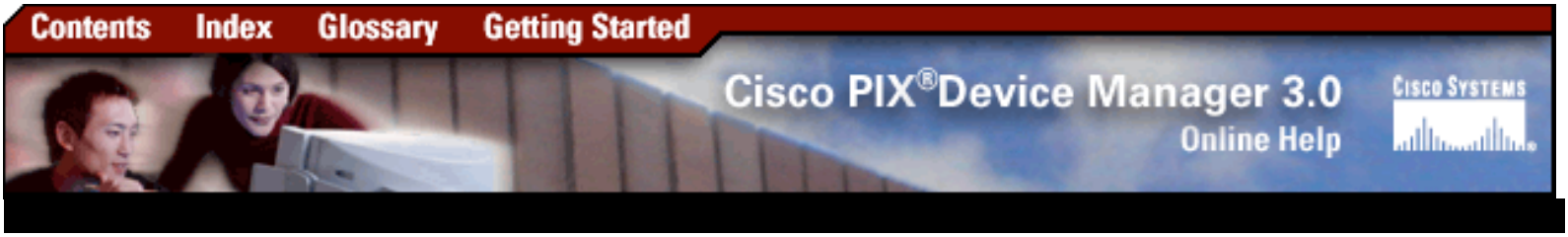
Follow these steps to change the SMTP fixup ports:

1. Select the port or port range you want to change in the SMTP table.
2. Click **Delete**.
3. Enter a port number or a lower port number range into the **Low port** box.
4. Enter an upper port number range (if applicable) into the **High port** box.
5. Click **Add**. The port or port range appears in the SMTP table.
6. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.



SNMP

Configuration>System Properties>Fixup>SNMP

The SNMP fixup allows the firewall to be configured to drop SNMP packets based on the protocol version. The protocol versions can be 1, 2, 2c or 3. This fixup is disabled by default.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Enabling SNMP Fixup
- Disabling SNMP Fixup
- Resetting to Last Applied Settings

Important Notes

For more information about the protocols used in the **Fixup** panels, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

▲

Field Descriptions

The **SNMP** panel displays the following fields:

- **SNMP table**
  - **Protocols**—Displays the protocols available for the SNMP fixup.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

▲

Enabling SNMP Fixup

This feature is disabled by default. Follow these steps to enable SNMP fixup:

1. Select the port number to be enabled in the SNMP table.
2. Click **Apply**.

Disabling SNMP Fixup

Follow these steps to disable SNMP fixup after it is enabled:

1. Deselect the protocol to be disabled.
2. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

SQL*Net

Configuration>System Properties>Fixup>SQL*Net

The **SQL*Net** panel lets you enable or disable the firewall to look into the payload of SQL*Net traffic and apply the Adaptive Security Algorithm (ASA). You can specify the port(s) at which the firewall listens for SQL*Net traffic. SQL*Net fixup is enabled for port 1521 by default. Port 1521 is the default port used by Oracle for SQL*Net; however, this value does not agree with IANA port assignments.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Disabling SQL*Net Fixup
- Enabling SQL*Net Fixup
- Changing the SQL*Net Fixup Port Number
- Resetting to Last Applied Settings

Important Notes

For more information about the protocols used in the **Fixup** panels, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

For a list of applications and protocols supported, see IP.

Field Descriptions

The **SQL*Net** panel displays the following fields:

- **SQL*Net table**
  - **Low Port**—Displays the port number or lower port number range for the SQL*Net fixup.
  - **High Port**—Displays the upper port number range (if applicable) for the SQL*Net fixup.
- **Add**—Copies the new entry into the SQL*Net table.
- **Low port**—Lets you enter a port number or lower port number range for addition to the SQL*Net table.
- **High port (optional)**— Lets you enter an upper port number range for addition to the SQL*Net table.
- **Delete**—Deletes the highlighted row from the SQL*Net table.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use

the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Disabling SQL*Net Fixup

This feature is enabled by default. Follow these steps to disable SQL*Net fixup:

1. Select the port number to be disabled in the SQL*Net table.
2. Click **Delete**.
3. Click **Apply**.

Enabling SQL*Net Fixup

Follow these steps to re-enable SQL*Net fixup after it is disabled:

1. Enter **1521** or a lower port number range in the **Low port** box.
2. Enter an upper port number range (if applicable) in the **High port** box.
3. Click **Add**.
4. Repeat Steps 1 through 3 if necessary.
5. Click **Apply**.

Changing the SQL*Net Fixup Port Numbers

Follow these steps to change the SQL*Net fixup ports:

1. Select the port or port range you want to change in the SQL*Net table.
2. Click **Delete**.
3. Enter a port number or a lower port number range in the **Low port** box.
4. Enter an upper port number range (if applicable) in the **High port** box.
5. Click **Add**. The port or port number range appears in the SQL*Net table.
6. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

TFTP

Configuration>System Properties>Advanced>Fixup>TFTP

The **TFTP** panel lets you enable or disable the firewall to look into the payload of TFTP packets and apply the Adaptive Security Algorithm (ASA). You can specify the port(s) at which the firewall listens for TFTP traffic. TFTP fixup is enabled on port 69 by default.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Disabling TFTP Fixup
- Enabling TFTP Fixup
- Changing the TFTP Fixup Port Numbers
- Resetting to Last Applied Settings

Important Notes

The TFTP port can be changed; however if you change the default of port 69 to something like 2069, all TFTP clients must use port 2069 to send data, and TFTP control connections on port 69 will no longer work.

For more information about the protocols used in the **Fixup** panels, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

Field Descriptions

The **TFTP** panel displays the following fields:

- **TFTP table**
  - **Low Port**—Displays the port number or lower port number range for the TFTP fixup.
  - **High Port**—Displays the upper port number range (if applicable) for the TFTP fixup.
  - **Strict**—Displays whether the "strict" option (see the **Strict** check box description) is in effect for this TFTP fixup.
- **Add**—Opens the **Add** dialog box.
- **Low port**—Enter a port number or lower port number range for addition to the TFTP table.
- **High port (optional)**—Enter an upper port number range for addition to the TFTP table.
- **Strict**—Select the **Strict** check box to prevent web browsers from sending embedded commands in TFTP

requests. Each TFTP command must be acknowledged before a new command is allowed. Clear the **Strict** check box to allow multiple embedded commands in TFTP requests.

- **Delete**—Deletes the selected item.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Disabling TFTP Fixup

This feature is enabled by default. Follow these steps to disable TFTP fixup:

1. Select any row displayed in the TFTP table.
2. Click **Delete**. The port or port range is deleted from the TFTP table.
3. Click **Apply**.

Enabling TFTP Fixup

Follow these steps to re-enable TFTP fixup after it has been disabled:

1. Enter **69** or a lower port number range in the **Low port** box.
2. Enter an upper port number range (if applicable) in the **High port** box.
3. Click **Add**.
4. Repeat Steps 1 through 3 if necessary.
5. Click **Apply**.

Changing the TFTP Fixup Port Numbers

Follow these steps to change the TFTP fixup ports:

1. Select the port or port range you want to change in the TFTP table.
2. Click **Delete**.
3. Enter a port number or a lower port number range in the **Low port** box.
4. Enter an upper port number range (if applicable) in the **High port** box.
5. Click **Add**.
6. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Fragment

Configuration>System Properties>Advanced>Fragment

The **Fragment** panel lets you configure the IP fragment database for each interface of your firewall.

The following sections are included in this Help topic:

- Field Descriptions
- Changing Fragment Parameters
- Resetting to Last Applied Settings

Field Descriptions

The **Fragment** panel displays the following fields:

- **Fragment table**
  - **Interface Name**—List of the available interfaces on the firewall.
  - **Size**—Number of records in the fragment database for that interface. Default is 200.
  - **Chain Length**—Maximum number of elements allowed in a fragment set. Default is 24 fragments.
  - **Timeout**—Maximum number of seconds allowed to assemble a fragment set. Default is 5 seconds.
- **Edit**—Opens the **Edit** dialog box.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.
- **Show Fragment**—Displays the current fragment database statistics for each interface on the firewall.

Changing Fragment Parameters

Follow these steps to modify the fragment database parameters for a firewall interface:

1. Select the desired interface in the Fragment table and click **Edit**.
2. In the **Edit Fragment** dialog box, change the **Size**, **Chain**, and **Timeout** values as desired, and click **OK**. If

you make a mistake, click **Restore Defaults** to return to the original values.

3. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

ICMP

Configuration>System Properties>Administration>ICMP

The **ICMP** panel lets you configure rules that permit only specific hosts or networks to communicate with the firewall using the Internet Control Message Protocol (ICMP).

The following sections are included in this Help topic:

- Field Descriptions
- Adding Rules
- Editing Rules
- Deleting Rules
- Applying Changes

The ICMP protocol enables a network device to *ping* an IP address in order to discover the presence, identity, and function of other devices and to test intermediate communications links. When a device receives a ping (request), it can respond with an *echo* which includes its name, function, and other information. Routers can discover each other in this way. Administrators also use ping directly in network management applications and diagnostic tools, such as the Tools>Ping menu item in PDM.

The ICMP panel can enable or disable the ping response or echo of an interface on the firewall. When pinging is disabled, the firewall cannot be detected by other devices or software applications. However, "friendly" hosts, such as a PC running PDM or neighboring router may need to ping the firewall. This feature is also referred to as configurable proxy pinging.

The rule table configures an access-list command statement that permits or denies ICMP traffic terminating at the firewall unit. A permit or deny action is specified for each interface which is added to the rule table. If no interfaces are added to the rule table, the default action for each interface is to permit ICMP traffic.

When an interface receives an ICMP packet, the firewall searches the access list. If the first matched entry is a permit entry, the ICMP packet continues to be processed. If the first matched entry is a deny entry or an entry is not matched, firewall discards the ICMP packet and generates the %PIX-3-313001 syslog message. An exception is when an ICMP access-list command statement is not configured; then, permit is assumed.

Cisco recommends that you grant permission for ICMP unreachable message type (type 3). Denying ICMP unreachable messages disables ICMP Path MTU discovery, which can halt IPSec and PPTP traffic. See RFC 1195 and RFC 1435 for details about Path MTU Discovery.

Field Descriptions

The **Internet Control Message Protocol** (ICMP) panel displays the following fields in a rule table:

- **Interface**—Displays an interface which has been added to the ICMP rule table (access list).
- **Action**—Permit or deny ICMP traffic terminating at the firewall unit through this interface.
- **IP Address**—Displays the IP address of each host or network added to the ICMP rule table (access list) for this interface. Note: This is not the IP address of the firewall interface.
- **Netmask**—Displays the netmask for the IP address of each host or network added to the ICMP rule table (access list) for this. Note: This is not a netmask for the IP address of the firewall interface.
- **ICMP Type**—The type of ICMP packet to which the permit or deny action will be applied.
    - 0 echo-reply
    - 3 unreachable
    - 4 source-quench
    - 5 redirect
    - 6 alternate-address
    - 8 echo
    - 9 router-advertisement
    - 10 router-solicitation
    - 11 time-exceeded
    - 12 parameter-problem
    - 13 timestamp-reply
    - 14 timestamp-request
    - 15 information-request
    - 16 information-reply
    - 17 mask-request
    - 18 mask-reply
    - 31 conversion-error
    - 32 mobile-redirect

- **Add**—Opens the **Add** dialog box.
- **Edit**—Opens the **Edit** dialog box.
- **Delete**—Deletes the selected item.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Adding Rules

Follow these steps to add to the rule table:

1. Click **Add** to open the **Add** dialog box.

2. Select the **ICMP Type.**
3. Select an **Interface**.
4. Enter or edit the **IP address** which will be permitted or denied ICMP access through this interface.
5. If the IP address is a host, not a network, then select **Host**.
6. Select or enter a **Mask** for the IP address.
7. Select **permit** or **deny** for the **Action.**
8. To return to the previous panel click:
    - **OK**—Accepts changes and returns to the previous panel.
    - **Cancel**—Discards changes and returns to the previous panel.
    - **Help**—Provides more information.

Editing Rules

Follow these steps to edit the rule table:

1. Click **Edit** the **Edit** dialog box.
2. Select the **ICMP Type.**
3. Select an **Interface**.
4. Enter or edit the **IP address** which will be permitted or denied ICMP access through this interface.
5. If the IP address is a host, not a network, then select **Host**.
6. Select or enter a **Mask** for the IP address.
7. Select **permit** or **deny** for the **Action.**
8. To return to the previous panel click:
    - **OK**—Accepts changes and returns to the previous panel.
    - **Cancel**—Discards changes and returns to the previous panel.
    - **Help**—Provides more information.

    .

Deleting Rules

Follow these steps to delete a rule from the table:

1. Select a line item in the rule table.
2. Click **Delete**.

Applying Changes

Changes to the table made by **Add**, **Edit**, or **Delete** are not immediately applied to the running configuration. You must click on one of the following buttons to apply or discard changes:

1. **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use

the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

2. **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Auto Update

Configuration>System Properties>Auto Update

The **Auto Update** panel lets you configure the firewall to be managed remotely from a server that supports the Auto Update specification. Auto Update lets you apply configuration changes to the firewall and receive software updates from a remote location.

Auto Update is useful in solving many of the challenges facing administrators for firewall management:

- Overcomes dynamic addressing and NAT challenges
- Gives ability to commit configuration changes in one atomic action
- Provides a reliable method for updating software
- Leverages well understood methods for high scalability
- Open interface gives developers tremendous flexibility
- Simplifies security solutions for Service Provider environments
- High reliability, rich security/management features, broad support by many products

---

The following sections are included in this Help topic:

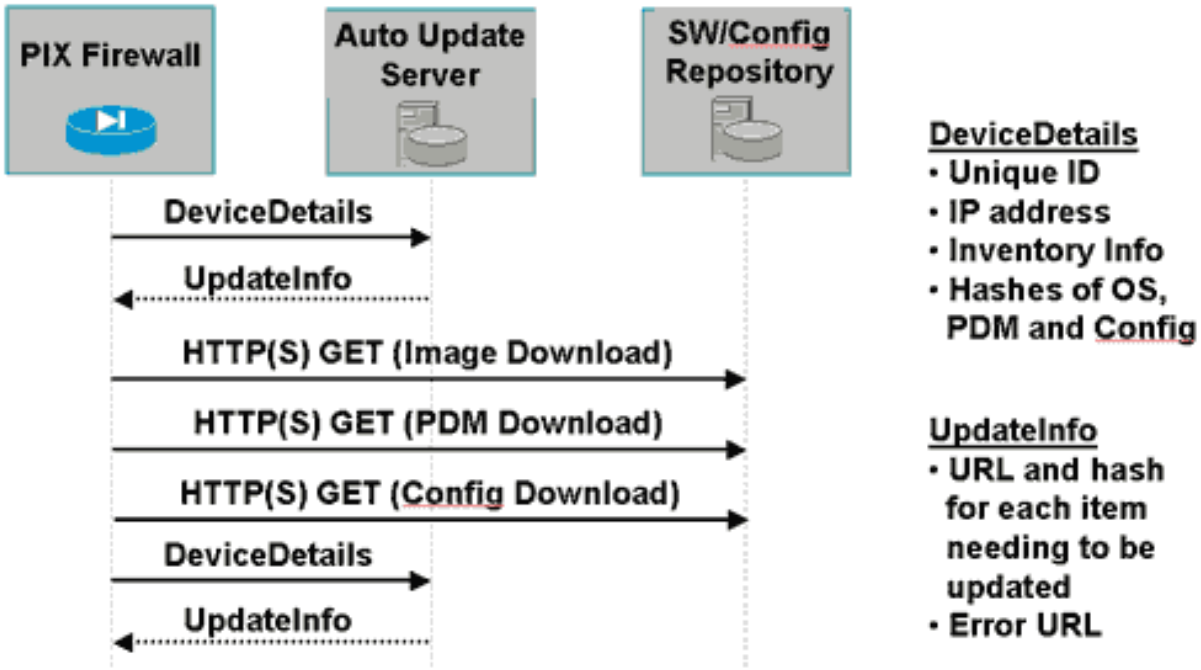
- Introduction to Auto Update
- Important Notes
- Field Descriptions
- Applying Changes
- Troubleshooting

Introduction to Auto Update

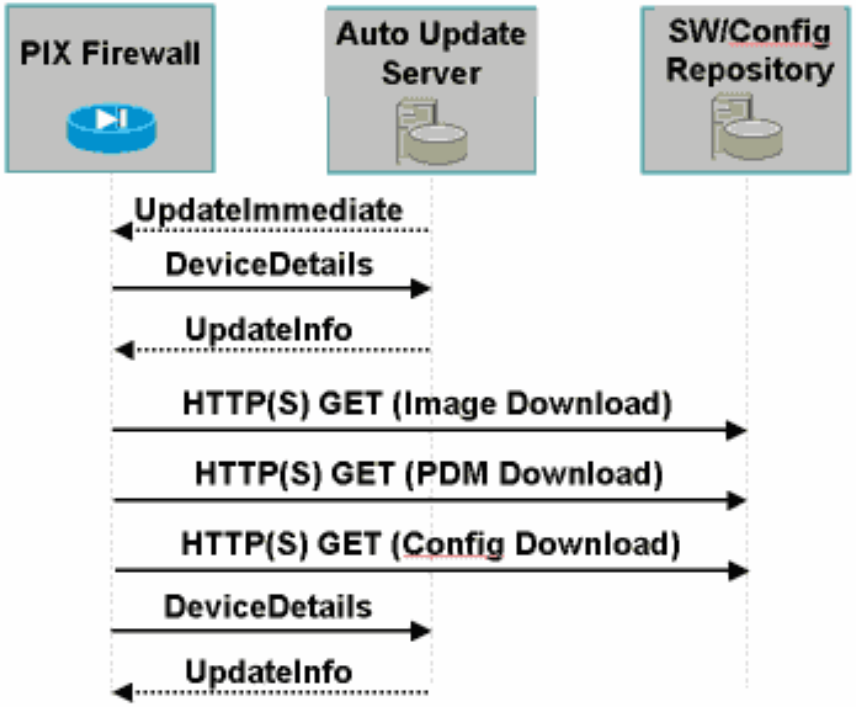
The Auto Update specification provides the infrastructure necessary for remote management applications to download firewall configurations, software Images, and to perform basic monitoring from a centralized location. This specification is used by the Auto Update feature in PDM 2.0 and higher and PIX MDC 1.0.

The Auto Update specification allows the Auto Update server to either push configuration information and send requests for information to the firewall, or to pull configuration information by causing the firewall to periodically poll the Auto Update server. The Auto Update server can also send a command to the firewall to send an immediate polling request at any time. Communication between the Auto Update server and the firewall requires a communications path and local CLI configuration on each firewall.

Auto Update Pull



Auto Update Push



The Auto Update feature on the firewall can be used with products such as the Cisco Secure Policy Manager, as well as third-party companies that want to manage the firewall.

▲

Important Notes

- If the firewall configuration is updated from an Auto Update Server, PDM is not notified. You must click **Refresh** or **File>Refresh PDM with the Running Configuration on the Firewall** to get the latest configuration, and any changes to the configuration made in PDM will be lost.
- If HTTPS is chosen as the protocol to communicate with the Auto Update Server, the firewall will use SSL. This requires the firewall to have a DES or 3DES license. License information is available from **About Cisco PIX Firewall**.

Field Descriptions

The **Auto Update** panel displays the following fields:

- **Enable Auto Update Support**—Select to enable the firewall to be configurable from an Auto Update Server.

HTTP(S) server—Lets you configure the location of the Auto Update Server.

- **Verify Certificate**—Select to verify the certificate returned by the Auto Update Server will be checked against the Certificate Authority (CA) root certificates. This requires that the Auto Update Server and the firewall use the same CA.
- **Protocol**—Select the protocol the Auto Update Server will use to communicate with the firewall. The choices are **http** and **https**.
- **Server**—The name or IP address of the Auto Update Server. Specify the name only if the firewall can resolve hostnames.
- **User Name (Optional)**—Enter the user name needed to access the Auto Update Server.
- **Port**—Specifies the port to contact on the Auto Update Server. It will default to TCP port 80 for http and TCP port 443 for https.
- **Path**—Enter the path on the Auto Update Server.
- **Interface**—Select the interface with the Auto Update Server.
- **Password (Optional)**—Enter the user password for the Auto Update Server.
- **Confirm Password (Optional)**—Reenter the user password for the Auto Update Server.

Timeout—Lets you set the amount of time the firewall will wait for the Auto Update Server to timeout.

- **Enable Timeout Period**—Check to enable the firewall to timeout if no response is received from the Auto Update Server.
- **Timeout Period (Minutes)**—Enter the number of minutes the firewall will wait to timeout if no response is received from the Auto Update Server.

Polling Parameters—Lets you configure how often the firewall will poll for information from the Auto Update Server.

- **Polling Period (minutes)**—The number of minutes the firewall will wait to poll the Auto Update Server for new information.
- **Retry Period (minutes)**—The number of minutes the firewall will wait to poll the Auto Update Server for

new information if the attempt to poll the server fails.

- **Retry Count**—The number of times the firewall will attempt to retry to poll the Auto Update Server for new information.
- **Advanced**— Displays Advanced Auto Update Properties.
  - **Use Device ID**—Enables authentication using a Device ID. The Device ID is used to uniquely identify the firewall to the Auto Update Server.
  - **Device ID**—Type of Device ID to use.
    - **Hostname**—The name of the host.
    - **Serial Number**—Device serial number.
    - **IP Address on**—The IP address of the selected interface, used to uniquely identify the firewall to the Auto Update Server.
    - **MAC Address on**—The MAC address of the selected interface, used to uniquely identify the firewall to the Auto Update Server.
    - **User Input**—A unique user ID.

Applying Changes

Changes to the table made to the **Auto Update** panel are not immediately applied to the running configuration. You must click on one of the following buttons to apply or discard changes:

1. **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
2. **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Troubleshooting Auto Update Configuration

Tools>CLI provides access to the command line interface. These CLI commands will aid in troubleshooting your Auto Update configuration.

View (show command)

To display the Auto-Update server, poll time, timeout period, device ID, poll statistics and update statistics, enter the **show auto-update** command.

The following is sample output from the **show auto-update** command:

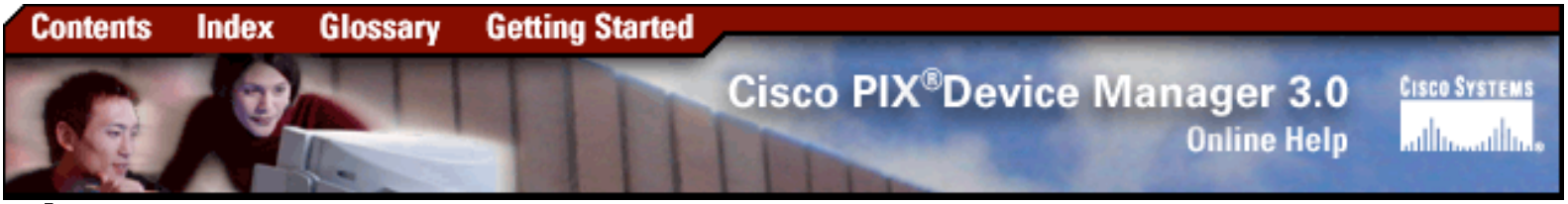
```
show auto-update
           Server: https://********@172.23.58.115:1742/management.cgi?1276
```

```
        Certificate will be verified
        Poll period: 720 minutes, retry count: 2, retry period: 5 minutes
        Timeout: none
        Device ID: host name [jeffryp-pix-pri]
        Next poll in 4.93 minutes
        Last poll: 11:36:46 PST Tue Nov 13 2001
        Last PDM update: 23:36:46 PST Tue Nov 12 2001
```

Remove (clear command)

To remove the entire Auto Update configuration, enter the **clear auto-update** command.

Copyright © 2001-2004, Cisco Systems, Inc.



Timeout

Configuration>System Properties>Advanced>Timeout

The **Timeout** panel lets you set the timeout durations for use with the firewall. All durations are displayed in the format `hh:mm:ss`.

The **timeout** option sets the idle time for the connection and translation slots of various protocols. If the slot has not been used for the idle time specified, the resource is returned to the free pool. TCP connection slots are freed approximately 60 seconds after a normal connection close sequence.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Specifying the Timeout Duration
- Resetting to Last Applied Settings

Important Notes

- We recommend that you do not change these values unless advised to do so by Customer Support.
- In all cases, except for **Authorization absolute** and **Authorization inactivity**, disabling the field means there is no timeout value. For those two cases, disabling the field means to reauthenticate on every new connection.
- For more information about timeout values, refer to the *Cisco PIX Firewall Command Reference* for your version of software.

Field Descriptions

Timeouts displays the following fields:

- **Connection**—Modifies the idle time until a connection slot is freed. Enter `0:0:0` to disable timeout for the connection. This duration must be at least 5 minutes. The default is **1 hour**.
- **H.225**—Modifies the idle time until an H.225 service connection closes. The H.225 default timeout is **1 hour** (`01:00:00`). Setting the value of `00:00:00` means never close this connection. To close this connection immediately after all calls are cleared, a value of 1 second (`00:00:01`) is recommended.
- **H.323**—Modifies the idle time until an H.323 service connection closes. This duration must be at least 5

minutes. The default is **5 minutes**. Enter `0:0:0` to disable timeout.

- **SIP**—Modifies the idle time until an SIP signalling port connection closes. The default is **30 minutes**. Enter `0:0:0` to disable timeout.
- **SIP Media**—Modifies the idle time until an SIP media port connection closes. The default is **2 minutes**. Enter `0:0:0` to disable timeout.
- **MGCP**—Modifies the timeout value for MGCP which represents the idle time after which MGCP media ports are closed. The MGCP default timeout is **5 minutes** (`00:05:00`). Enter `0:0:0` to disable timeout.
- **Authorization absolute**—Modifies the duration until the authentication and authorization cache times out and you have to reauthenticate a new connection. This duration must be shorter than the **Translation Slot** value. The system waits to reprompt you until you start a new connection, such as clicking a link in a web browser. Enter `0:0:0` to disable caching and reauthenticate on every new connection.

Note: Do not set this value to **`0:0:0`** if passive FTP is used on the connections.

- **Authorization inactivity**—Modifies the idle time until the authentication and authorization cache times out and users have to reauthenticate a new connection. This duration must be shorter than the **Translation Slot** value.
- **Half-closed**—Modifies the idle time until a TCP half-closed connection closes. The minimum is 5 minutes. The default is **10 minutes**. Enter `0:0:0` to disable timeout for a half-closed connection.
- **Translation Slot**—Modifies the idle time until a translation slot is freed. This duration must be at least 1 minute. The default is **3 hours**. Enter `0:0:0` to disable timeout.
- **UDP**—Modifies the idle time until a UDP protocol connection closes. This duration must be at least 1 minute. The default is **2 minutes**. Enter `0:0:0` to disable timeout.
- **RPC**—Modifies the idle time until an RPC slot is freed. This duration must be at least 1 minute. The default is **10 minutes**. Enter `0:0:0` to disable timeout.
- **SIP Disconnect**—This timeout value indicates the maximum time the PIX Firewall will wait for the 200 OK response for a CANCEL or a BYE message. If the 200 OK message is not received before the timer expires, then the media connections for that call will be deleted. The default value is two minutes .This field is only available if you are running Cisco PIX Firewall version 6.3(5).
- **SIP Invite**—This timeout value indicates the maximum time the pin holes are kept opened by the INVITE message if the Expires header is missing. The default value is three minutes. This field is only available if you are running Cisco PIX Firewall version 6.3(5).

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Specifying the Timeout Duration

Follow these steps to specify the timeout duration for a connection, translation, or protocol slot:

1. Verify with Customer Service that an idle timer value should change.
2. Verify the duration limitations and default times for the idle timer you specify.
3. In the **Timeout** panel, select the appropriate check box for the timeout feature you want to enable.
4. Enter the idle time duration in hours, minutes, and seconds (`hh:mm:ss`) for the connection, translation, or

protocol slot you select.

5. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Setup

Configuration>System Properties>Routing>OSPF>Setup

Overview
PDM 3.0 introduces support for dynamic routing using the Open Shortest Path First (OSPF) routing protocol. OSPF is widely deployed in large networks because of its efficient use of network bandwidth and its rapid convergence after changes in topology.

The OSPF functionality in PIX Firewall Version 6.3 is similar to that provided by Cisco IOS Software Release 12.2 (3a). For details about the syntax for each command and subcommand used to manage OSPF, refer to the *Cisco PIX Firewall Command Reference* or to Cisco IOS software documentation.

The following sections are included in this Help topic:

- Security Issues When Using OSPF
- OSPF Features Supported
- Field Descriptions
  - Process Instances
  - Area/Networks
  - Route Summarization
- Applying Changes to the Firewall

Security Issues When Using OSPF
Authentication should be used with all routing protocols when possible because route redistribution between OSPF and other protocols (like RIP) can potentially be used by attackers to subvert routing information. If MD5 authentication is used on all segments, security should not be an issue with OSPF.

When using dynamic routing, the physical security of the PIX Firewall is of increased importance. Access to the physical device and configuration information should be kept secure. Shared-keys should be changed at a reasonable interval.

As part of its normal operation, OSPF advertises routes to networks, and this may not be desirable in many PIX Firewall implementations. You may need to prevent networks from being advertised externally when using private addressing or when required by your security policy.

If NAT is used, if OSPF is operating on public and private areas, and if address filtering is required, then you need to run two OSPF processes—one process for the public areas and one for the private areas.

A router that has interfaces in multiple areas is called an Area Border Router (ABR). A router that acts as a gateway to redistribute traffic between routers using OSPF and routers using other routing protocols is called an Autonomous System Boundary Router (ASBR).

An ABR uses link-state advertisements (LSA) to send information about available routes to other OSPF routers. Using ABR type 3 LSA filtering, you can have separate private and public areas with the PIX Firewall acting as an ABR. Type 3 LSAs (inter-area routes) can be filtered from one area to other. This lets you use NAT and OSPF together without advertising private networks.

Note: Only type 3 LSAs can be filtered. If you configure PIX Firewall as an ASBR in a private network, it will send type 5 LSAs describing private networks, which will get flooded to the entire AS including public areas.

If NAT is employed but OSPF is only running in public areas, then routes to public networks can be redistributed inside the private network, either as default or type 5 AS External LSAs. However, you need to configure static routes for the private networks protected by the PIX Firewall. Also, you should not mix public and private networks on the same PIX Firewall interface.

OSPF Features Supported

The following is a list of OSPF features supported by PDM Version 3.0:

- Support of intra-area, inter-area and External (Type I and Type II) routes
- Support for virtual links
- OSPF LSA flooding
- Authentication for OSPF packets (both clear text and MD5 authentication)
- Support for configuring the PIX Firewall as a designated router (DR) or ABR
- Support for configuring the PIX Firewall as an ASBR, limited to default-information only
- Support for stub areas and not so stubby areas (NSSA)
- ABR type 3 LSA Filtering
- Route redistribution between OSPF processes including OSPF, static, and connected routes

---

Note:

- Running both OSPF and RIP concurrently on the same PIX Firewall is unsupported.
- OSPF is not supported on the PIX 501.
- Only two OSPF processes can be enabled on the PIX Firewall.

Field Descriptions

Process Instances

- **OSPF Process 1**

- **Enable This OSPF Process**—Select this check box to enable OSPF process 1 on the PIX Firewall.
- **OSPF Process ID**—Internally used identification parameter for an OSPF routing process. You assign it locally on the firewall, and it can be from 1 to 65535. A unique value must be assigned for each OSPF routing process.
- **Advanced**—Opens the Edit OSPF Process Advanced Properties dialog box.

- **OSPF Process 2**
  - **Enable This OSPF Process**—Select this check box to enable OSPF process 2 on the PIX Firewall.
  - **OSPF Process ID**—Internally used identification parameter for an OSPF routing process. You assign it locally on the firewall, and it can be from 1 to 65535. A unique value must be assigned for each OSPF routing process.
  - **Advanced**—Opens the Edit OSPF Process Advanced Properties dialog box.

Area Networks

This area lets you configure the new areas in a specific OSPF process instance. With the Add, Edit and Delete buttons you can configure the OSPF process, area ID, area type, networks, authentication, options and cost of an OSPF process.

Route Summarization

This area lets you configure route summarization information for a selected OSPF process. Route summarization is the consolidation of advertised addresses. This feature causes a single summary route to be advertised to other areas by an ABR. In OSPF, an ABR will advertise networks in one area into another area. If the network numbers in an area are assigned in a way such that they are contiguous, you can configure the ABR to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

Applying Changes to the Firewall

Changes are not immediately applied to the running Firewall configuration. You must click on one of the following buttons to apply or discard changes:

1. **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See More Configuration Changes.
2. **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Edit OSPF Process Advanced Properties

Configuration>System Properties>Routing>OSPF>Setup>Process Instances>
Edit OSPF Process Advanced Properties

The **Edit OSPF Process Advanced Properties** dialog box lets you edit the properties of a selected OSPF process.

The following sections are included in this Help topic:

- Field Descriptions
  - Adjacency Changes
  - Administrative Route Distances
  - Timers (in seconds)
  - Default Information Originate
- Applying Changes to the Firewall

Field Descriptions

- **Process ID**—Displays the ID of the current OSPF process.
- **Router ID**—OSPF uses the largest IP address configured on the interfaces as its router ID. If the interface associated with this IP address is ever brought down, or if the address is removed, the OSPF process must recalculate a new router ID and resend all its routing information out its interfaces. If the highest-level IP address on the firewall is a private address, then this address is sent in hello packets and database definitions (DBDs). To prevent this, set the router-id address to a global address.
- **Ignore LSA MOSPF**—Select this check box to suppress the sending of syslog messages when the router receives link-state advertisement (LSA) for Type 6 Multicast OSPF (MOSPF) packets, which are unsupported. To restore the sending of these syslog messages, clear this check box.
- **RFC1583 Compatible**—Select this check box to restore the method used to calculate summary route costs per RFC 1583. Clear this check box to disable RFC 1583 compatibility. By default, OSPF routing through the firewall is compatible with RFC 1583.

Adjacency Changes

- **Log Adjacency Changes**—Select to enable syslog for OSPF neighbors' state changes. Clear this check box to turn off this function.
- **Log Adjacency Change Details**—Select to enable detailed syslog entries for OSPF neighbors' state changes.

Administrative Route Distances

Configures administrative distances for the OSPF process.

- **Inter Area**—Sets the distance for all routes within an area.
- **Intra Area**—Sets the distance for all routes from one area to another area.
- **External**—Sets the distance for all routes from other routing domains learned by redistribution.

Timers (in seconds)

Configures timers for the OSPF process.

- **SPF Delay Time**—The delay time between when OSPF receives a topology change and when it starts a shortest path first algorithm (SPF) calculation, in seconds, from 0 to 65535. The default is 5 seconds.
- **SPF Hold Time**—The hold time between two consecutive SPF calculations, in seconds, from 0 to 65535. The default is 10 seconds.
- **LSA Group Pacing**—The interval at which OSPF link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, from 10 to 1800 seconds. The default value is 240 seconds.

  The OSPF LSA group pacing feature allows the router to group OSPF LSAs and pace the refreshing, checksumming, and aging functions. The group pacing results in more efficient use of the router.

  The router groups OSPF LSAs and paces the refreshing, checksumming, and aging functions so that sudden increases in CPU usage and network resources are avoided. This feature is most beneficial to large OSPF networks.

  OSPF LSA group pacing is enabled by default. For typical customers, the default group pacing interval for refreshing, checksumming, and aging is appropriate. You need not configure this feature.

Default Information Originate

Routes that originate from other routing protocols (or different OSPF processes) and injected into OSPF through redistribution are called external routes. There are two forms of external metrics: type 1 and type 2. These routes are represented by O E2 (for type 2) or O E1 (for type 1) in the IP routing table, and they are examined after the firewall is done building its internal routing table. After they are examined, they are flooded throughout the autonomous systems (AS), unaltered. (Autonomous systems are a collection of networks, subdivided by areas, under a common administration sharing a common routing strategy.)

OSPF type 1 metrics result in routes adding the internal OSPF metric to the external route metric; they are also expressed in the same terms as an OSPF link-state metric. The internal OSPF metric is the total cost of reaching the external destination, including whatever internal OSPF network costs are incurred to get there. (These costs are calculated by the device wanting to reach the external route.) Because it is calculated this way, the OSPF type 1 metric is generally preferred.

OSPF type 2 metrics do not add the internal OSPF metric to the cost of external routes and are the default type used by OSPF. The use of OSPF type 2 metrics assumes that you are routing between autonomous systems (AS); therefore, the cost is considered greater than any internal metrics. This eliminates the need to add the internal OSPF metrics.

- **Enable Default Information Originate**—Select this check box to enable default information originate.
- **Always Advertise Default Route**—Select this check box to always advertise the default route.
- **Metric Value**—Select this check box and specify the OSPF default metric value, from 0 to 16777214.
- **Metric Type**—Select this check box and specify OSPF metric type for default routes, either type 1 or 2. The default is type 2.
- **Route Map**—Select this check box and specify the text for the route map tag, meant to define a meaningful name for the route map. Multiple route maps may share the same map tag name.

Applying Changes to the Firewall

OK—Accepts changes and returns to the previous panel.
Cancel—Discards changes and returns to the previous panel.
Help—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

ESP-IKE

Configuration>System Properties>Advanced>Fixup>ESP-IKE

The **ESP-IKE** panel lets you enable the use of Encapsulating Security Protocol (ESP) with Port Address Translation (PAT). The ESP-IKE fixup feature is disabled by default.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Disabling ESP-IKE Fixup
- Enabling ESP-IKE Fixup
- Resetting to Last Applied Settings

Important Notes

With this feature enabled, you cannot use the PIX Firewall as a VPN tunnel termination endpoint. You cannot have IKE enabled on the PIX Firewall, and additionally, only one ESP tunnel is permitted to pass through the PIX Firewall at a time.

Field Descriptions

The **ESP-IKE** panel displays the following fields:

- **Enable ESP traffic through the firewall configured for PAT**—Allows ESP traffic to pass through the PIX Firewall that is configured for PAT.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Disabling ESP-IKE Fixup

This feature is enabled by default. Follow these steps to disable ESP-IKE fixup:

1. In the **ESP-IKE** panel, select the **Enable ESP traffic through the firewall configured for PAT** check box.
2. Click **Apply**.

Enabling ESP-IKE Fixup

Follow these steps to re-enable ESP-IKE fixup after it has been disabled:

1. In the **ESP-IKE** panel, clear the **Enable ESP traffic through the firewall configured for PAT** check box.
2. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Logging Setup Edit

Configuration>System Properties>Logging>Logging Setup Edit

The **Syslog Logging** panel lets you modify the logging level or suppression setting for selected syslog messages.

The following sections are included in this Help topic:

- Field Descriptions
- Suppressing or Restoring a Message Type
- Setting the Logging Level

Field Descriptions

The **Syslog Logging** panel displays the following fields:

- **Syslog ID(s)**—This text area is read-only. The values displayed in this field are determined by the entries selected in the Syslog ID table located in the Logging Setup panel.
- **Suppress Message(s)**—Select this check box to suppress messages for the syslog ID(s) displayed in the Syslog ID(s) list.
- **Logging Level**—Choose the level of logging messages to be sent to the syslog server for the syslog ID(s) displayed in the Syslog ID(s) list. Levels are defined as follows:
  - Disabled (no logging)
  - Emergency (level 0, system unusable)
  - Alert (level 1, immediate action needed)
  - Critical (level 2, critical condition)
  - Error (level 3, error condition)
  - Warning (level 4, warning condition)
  - Notification (level 5, normal but significant condition)
  - Informational (level 6, informational message only)
  - Debugging (level 7, appears during debugging only)
- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Suppressing or Restoring a Message Type

To suppress or restore the message type(s) listed in the Syslog ID(s) list, select or clear the **Suppress Message** check box and then click **OK**.

Setting the Logging Level

To set the logging level for the message type(s) listed in the Syslog ID(s) list, click the **Logging Level** drop-down list and choose the desired level. Click **OK**.

OK—Accepts changes and returns to the previous panel.

Cancel—Discards changes and returns to the previous panel.

Help—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

Management Access

Configuration>System Properties>Administration>Management Access

The **Management Access** panel lets you perform PIX management functions, such as running PDM, on an internal interface with a fixed IP address over an IPSec VPN tunnel. Use this feature if VPN is configured on the PIX and the external interface is using a dynamically assigned IP address. For example, this feature is helpful in low-end PIX platforms used as Easy VPN Remote clients, where the externally reachable interface usually has a dynamically assigned IP address. Make sure to include the IP address of the internal management interface in the crypto ACL.

Note: Refer to the *Cisco PIX Firewall and VPN Configuration Guide* for more information about configuring IPSec.

The following sections are included in this Help topic:

- Field Descriptions
- Specifying the Management Access Interface

Field Descriptions

The **Management Access** panel displays the following fields:

- **Management Access Interface**—Enables the Management Access feature on the selected interface, which allows the PIX to perform management functions on the interface over an IPSec VPN tunnel.

Specifying the Management Access Interface

To specify the management access interface, select the interface in the **Management Access Interface** drop-down list. You can enable the Management Access feature on only one interface at a time.

Select **None** to disable the Management Access feature on the PIX. **None** is selected by default.

Copyright © 2001-2004, Cisco Systems, Inc.

Console

Configuration>System Properties>Administration>Console

The **Console** panel lets you set the time a console connection remains open when idle. If the console is not used for the time specified in the **Console Timeout** box, the console connection ends. This feature prevents unauthorized access to your firewall console session when it is left open, idle, and unattended.

The following sections are included in this Help topic:

- Field Descriptions
- Changing the Console Timeout

Field Descriptions

- **Console Timeout**—Specifies the time, in minutes, that a console session remains open when idle. If you want the console session to remain open all the time, enter **0** minutes. The default value is 0 minutes; the range is 0 to 60 minutes.

Changing the Console Timeout

In the **Console Timeout** box, enter the time, in minutes, that you want the console session to remain open when idle. To keep the console session open at all times, enter **0** minutes.

Caution: If the console session is open at all times, and the firewall is left unattended, it is vulnerable to unauthorized access.

Copyright © 2001-2004, Cisco Systems, Inc.

Banner

System Properties>Administration>Banner

The **Banner** panel lets you configure message of the day, login, and session banners.

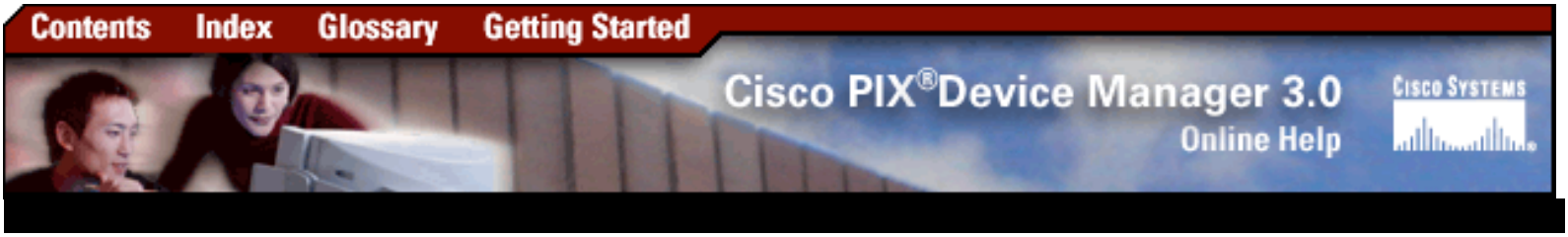
To create a banner, enter text into the appropriate box. Spaces in the text are preserved, however, tabs cannot be entered. The tokens $(domain) and $(hostname) are replaced with the host name and domain name of the firewall.

Multiple lines in a banner are handled by entering a line of text for each line you wish to add. Each line is then appended to the end of the existing banner. If the text is empty, then a carriage return (CR) will be added to the banner. There is no limit on the length of a banner other than RAM and Flash memory limits.

When accessing the firewall through Telnet or SSH, the session closes if there is not enough system memory available to process the banner messages or if a TCP write error occurs when attempting to display the banner messages.

To replace a banner, change the contents of the appropriate box and click **Apply**. To clear a banner, clear the contents of the appropriate box and click **Apply**.

Copyright © 2001-2004, Cisco Systems, Inc.



Home

The PDM home page lets you view at a glance important information about your PIX Firewall such as the status of your interfaces, the version you are running, licensing information, and performance. Many of the details available on the PDM home page are available elsewhere in PDM, but this is a useful and quick way to see how your PIX Firewall is running. All information on the **Home** page is updated every ten seconds, except for the **Device Information**.

You can access the Home page any time by clicking **Home** on the main toolbar.

Note—If the interface is configured to use DHCP or PPPoE to obtain an IP address, and running PIX Firewall Version 6.3(2) or higher, your IP address will be displayed in the **Interface Status** table. If you are running an earlier version of the PIX Firewall software, the IP address will not be displayed.

Note—On a PIX 501, the inside interface link will always be displayed as up, because this interface acts as a built-in switch. Be sure to check for physical connectivity on the inside interface of a PIX 501.

The following sections are included in this Help topic:

- Field Descriptions
- Home Panel

Field Descriptions

The **Home** panel displays the following fields:

Area	Description	
Device Information	This area displays the following information:	
	Host Name, **PIX Version**, **Device Type**, **License**, **PDM Version**, **Total Memory**, and **Total Flash**.	
	Licensed Features—This area displays the features your PIX Firewall is	Encryption
		Failover

	licensed to use.	Max Interfaces
		Inside Hosts
		IKE Peers
		Max Physical Interfaces
Interface Status	**Interface**—This displays the interface name as configured in the **Interfaces** panel. You can click any of the table headings to sort by that value.	
	IP Address/Mask—This displays the IP address and netmask of the associated interface.	
	Link—This displays the link status of the interface. A red icon is displayed if the physical status of the link is down, and a green icon is displayed if the physical status of the link is up. Note that on a PIX 501, the inside interface link will always be displayed as up, because this interface acts as a built-in switch. Be sure to check for physical connectivity on the inside interface of a PIX 501. The color of the icon does not reflect the administrative status of the interface. The administrative status might be configured down, denying traffic to pass, even if the physical link is up and the link icon is green.	
	Current Kbps—This displays the current number of kilobits per second that cross the interface.	
VPN Status	This area displays the status of your VPN tunnels, if they are configured.	
Traffic Status	**Connections Usage**—This displays the number of TCP and UDP connections that occur each second. Their sum is displayed as the total number of connections.	
	Outside Interface Traffic Usage—This displays the traffic going through **outside** interface in kilobits per second.	
System Resources Status	**CPU**—Displays the percentage of CPU being utilized at the moment.	
	CPU Usage (percent)—This displays the real time status of CPU usage and history for the last five minutes.	
	Memory—Displays the total amount of memory being utilized at the moment.	
	Memory Usage (percent)—This displays the real time memory usage and history for the last five minutes, in megabytes.	
	Memory (MB)—Displays information about free, used and total memory in megabytes. Note that one megabyte is equal to 1,048,576 bytes.	

Copyright © 2001-2004, Cisco Systems, Inc.

Main Toolbar

The main toolbar gives you quick access to the home page, configuration panels, PDM monitoring, and context sensitive help. You can also save your running configuration to flash memory using **Save**, or reload the running configuration from flash using **Refresh**.

The following sections are included in this Help topic:

- Field Descriptions
- Main Toolbar

Field Descriptions

The main toolbar contains the following:

Button/Tab	Description
Home	Opens the Home Page.
Configuration	Opens the Configuration Page, which contains the following tabs:
	Access Rules—This tab lets you configure Access Rules for PDM, controlling who can access your network.
	Translation Rules—This tab lets you configure Translation Rules for Network Address Translation (NAT) or Port Address Translation (PAT) on PDM.
	VPN—This tab lets you configure virtual private networks (VPN) on PDM.
	Hosts/Networks—This tab lets you configure hosts or networks that are connected to your firewall.
	System Properties—The Systems Properties tab lets you configure a wide variety of features in PDM, such as interfaces, routing, and failover.
Monitoring	Monitoring lets you view PDM logging, monitor who is connected to PDM, and a large selection of graphs.
Refresh	Click to refresh PDM with the current running configuration.

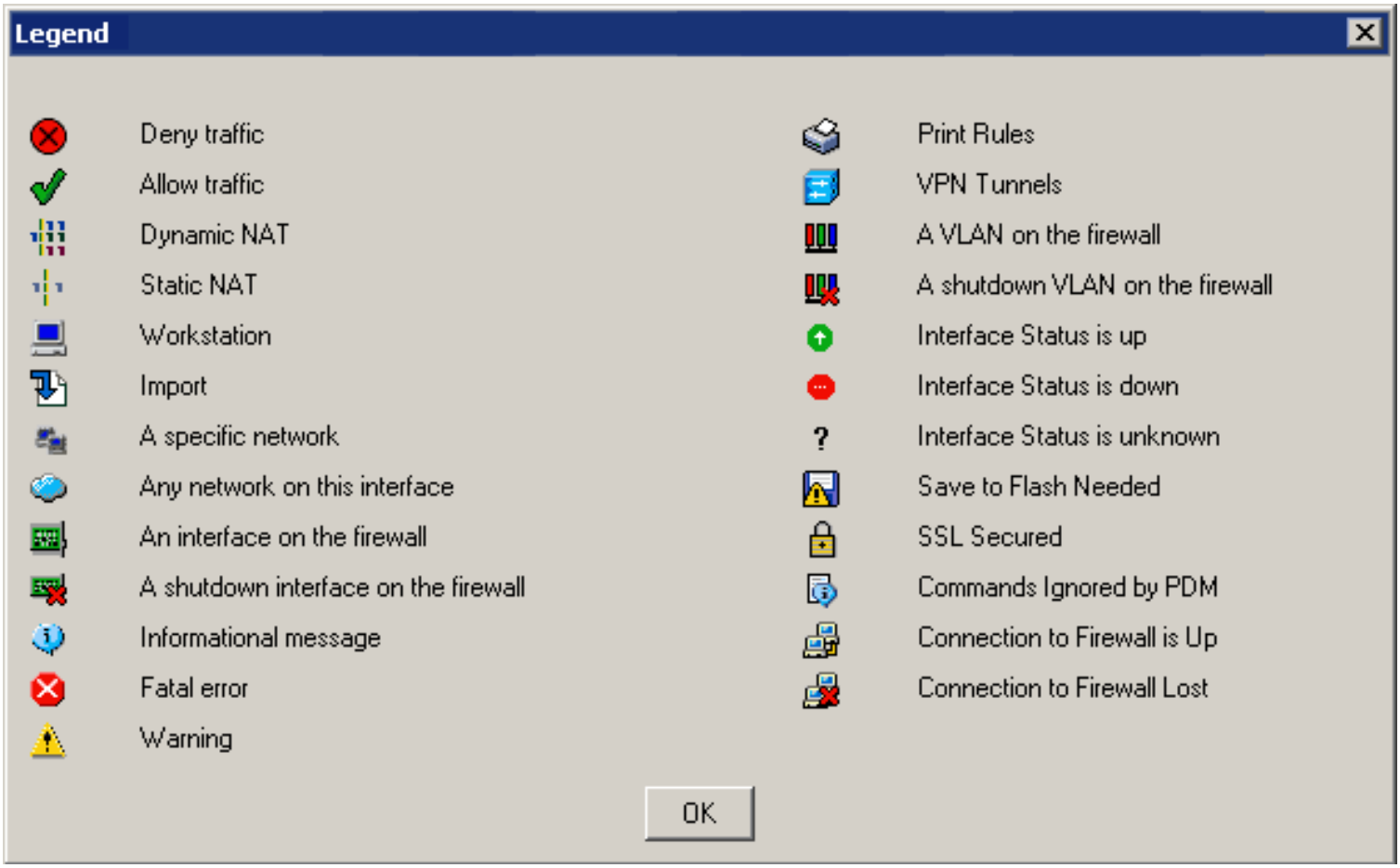
Save	Click to write a copy of the running configuration to the Flash memory inside the firewall chassis.
Help	Click for context sensitive help at any time while running PDM.

Copyright © 2001-2004, Cisco Systems, Inc.

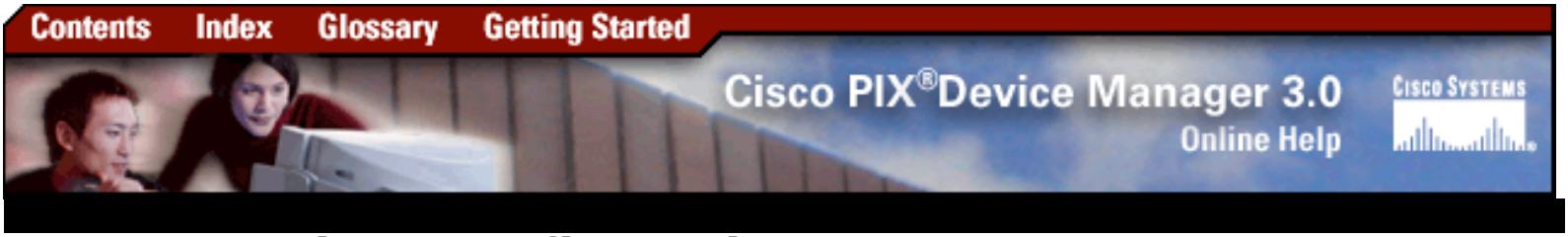
Legend

Help>Legend

The **Legend** panel displays a list of icons used within PDM, and provides a short description of what each icon represents. Select **Help>Legend** to display the icon legend.



Copyright © 2001-2004, Cisco Systems, Inc.



Save Running Configuration to TFTP Server

File>Save Running Configuration to TFTP Server

The **Save Running Configuration to TFTP Server** panel lets you write the current running configuration to a Trivial File Transfer Protocol (TFTP) server.

The following sections are included in this Help topic:

- Field Descriptions
- Defining a TFTP Server and Configuration File Name

Field Descriptions

The **Save Running Configuration to TFTP Server** panel displays the following fields:

- **Interface Name**—The interface on which your TFTP server resides. This information reflects what is configured in **Configuration>System Properties>Administration>TFTP Server**. The default interface is **inside**.
- **TFTP Server IP Address**—Enter the IP address of the TFTP server.
- **Configuration File Name**—Enter the path and filename of the configuration file to be saved on your TFTP Server.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.
- **Cancel**—Discards changes and returns to the previous panel.

Defining a TFTP Server and Configuration File Name

Follow these steps to define a TFTP server and configuration file name:

1. Enter the IP address of the TFTP server to write the configuration file to.
2. Enter the TFTP server **Path/filename**, beginning with a forward slash (/) and ending with the filename you want to write the running configuration file to. The path must begin with a forward slash (/); for example, **`/tftpboot/pixfirewall/config3`**. In this example, **`config3`** is the name of the file the running configuration is written to.
3. Click **Apply**.

Copyright © 2001-2004, Cisco Systems, Inc.

Preferences

Options>Preferences

The **Preferences** panel lets you change the behavior of some PDM functions between sessions by using your web browser's cookie feature.

The following sections are included in this Help topic:

- Preference Items Saved
- Field Descriptions

Preferences Items Saved

The following preferences are saved in your web browser's cookie:

- Preview commands before sending to the firewall.
- Confirm before exiting from PDM.
- Display dialog about the VPN Wizard when the VPN tab is selected.

Note: If cookies are disabled in your web browser, the settings are lost when you exit PDM.

Field Descriptions

The **Preferences** panel includes the following fields:

- **Preview Commands Before Sending to the firewall**—Lets you view CLI commands generated by PDM.
- **Confirm before exiting from PDM**—Displays a prompt when you try to close PDM to confirm that you want to exit.
- **Display dialog about the VPN Wizard when the VPN tab is selected**—Displays a dialog box about the VPN Wizard the first time you select the **VPN** tab each session.

Limitations

The following limitations apply:

- Enable your web browser's cookies for this feature to work. If cookies are disabled, the settings apply only to the current session. PDM does not warn you if cookies are disabled because this setting is controlled by your web browser, not PDM. The settings are saved only if cookies are enabled.
- Cookies are stored on your local hard drive (client side). If your run PDM on another PC, the stored settings of the other PC are not used.
- Cookies are stored on a per-site basis. The preferences made for one firewall do not carry over to another. There is no way to make a global change for all firewalls.

Copyright © 2001-2004, Cisco Systems, Inc.

Search by Field

Search>Search by Field

The **Search by Field** panel lets you find rules, based on a selected criteria, displayed by the **Configuration>Access Rules** or **Configuration>Translation Rules** tabs.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
  - Access Rules
  - Translation Rules
- Searching for Access Rules Containing a Pattern
- Searching for a Translation by Field

Important Notes

- The **Search by Field** panel uses a simple text compare.
- The matching rules are highlighted in yellow.
- Select **Search>Clear Search Selections** to clear the yellow highlights and the search results text from the panel.
- When a search is complete, a line of text appears on the panel showing how many rules, or **Hits**, were matched. The following example shows what would display in the upper right corner of the **Configuration>Access Rules** tab:

  ```
  Search Results: Access rules:999 AAA:888 Filter:777
  ```

- If you perform a new search, the previous search selections are cleared and the results are no longer filtered.

Field Descriptions

The **Search by Field>Search** dialog box displays the following fields when started from the **Configuration>Access Rules** tab:

- **Match all of the following**—Specifies to perform your search matching all of the selected criteria.

- The three search criteria boxes on the left let you select specific search criteria. The following are the options:

    - **None**
    - **Source Address**
    - **Source Name**
    - **Destination Address**
    - **Destination Name**
    - **Action**
    - **Service**

    These let you select a data type on which the search will be performed. On the right side are list boxes in which the actual pattern to be matched can be entered. For each field **Browse** (**...**) will display a list of items that are appropriate for the selected data type.

- **Search**—Initiates the search function. Results will be highlighted in yellow on PDM.
- **Reset**—Clears the search panel so the choices can be reentered.
- **Help**—Provides more information.
- **Close**—Clears any changes you may have made and closes this panel.

The **Search by Field>Search** dialog box opened from the **Configuration>Translation Rules** tab lets you search for translation rules by the following methods:

- **Type**—The type of translation. In this case the options are Static and Dynamic.
    - **Original Interface**—The interface where the translation originates.
    - **Original Address**—The original address that is to be translated.
    - **Translated Interface**—The address where the translation occurs.
    - **Translated Address**—The address to which the original address is translated.
    - **Name**—The name of the host or network.

- **Search**—Initiates the search function. Results will be highlighted in yellow on PDM.
- **Close**—Clears any changes you may have made and closes this panel.
- **Help**—Provides more information.
- **Reset**—Clears the search panel so choices can be reentered.

Searching for Access Rules Containing a Pattern

Follow these steps to search for an access rule containing a pattern:

1. Click **Search>Search by Field**.
2. Click **Match any of the following** or **Match all of the following**.
3. From the search criteria option lists on the left, select the type of data to be searched.
4. In the boxes on the right either enter or select the pattern to be matched. To select a pattern, click

Browse and select the desired item from the list of items displayed. To enter a pattern, type the pattern in the box. Partial patterns are allowed on the following search criteria options:

- **Source Address**
- **Source Name**
- **Destination Address**
- **Destination Name**
- **Service**

A partial pattern must have a trailing asterisk (*). For example, "139.1*" would match any IP address starting with "139.1", "web*" would match any host or network name starting with "web". Patterns such as "*" or 139.1*.22" or "*11" are not allowed.

The search results display in the **Configuration>Access Rules** tab. The rules that match the search criteria will be highlighted in yellow on PDM.

Follow these steps to search for access rules containing a pattern:

1. Click **Browse**. The associated dialog box opens, displaying options to search.
2. Click **Search** to initiate the search.
3. Click **OK**.

Search for a Translation by Field

Complete the following steps to search for a translation:

1. Select the method by which you wish to search, such as **Type** or **Original Interface**.
2. Click the **Browse** to browse for selectable options.
3. Click **Search**.

Copyright © 2001-2004, Cisco Systems, Inc.

Search>Search by Host/Network

The **Top Menu>Search>Search by Host/Network** panel lets you search for an access rule by host or network.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Searching by Host/Network

Important Notes

Unlike the **Search>Search by Field** dialog box, which performs a plain text comparison search, **Search>Search by Host/Network** menu item uses a more complex, applicability heuristic search. **Search by Host/Network** will search for all rules that affect the host or network the search is performed on.

#	Action	Source Name/Address	Destination Name/Address	Interface	Service	Description
1		outside:any	10.130.44.11	(inbound)	http/tcp	
2		outside:any	10.130.44.0/24	(inbound)	ip	

In this example the search for host 10.130.44.11 will cause the #1 and #2 rules to be highlighted because the first rule contains the host 10.130.44.11 as the destination. The second rule operates on the network 10.130.44.0/24, which is where host 10.130.44.11 is located. Any rules that apply to 10.130.44.0/24 also apply to 10.130.44.11.

The matching access rules will be highlighted in yellow.

Clicking **Search>Clear Search Selections** will clear the yellow highlights and the search results text from the screen.

Search Results—When a search is complete a line of text will appear on the **Access Rules** or **Translation Rules** tab showing how many rules were matched for each type.

For example: "Search Results: Access rules:999 AAA:888 Filter:777" would be displayed in the upper right corner of the **Access Rules** tab.

If you perform a new search, the previous search selections will be cleared. They will not further filter the results.

Field Descriptions

The **Search>Search by host/network** dialog box displays the following fields:

- **Interface**—Lets you select which interface to search for an access rule by host or network.
- **Network tree**—Lets you browse to a host or network and select it as search criteria. You must have already configured the host or network by which you wish to search in the **Hosts/Networks** tab.
- **Search**—Initiates the search for the selected host or network.
- **Help**—Provides more information.
- **Close**—Closes the **Search>Search by Host/Network** dialog box.

Searching by Host/Network

Follow these steps to search for an access rule by host or network:

1. Click an Interface in the **Interface** list.
2. In the **Network tree**, browse to select the host or network you wish to search.
3. Click **Search**.

Results will be highlighted in yellow on the **Access Rules** tab.

Copyright © 2001-2004, Cisco Systems, Inc.

Add, Edit, Insert or Paste Access Rule

Configuration>Access Rules>Access Rules>Add, Edit, Insert or Paste Rule

The **Add, Edit, Insert,** or **Paste Rule** dialog boxes let you create a new rule, or modify an existing rule.

The following sections are included in this Help topic:

- Field Descriptions
- Editing a Rule

Field Descriptions

The **Add, Edit, Insert,** or **Paste Rule** dialog boxes display the following areas and fields:

Area	Description and Fields	
Action	Determines the action type of the new rule. Choose the type of action from the list:	
	Permit	Permits all matching traffic.
	Deny	Denies all matching traffic.
Syslog	Enable logging for the ACL and set logging options.	
	Enable Syslog check box	Enable logging for the ACL; when a packet matches the ACL (permit or deny), a message is logged on the firewall. See syslog message number 106100.
	More Options button	Click this button to set logging options. Even if you do not check the **Enable Logging** check box, this button allows you to: • Revert to default logging (logging only when a packet is denied; see syslog message number 106023). This option unchecks the **Enable Logging** check box. • Stop all logging. This option unchecks the **Enable Logging** check box. • Set the level and interval for permit and deny logging. This option checks the **Enable Logging** check box. See **Log Options** for more information. Also, see **Advanced**

		Access Rule Configuration to set global logging options.	
Source and Destination Host/ Network	Defines the source and destination hosts/networks for the rule.		
	IP Address option button	Click this option button to identify the networks by IP address.	
		Interface	The interface on which the host or network resides.
		IP address	The IP address of the host or network.
		Mask	The subnet mask of the host or network.
		Browse	Lets you select an existing host or network by clicking the options under the **Select Host/ Network** panel to populate the **Name**, **Interface**, **IP address**, and **Mask** boxes with the properties of the selected host or network.
	Name option button	Click this option button to identify the networks by name. To name hosts/networks, see the Hosts/Networks tab.	
		Name	The name of the host or network. If you choose this option, and reopen the rule to edit it, the option button selection reverts to IP Address, and the named host/network IP address information appears in the fields.
	Group option button	Click this option button to identify a group of networks and hosts that you grouped together on the Hosts/Networks tab.	
		Interface	The interface connected to the hosts and networks in the group.
		Group	The group name.
Protocol and Service	Specify the protocol and service for the rule, in addition to the source and destination ports. See the following buttons and protocol option button options:		
	Manage Service Groups button	Manages service groups. Service groups allow you to identify multiple non-contiguous port numbers that you want the ACL to match. For example, if you want to filter HTTP, FTP, and port numbers 5, 8, and 9, you can define a service group that includes all these ports. Without service groups, you would have to create a separate rule for each port. You can create service groups for TCP, UDP, and TCP-UDP. A service group with the TCP-UDP protocol contains services, ports, and ranges that might use either the TCP or UDP protocol. See Manage Service Groups for more information.	
	TCP and **UDP** option buttons	Selects the TCP or UDP protocol. The **Source Port** and **Destination Port** areas allow you to specify the ports that the ACL uses to match packets.	

Service option button	Click this option button to specify a port number, a range of ports, or a well-known service name from a list of services, such as HTTP or FTP. See the following field descriptions:
	Operator list—Specifies how the ACL matches the port. Choose one of the following operators: • **=** —Equals the port number. • **not =** —Does not equal the port number. • **>** —Greater than the port number. • **<** —Less than the port number. • **range** —Equal to one of the port numbers in the range.
	Service name/Port number box—Specifies the port number or well-known service name. This field depends on the operator you choose: • **=**, **not =** —Enter a single port number or service name in the field. The default is **any**. For a list of well-known service names (for the chosen protocol), click to select from the **Service** list. If you enter a well-known port number, the service name is shown in the Access List table instead of the port number. For example, if you specify port **80**, the table shows **http**. • **>**, **<** —Enter a single port number. You can type a service name, but the Access List table shows the port number instead. For example, if you enter **http**, the table shows **80**. This option does not provide a browse function for the service name. • **range** —Enter the starting port number in the first field, and the ending port number in the second field. You can type a service name, but the Access List table shows the port number instead. For example, if you enter **http**, the table shows **80**. This option does not provide a browse function for the service name.

		Service Group option button	Click this option button to select a service group. Choose the service group name from the list. Only groups assigned to the chosen protocol appear. To create a service group, click the **Manage Service Groups** button.
	ICMP option button	Selects the ICMP protocol.	
		ICMP Type	Enter a single ICMP type number or type name in the field. The default is **any**. For a list of well-known type names, click ... to select from the **Service** list. If you enter a well-known type number, the type name is shown in the Access List table instead of the type number. For example, if you specify type **8**, the table shows **echo**.
	IP option button	Selects IP. This option allows you to specify an IP protocol, although it does not allow you to specify the port numbers. IP protocols include TCP and UDP (which are configurable in PDM separately because they are so common), as well as many other protocols such as ESP and GRE. For example, choosing TCP for this option is equivalent to clicking the **TCP** option button and specifying **any**.	
		IP Protocol	Enter a single IP protocol number or name in the field. The default is **any**. For a list of well-known protocol names, click ... to select from the **Service** list. If you enter a well-known protocol number, the protocol name is shown in the Access List table instead of the number. For example, if you specify number **6**, the table shows **tcp**.
Please enter the description below (optional)	Enter a description of the access rule.		

Editing a Rule

Follow these steps to add a new rule or to modify an existing rule:

1. From the **Action** list, choose an action:
    - **Permit**
    - **Deny**
2. To enable logging, click the **Enable Syslog** check box.

3. To change the default logging parameters, click the **More Options** button.

   See **Log Options** for more information.
4. Define the source and destination hosts or networks. ACLs only apply to the inbound traffic on an interface.

- By IP Address—If you select this option, you can specify a particular network or host behind an interface, or you can use wildcards to specify any network behind the interface. By default, the IP address and mask are 0.0.0.0, the wildcard notation signifying any address.
  - To browse to an IP address:
    a. Click the **IP Address** option button.
    b. Click the **Browse** button.
    The Select Host/Network dialog box appears.
    c. From the list, choose the interface in front of the host/network.
    All the hosts and networks behind the interface are displayed.
    d. Select the host/network, and click **OK**.
    The interface, IP address, and subnet mask fields are automatically filled.
  - To type an IP address:
    a. Click the **IP Address** option button.
    b. From the **Interface** list, select an interface name.
    c. In the **IP address** box, enter the IP address of the host or network.
    d. In the **Mask** box, enter the netmask of the source host or network, or select a netmask from the list.
- By Name—If you select this option, the firewall applies the ACL to the specific network identified by name. By default, the networks directly connected to the firewall are named after the firewall interfaces; however, only the directly connected network is specified. If you want to match all networks behind an interface, use the IP Address option (above). To name other hosts/networks, see the **Hosts/Networks** tab.
  a. Click the **Name** option button.
  b. In the **Name** box, type the name of the source host or network; or click the **down arrow** and choose a name from the list.
- By Group—If you select this option, the firewall applies the ACL to a group of networks and hosts that you grouped together on the **Hosts/Networks** tab.
  a. Click the **Group** option button.
  b. In the **Interface** box, choose a name from the list.
  c. In the **Group** box, type the name of the group; or click the **down arrow** and choose a name from the list.

5. In the Protocol and Service area, click one of the following option buttons:

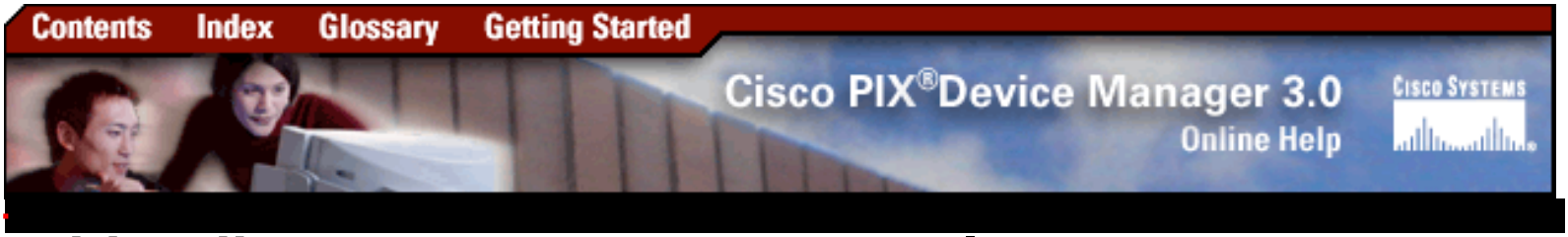
   - **TCP**
   - **UDP**
   - **ICMP**
   - **IP**

   See the **Protocol and Service** area field descriptions above for details about all settings.

6. For TCP and UDP, you can create service groups by clicking the **Manage Service Groups** button.

7. Click **OK** to finish editing the rule, or **Cancel** to discard your changes.

Copyright © 2001-2004, Cisco Systems, Inc.



Add, Edit, Insert or Paste AAA Rule

Configuration>Access Rules>AAA Rule>Add, Edit, Insert or Paste Rule

The **Add, Edit, Insert,** or **Paste Rule** dialog boxes let you create a new rule, or modify an existing rule.

The following sections are included in this Help topic:

- Field Descriptions
- Creating a Rule

Note: Review **Important Notes about Object Groups** regarding the naming of Service Groups**.**

Field Descriptions

The **Add, Edit, Insert,** or **Paste Rule** dialog boxes display the following fields:

- **Action**—Determines the action type of the new rule. The choices are different based on the type of AAA Rule you select.
- Source Host/Network
- Destination Host/Network

The **AAA** dialog box has an associated configuration panel, which appears at the bottom of the dialog box after the option is selected. The associated configuration area lets you finish the configuration for the rule.

- **AAA Options**
  - Authenticate
  - Do not authenticate
- Authorize
- Do not authorize
- Account
- Do not account
- Exempt MAC
- Do not exempt MAC

- **Please enter the description below (optional)**—Enter a description of the rule.

Action

The Action group box allows you to select the action, authenticate or do not authenticate, that this exemption rule will take if the host/network meets the criteria defined.

The **Select an action** list options are as follows:

- **Authenticate**—Specifies that the traffic defined will be authenticated.
- **Do Not Authenticate**—Specifies that the traffic defined will not be authenticated.

Source Host/Network

The Source Host/Network group box allows you to define the criteria which must be met for the Action to be performed. The criteria my be defined by selecting an IP address, Name, Group, or by browsing a previously defined list of hosts/networks.

IP Address—Selects the criteria of testing the IP address of the source host or network to determine if the Action of the exemption rule will be applied. Selecting this option displays the following fields:

- **Interface**—Selects the firewall network interface name on which the original host or network resides.
- **IP address**—Specifies the IP address of the host or network to which you would like to apply a rule.
- **Mask**—Select the network mask (netmask) for the address.

Name—Selects the criteria of testing the name of the source host or network to determine if the Action of the exemption rule will be applied. Selecting this option displays the following fields:

- **Name**—Lets you select a previously defined name of a host or network to which you would like to apply the rule. Note: The firewall also automatically generates a host name for each interface by using the interface name, such as `inside` or `outside`.

Group—Selects the criteria of testing a group of the source host or network to determine if the Action of the exemption rule will be applied. Selecting this option displays the following fields:

- **Interface**—Interface—Selects the firewall network interface name on which the original host or network resides.

- **Group**— Selects the group of the host or network to which you would like to apply the rule.

Browse—Lets you select the correct IP address and mask from the Hosts/Networks tree from a predefined host or network.

Destination Host/Network

IP address—Specifies the IP address of the destination host or network to which you would like to apply the exemption rule.

- **Interface**—Selects the firewall network interface name on which the original host or network resides.
- **IP address**—Specifies the IP address of the host or network to which you would like to apply a rule.
- **Mask**—Select the network mask (netmask) for the address.

Name—Selects the criteria of testing the name of the source host or network to determine if the Action of the exemption rule will be applied. Selecting this option displays the following fields:

- **Name**—Lets you select a previously defined name of a host or network to which you would like to apply the rule. Note: The firewall also automatically generates a host name for each interface by using the interface name, such as `inside` or `outside`.

Group—Selects the criteria of testing a group of the source host or network to determine if the Action of the exemption rule will be applied. Selecting this option displays the following fields:

- **Interface**—Interface—Selects the firewall network interface name on which the original host or network resides.
- **Group**— Selects the group of the host or network to which you would like to apply the rule.

Browse... —Lets you select the correct IP address and mask from the Hosts/Networks tree from a predefined host or network.

AAA Option—This area is associated with the action types of **authenticate/do not authenticate**, **authorize/do not authorize**, **account/do not account**, and **exempt MAC/do not exempt MAC**. The **AAA Option** area lets you specify the service and AAA server group. Each AAA option provides associated options to configure. AAA accounting rules are not supported using the local database as the **AAA Server Group**.

The **authenticate** and **do not authenticate** action rule types display the following fields:

- **TCP**—Lets you select the TCP service/protocol.
  - **Authentication Service**—Lets you specify the TCP service that the firewall will use to authenticate a user.
    Select Application—Lets you select a TCP protocol, such as ftp, http, or telnet from the **Select Application** list.
- **AAA Server Group**—Lets you specify the server group on which to run the selected AAA service.
  - **Group Tag**—Lets you select a server group from the **Group Tag** list.

The **authorize, do not authorize, account** and **do not account** action rule types display the following:

- **TCP**—Lets you select the TCP service/protocol.
  Application Port—Lets you specify the application port by either typing this information in the **Application Port** box or selecting it from the **Service** list.
  Click to select the application port from the **Service** dialog box that is displayed.
- **UDP**—Lets you select the UDP service/protocol.
  Application Port—Lets you specify the application port by either entering it or selecting it from a list of application ports.
  Click to select the application port from the **Service** dialog box that is displayed.
- **ICMP**—Lets you select the ICMP service.
  ICMP Type—Lets you specify the ICMP message type by either typing this information in the **ICMP Type** box or selecting it from the **Service** list.
  Click to select the ICMP message type from the **Service** dialog box that is displayed.
- **IP**—Lets you select the IP service.
  IP Protocol—Lets you specify the IP protocol type by either typing this information in the **IP protocol** box or selecting it from the **IP protocol** list.
  Click to select the IP protocol type from the **Service** dialog box that is displayed.
- **AAA Server Group**—Lets you specify the server group on which to run the selected AAA service.
  AAA accounting rules are not supported when **LOCAL** is selected as the **AAA Server Group**.
- **Group Tag**—Lets you select a server group from the **Group Tag** list. The default options are TACACS+ and RADIUS.

The **exempt MAC** and **do not exempt MAC** action rule types display the following fields:

- **MAC Address**—Lets you specify a MAC address.
- **Mask**—Lets you specify a mask for the MAC address.

Creating a Rule

Follow these steps to add a new rule or to modify and existing rule:

1. Under **Action**, select an action from the **Select an action** list.
2. Define the source host or network.

- Click the **Name** option, and type the name of the source host or network in the **Name** box

  or

- In the **Interface** list, select an interface name.
- In the **IP address** box, enter the IP address of the source host or network.
- In the **Mask** box, enter the netmask of the source host or network, or select a netmask from the list.

  Browse lets you select an existing host or network under **Select Host/Network** to populate the **Name**, **Interface**, **IP address**, and **Mask** boxes with the selected host or network properties.

3. Define the rule's destination host or network by name or interface, IP address, and netmask. Under **Destination Host/Network**, perform the following:

   - Click **Name**.
   - In the **Name** box, enter the name of the destination host or network

     or

   - From the **Interface** list, select an interface name.
   - In the **IP address** box, type the IP address of the destination host or network.
   - In the **Mask** box, type the netmask of the destination host or network, or select a netmask from the list.

     Browse lets you select an existing host or network under **Select Host/Network** to populate the **Name**, **Interface**, **IP address**, and **Mask** boxes with the selected host or network's properties.

4. Define the additional parameters associated with the action type you selected in Step 1. The area that appears at the bottom of the dialog box depends on the type of action selected. Each of the action types has an associated option area in which you can configure the additional rule parameters.

5. Click **OK** to create the rule, or **Cancel** to discard your changes.

   If you click **OK**, the new rule is added to your firewall security policy and appears in the **AAA Rules** tab.

Alternatively, you can click **Insert Before** or **Insert After** on the **Rules** menu to add a rule before or after a selected rule. The **Insert Rule Before** or **Insert Rule After** dialog box appears, letting you configure the rule you want to add.

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

Edit NAT

Configuration>Host/Networks>Edit>Edit host/network>NAT

The **Edit host/network>NAT** dialog box lets you modify the address translation rules enforced by a Firewall when network packets destined to or originating from the selected host or network are transferred between two interfaces attached to the firewall unit (inter-interface communications). In this dialog box, you can only modify translation rules between the selected interface and interfaces of lower security levels. You cannot modify NAT rules for networks or hosts defined on the interface with the lowest security level (typically, the outside interface).

Note: Both translation rules and access rules are required for the firewall to allow hosts on low security interfaces to initiate connections to hosts on high security interfaces. The translation rules are necessary to create mapping of the actual address of the host on the high security interface to the address that it will be identified as on the low security interface. The access rules can then permit or deny traffic to the host on the high security interface.

For the selected host or network, you can modify/change one type of NAT rule per interface. The following types of NAT rules are valid:

- **Static**—Static NAT rules expose all IP services on an internal host to external users. They also override dynamic NAT rules that apply to a specific host or network. Static rules expose the address of the host or network on higher security interfaces to hosts on lower security interfaces, making those addresses visible to the lower security interface. In this case, hosts with static address translations on either interface can initiate connections assuming the appropriate access rules are defined to enable the connections. For more information on static NAT and its uses, refer to Understanding Static NAT.
- **Dynamic**—Dynamic NAT rules map between external, exposed IP address(es) and an internal network or host address. They hide specific networks and hosts behind a higher security interface from hosts on lower security interfaces. When using dynamic NAT rules, hosts behind the higher security interfaces can initiate connections to hosts behind lower security interfaces, but hosts behind lower security interfaces cannot initiate connections to the hosts behind the higher security interface. This effect results from the fact that such addresses are dynamically assigned by the firewall unit, rather than statically defined as static NAT rules.

  For the selected host or network, which resides behind the higher security interface, you can dynamically map its address to one of the following dynamic rule types:

  - **Address pool ID**—A pool can be defined as a range of IP addresses, a Port Address Translation (PAT) for a single, valid IP address for the less secure interface, or the IP address assigned to that less secure interface. This type of rule allows hosts routed through an interface with a higher security level to conduct sessions between hosts reached through an interface with a lower security level

without exposing the addresses behind the interface with the higher security level.

- **Same address**—Specifies that the firewall unit use the original address of the network or host. When translation rules of this type are defined, the firewall does not modify the packet headers. However, the firewall does allow the hosts on high security interfaces to initiate connections using their actual, untranslated addresses. This type of rule is different form a static rule because the address is not exposed to the lower security interface. This type of rule also differs from the *No NAT* type because No NAT prevents the affected hosts from initiating connections, and they have no visible address on the lower security interface.
- **No NAT**—The hosts on the high security interfaces cannot initiate connections to hosts on low security interfaces because the firewall does not perform an address mapping.

In other words, the firewall dynamically maps a valid IP address from the selected type to the lower security interface for connections traversing the firewall between the selected host/network and another node. For example, your internal network hosts can conduct outbound connections using a dynamic rule. For each internal host that requests an outbound connection, the firewall unit dynamically maps the request to the IP address. For more information on dynamic NAT rules and its uses, refer to Understanding Dynamic NAT.

The following sections are included in this Help topic:

- Field Descriptions
- Editing Dynamic NAT rules
- Editing Static NAT rules

Field Descriptions

The **Edit host/network>NAT** dialog box displays the following fields:

- **Static**—Clicking this option defines a permanent map between the internal IP address and a valid IP address on the lower security interface. This rule allows hosts from the lower security interface to gain access to the selected host or network, and vice versa. When this option is selected, the **Static** box and the **Advanced** button appears.
  - **IP address box**—Identifies the IP address (translated address) that is exposed to the interface from which the network or host's address is hidden. The Firewall uses this address to replace the network or host's address for any network packets that traverse from the interface on which the network or host exists to the interfaces listed in rule. This value is the specific translated IP address to which you want to map the original addresses of the translated object. You can define exactly one address.
  - **Advanced**—Clicking this button opens the **Static NAT Options** dialog box, from which you can configure the maximum connections permitted through this static address, the maximum number of embryonic connections allowed, and whether the firewall unit generates random sequence numbers for TCP packets belonging to a translated session.
- **Dynamic**—Clicking this option defines a dynamic NAT rule. The rule dictates which address pool is used to translate addresses for the host or network being added when the host initiates a connection passing through the interface. When this option is selected, the **Addresses Pool ID** list and the **Manage Pools** button appear.
  - **Address Pool ID**—Identifies the type of dynamic NAT rule to define for the selected host or network. You can select one of the following values in this list:

        - **No NAT**—Specifies that no dynamic NAT rule be used for the selected host or network. If an existing dynamic NAT rule covers the selected address (such as one for the network to which a host address belongs) or the selected interfaces is the outside interface, this option does not appear. If there is an existing rule, you can edit that rule on the **Configuration> Translation Rules** tab.
        - **same address**—Specifies that the firewall unit use the original IP address of the selected host or network to access hosts on the interface specified in the dynamic rule. This type of rule is different from a static rule because the address is not exposed to the lower security interface.
        - <***ID_number***>—Specifies that the firewall unit use the address(es) defined by this address pool for the selected network or host. For PAT-based rules, this address can be a valid IP address or the address that is assigned to the external interface. This list of pools only includes the predefined pools on lower security interfaces.
    - **Manage Pools**—Clicking this button opens the **Manage Global Address Pools** dialog box, from which you can view, add to, or delete from the existing address pool definitions.
- **OK**—Retains your changes and closes the **Edit host/network>NAT** dialog box.
- **Cancel**—Clears any changes you may have made and returns to the **Configuration>Hosts/Networks** tab.
- **Help**—Provides more information.

Editing a Dynamic NAT Rule

Follow these steps to edit a dynamic NAT rule:

1. Select the host or network you want to modify and click **Edit** on the **Configuration>Hosts/Networks** tab.
2. The **Edit host/network** dialog box appears.
3. Click the **NAT** tab.
4. Click the **Dynamic** option.
5. The **Addresses Pool ID** list and the **Manage Pools** button appear.
6. To modify the global address pool to use for this dynamic NAT rules, select the corresponding ID value in the **Address Pool ID** list.
7. For each interface that you want to modify a dynamic NAT rule, repeat Steps 3 and 4.
8. Alternatively, you can modify static NAT rules for an interface.
9. To retain your changes and close the **Edit host/network>NAT** dialog box, click **OK**.
10. Click **Apply** to activate your changes on the firewall.

Editing Static NAT

Follow these steps to modify a static NAT rule:

1. Select the host or network you want to modify on the **Configuration>Hosts/Networks** tab and click **Edit**.
2. The **Edit host/network** dialog box appears.
3. Click the **NAT** tab.
4. Click the **Static** option.
5. The IP address box and the **Advanced** button appear to the right of the **Static** option.
6. To modify the IP address (translated address) that is exposed to the interface from which the network or

host's address is hidden, enter that IP address in the box to the right of the **Static** option.

7. For each interface that you want to modify a static NAT rule, repeat Steps 3 and 4.
8. Alternatively, you can modify dynamic NAT rules for an interface.
9. To retain your changes and close the **Edit host/network>NAT** dialog box, click **OK**.
10. Click **Apply** to activate your changes on the firewall.

Copyright © 2001-2004, Cisco Systems, Inc.

Static NAT Options

Configuration>Hosts/Networks>Add>Create host/network>NAT>Advanced

In the **Static NAT Options** dialog box, you can configure the advanced features associated with the selected static NAT rule.

The following sections are included in this Help topic:

- Field Descriptions
- Configuring Advanced Static NAT Rule Options

Field Descriptions

The **Static NAT Options** dialog box displays the following fields:

- **Maximum Connection**—Identifies the maximum number of simultaneous TCP connections that are permitted at one time through the static NAT. The default value is **0**, which indicates an unlimited number of simultaneous TCP connections are permitted. To change the default value, enter the maximum number of TCP connections in the **Maximum Connection** box.
- **Embryonic Limit**—Identifies the embryonic connection limit to prevent TCP_SYN flood attacks. An embryonic connection is a TCP connection that is initiated but has not yet completed. Every TCP connection is embryonic until the TCP three-way handshake is completed, at which point the firewall allows for an exchange of data between the given client and server. The default value is **0**, which means unlimited embryonic connections are permitted. To change the default value, enter the maximum number of embryonic connections in the **Embryonic Limit** box.
- **Randomize Sequence Number**—Instructs the firewall to randomize TCP sequence numbers to minimize the risk of initial sequence number prediction attacks. By default, the **Randomize Sequence Number** check box is selected. Clear this check box only if you are using another inline firewall that randomizes TCP sequence numbers.

Configuring Advanced Static NAT Options

Follow these steps to configure the advanced options for a static NAT rule:

1. To define advanced options for a static NAT rule, click **Advanced** in the **Create host/network>NAT (Network Address Translation)** dialog box. The **Static NAT Options** dialog box appears.
2. To specify the maximum number of simultaneous connections that can use this translation rule, enter the number in the **Maximum Connection** box. The firewall unit enforces this value against new session requests.
3. To specify the maximum number of simultaneous embryonic links that can use this translation rule, enter the number in the **Embryonic Limit** box. The firewall unit enforces this value against new session requests by restricting the number of session requests that have not completed the handshake. This feature enables you to guard against TCP_SYN attacks. The value must be a whole number smaller than the **Maximum Connection** value.
4. Verify that the **Randomize Sequence Number** check box is selected.
   This option randomizes the sequence numbers generated for TCP/IP packets and reduces the risk of initial sequence number prediction attacks on the firewall unit. You should only clear this check box if you are using another inline firewall that randomizes TCP sequence numbers.
5. To retain your changes and close the **Static NAT Options** dialog box, click **OK**.

Copyright © 2001-2004, Cisco Systems, Inc.

Add NAT

Configuration>Hosts/Networks>Add>Create host/network>NAT

In the **Create host/network>NAT (Network Address Translation)** dialog box, you can define two types of address translation rules enforced by a PIX Firewall when network packets destined to or originating from the selected host or network are transferred between two interfaces attached to the firewall unit (inter-interface communications). In this dialog box, you can only define translation rules between the selected interface and interfaces of lower security levels. You cannot define NAT rules for networks or hosts defined on the interface with the lowest security level (typically, the outside interface).

Note: Both translation rules and access rules are required for the firewall to allow hosts on low security interfaces to initiate connections to hosts on high security interfaces. The translation rules are necessary to create mapping of the actual address of the host on the high security interface to the address that it will be identified as on the low security interface. The access rules can then permit or deny traffic to the host on the high security interface.

For the selected host or network, you can define up to one type of NAT rule per interface. The following types of NAT rules are valid:

- **Static**—Static NAT rules expose all IP services on an internal host to external users. They also override dynamic NAT rules that apply to a specific host or network. Static rules expose the address of the host or network on higher security interfaces to hosts on lower security interfaces, making those addresses visible to the lower security interface. In this case, hosts with static address translations on either interface can initiate connections assuming the appropriate access rules are defined to enable the connections. For more information on static NAT and its uses, refer to Understanding Static NAT.
- **Dynamic**—Dynamic NAT rules map between external, exposed IP address(es) and an internal network or host address. They hide specific networks and hosts behind a higher security interface from hosts on lower security interfaces. When using dynamic NAT rules, hosts behind the higher security interfaces can initiate connections to hosts behind lower security interfaces, but hosts behind lower security interfaces cannot initiate connections to the hosts behind the higher security interface. This effect results from the fact that such addresses are dynamically assigned by the firewall unit, rather than statically defined as static NAT rules.

  For the selected host or network, which resides behind the higher security interface, you can dynamically map its address to one of the following dynamic rule types:

  - **Address pool ID**—A pool can be defined as a range of IP addresses, a Port Address Translation (PAT) for a single, valid IP address for the less secure interface, or the IP address assigned to that

less secure interface. This type of rule allows hosts routed through an interface with a higher security level to conduct sessions between hosts reached through an interface with a lower security level without exposing the addresses behind the interface with the higher security level.

- **Same address**—Specifies that the firewall unit use the original address of the network or host. When translation rules of this type are defined, the firewall does not modify the packet headers. However, the firewall does allow the hosts on high security interfaces to initiate connections using their actual, untranslated addresses. This type of rule is different form a static rule because the address is not exposed to the lower security interface. This type of rule also differs from the *No NAT* type because No NAT prevents the affected hosts from initiating connections, and they have no visible address on the lower security interface.
- **No NAT**—The hosts on the high security interfaces cannot initiate connections to hosts on low security interfaces because the firewall does not perform an address mapping.

In other words, the firewall dynamically maps a valid IP address from the selected type to the lower security interface for connections traversing the firewall between the selected host/network and another node. For example, your internal network hosts can conduct outbound connections using a dynamic rule. For each internal host that requests an outbound connection, the firewall unit dynamically maps the request to the IP address. For more information on dynamic NAT rules and its uses, refer to Understanding Dynamic NAT.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Defining Dynamic NAT Rules
- Defining Static NAT Rules

Important Notes

Consider the following notes and usage guidelines before defining a NAT rule for the selected host or network:

- Only those enabled interfaces with lower security level values than the interface for which you are defining this host or network appear in this **Create host/network>NAT (Network Address Translation)** dialog box.
- A *valid IP address* refers to an IP address that is routable on the network directly attached to the exposing interface.
- Invalid IP addresses are also referred to as *reserved addresses*, which are IP addresses restricted to special purposes, such as internal domain or Internet service provider network usage. Such addresses cannot be legally routed on the network directly attached to the exposing interface.
- Because PAT requires port information, only TCP, UDP, and ICMP echo/echo-reply operate with PAT.
- If you expose your internal DNS servers using a static NAT rule, you do not benefit from the address hiding feature provided by translation rules. External users can simply request information about your trusted networks from the DNS servers that you expose.
- Because static NAT rules take precedence over dynamic NAT rules, you can use a static NAT rule to force a specific translation while allowing other communications to be translated using the more generic dynamic NAT rules.

Field Descriptions

The **Create host/network>NAT (Network Address Translation)** dialog box displays the following fields:

- **Static**—Selecting this option defines a permanent map between the internal IP address and a valid IP address on the lower security interface. This rule allows hosts from the lower security interface to gain access to the selected host or network, and vice versa. When this option is selected, the **Advanced** button appears.
  - **IP Address box**—Identifies the IP address (translated address) that is exposed to the interface from which the network or host's address is hidden. The Firewall uses this address to replace the network or host's address for any network packets that traverse from the interface on which the network or host exists to the interfaces listed in the rule. This value is the specific translated IP address to which you want to map the original addresses of the translated object. You can define exactly one address.
  - **Advanced**—Clicking this button opens the **Static NAT Options** dialog box, from which you can configure the maximum connections permitted through this static address, the maximum number of embryonic connections allowed, and whether the firewall unit generates random sequence numbers for TCP packets belonging to a translated session.
- **Dynamic**—Clicking this option defines a dynamic NAT rule. The rule dictates which address pool is used to translate addresses for the host or network being added when the host initiates a connection passing through the interface. When this option is selected, the **Addresses Pool ID** list and the **Manage Pools** button appear.
  - **Address Pool ID**—Identifies the type of dynamic NAT rule to define for the selected host or network. You can select one of the following values in this list:
    - **No NAT**—Specifies that no dynamic NAT rule be used for the selected host or network. If an existing dynamic NAT rule covers the selected address (such as one for the network to which a host address belongs) or the selected interfaces is the outside interface, this option does not appear. If there is an existing rule, you can edit that rule on the **Configuration> Translation Rules** tab.
    - **same address**— Specifies that the firewall unit use the original IP address of the selected host or network to access hosts on the interface specified in the dynamic rule. This type of rule is different from a static rule because the address is not exposed to the lower security interface.
    - ***<ID_number>***—Specifies that the firewall unit use the address(es) defined by this address pool for the selected network or host. For PAT-based rules, this address can be a valid IP address or the address that is assigned to the external interface. This list of pools only includes the predefined pools on lower security interfaces.
  - **Manage Pools**—Clicking this button opens the **Manage Global Address Pools** dialog box, from which you can view, add to, or delete from the existing address pool definitions.
- **Back**—Returns to the **Create host/network>Static Route** dialog box.
- **Finish**—Creates the host or network and returns to the **Configuration>Hosts/Networks** tab.
- **Cancel**—Clears any changes you may have made and returns to the **Configuration>Hosts/Networks** tab.
- **Help**—Provides more information.

Defining Dynamic NAT Rules

Follow these steps to define a dynamic NAT rule:

1. Click the **Dynamic** option in the **Create host/network>NAT (Network Address Translation)** dialog box.
2. The **Addresses Pool ID** list and the **Manage Pools** button appear.
3. To specify the global address pool to use for this dynamic NAT rules, select the corresponding ID value in the **Address Pool ID** list.
4. For each interface that you want to define a dynamic NAT rule, repeat Steps 1 and 2.
5. Alternatively, you can define static NAT rules for an interface.
6. To create the network or host that you have defined, click **Finish**.
7. To commit your changes and activate the new host or networks, click **Apply**.

Defining Static NAT Rules

Follow these steps to define a static NAT rule:

1. Click the **Static** option in the **Create host/network>NAT (Network Address Translation)** dialog box.
2. The IP address box and the **Advanced** button appear to the right of the **Static** option.
3. To specify the IP address (translated address) that is exposed to the interface from which the network or host's address is hidden, enter that IP address in the box to the right of the **Static** option.
4. For each interface that you want to define a static NAT rule, repeat Steps 1 and 2. Alternatively, you can define dynamic NAT rules for an interface.
5. To create the host or network that you have defined, click **Finish**.
6. To commit your changes and activate the new host or networks, click **Apply**.

Copyright © 2001-2004, Cisco Systems, Inc.

Add Static Route

Configuration>Hosts/Networks>Add>Create host/network>Static Route

Unless one of the following criteria is met (in which case, click **Next** to skip this dialog box), you should define a static route to ensure that the firewall unit correctly forwards network packets destined to the host or network:

- The network or host you are defining is connected directly to the selected interface
- Dynamic routing is enabled for the interface to discover the routes
- A more general static route, such as the default route, is already defined

After you enter the basic information for a host or network, PDM queries the current static routing table (including directly connected networks) to determine how the firewall should route packets destined to the specified IP address and mask. If the routing table query reveals that such packets are routed to an interface different from the one specified in the **Configuration>Hosts/Networks>Add>Create host/network> Basic Information** dialog box, PDM prompts you to define a static route by displaying the **Create host/ network>Static Route** dialog box. If you selected the **Never ask me this question again** check box during this administrative session, PIX Device Manager does not query the static routing table on the firewall, and skips the **Create host/network>Static Route** dialog box.

You can also use a static route to override any dynamic routes that are discovered for this host or network by specifying a static route with a lower metric than the discovered dynamic routes. To create a static route for a host or network, you must define the IP address and metric for the hop gateway to which the firewall will forward packets destined to the selected host or network. You can also define multiple static routes for a host or network. To do so, complete the **Create host/network Wizard**, and then add additional routes using the **Configuration>System Properties>Routing>Static Route** panel.

The following sections are included in this Help topic:

- Field Descriptions
- Defining Static Routes

Field Descriptions

The **Create host/network>Static Route** dialog box displays the following fields:

- **Define Static Route**—Select this check box to define a static route for this host or network.
- **Gateway IP Address**—Identifies the IP addresses of the default gateway (or the next hop gateway) that forwards any network packets destined to this network or host.

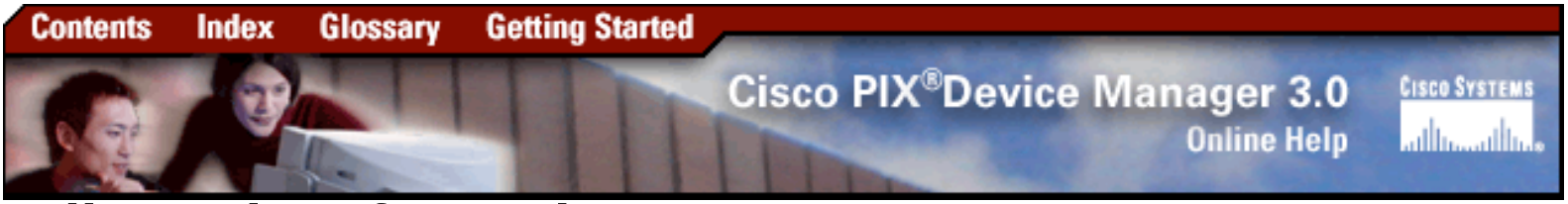
- **Metric**—Identifies the priority for using a specific route. When routing network packets, a PIX Firewall unit uses the rule with the most specific network within the rule's definition. Only in cases where two routing rules have the same network is the metric used to determine which rule will be applied. If they are the same, the lowest metric value takes priority. If no routing rule exists, the network packet is dropped, and if the gateway is not detected (dead), the network packet is dropped. A *metric* is a measurement of the expense of a route based on the number of hops (hop count) to the network on which a specific host resides. Hop count refers to the number of networks that a network packet must traverse, including the destination network, before it reaches its final destination. Because the hop count includes the destination network, all directly connected networks have a metric of 1. For the metric value, you can specify a number between 1 and 15.
- **Never ask me this question again**—Select this check box if you do not want to be prompted to define static routes for the remainder of this administrative session. You should only select this option if you are defining hosts and networks for an interface on which you have enabled dynamic routes and for which you do not need to override any of the discovered routes.
- **Back**—Returns you to the **Create host/network>Basic Information** dialog box.
- **Next**—Continues to the **Create host/network>NAT (Network Address Translation)** dialog box.
- **Cancel**—Clears any changes you may have made and returns to the **Configuration>Hosts/Networks** tab.
- **Help**—Provides more information.

Defining Static Routes

Follow these steps to define a static route for the selected host or network:

1. To specify that you want to define a static route, select the **Define Static Route** check box in the **Create host/network>Static Route** dialog box.
2. To identify the default or hop gateway used to reach the selected host or network from this interface, enter or click that address in the **Gateway IP Address** list.
3. To specify the priority for using this route, enter the number in the **Metric** box.
   Only in cases where two routing rules have the same network is the metric used to break the tie. In the case of a tie, the lowest metric value wins.
4. If you do not want to be prompted to define static routes for the remainder of this administrative session, select the **Never ask me this question again** check box.
5. To continue defining the settings for this host or network, click **Next**.
   The **Create host/network>NAT (Network Address Translation)** dialog box appears.

Copyright © 2001-2004, Cisco Systems, Inc.



Edit Basic Information

Configuration>Hosts/Networks>Edit>Edit host/network>Basic Information

In the **Edit host/network>Basic Information** dialog box, you can modify you specify values for the IP address, netmask, interface, and name of a host or network. This information provides the basic identification information for that host or network. PIX Device Manager uses the name and IP address/netmask pair to resolve references to this host or network in the source and destination conditions of access rules and in translation rules. PIX Device Manager uses the interface value to apply access and translation rules that reference this host or network to the correct interface. The interface delivers network packets to the host or network, and therefore, it enforces the rules that reference that host or network.

The following sections are included in this Help topic:

- Field Descriptions
- Editing Basic Information

Field Descriptions

The **Edit host/network>Basic Information** dialog box displays the following fields:

- **IP Address**—Identifies the IP address of the host or network you want to modify.
- **Mask**—(address mask) Identifies the bits of the IP address to treat as wildcard. When you define a host, this value must be 255.255.255.255. For example, to define a Class B network, with an address space between 192.168.0.0 and 192.168.255.255, you would specify an IP address value of 192.168.0.0 and a mask value of 255.255.0.0. To define the host, 192.168.1.1, on this network, you would specify an IP address value of 192.168.1.1 and a mask value of 255.255.255.255.
- **Interface**—Identifies the interface in the firewall unit from which this host or network is reachable. The host or network must either be directly connected to this interface or reside behind a gateway that is reachable from this interface.
- **Name [Recommended]**—Identifies the name used when referencing this host or network in access and translation rules. This name may include up to 16 characters. Valid characters are a to z, A to Z, 0 to 9, period ("."), and an underscore ("_"). The name must start with an alphabetic character. We recommend that you name all hosts and networks.
- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Editing Hosts and Networks

Follow these steps to edit the basic identification information for the host or network:

1. Select the host or network you want to modify and click **Edit** on the **Configuration>Hosts/Networks** tab. The **Edit host/network** dialog box appears.
2. To modify the address used to reach the host or network, enter the address in the **IP Address** box.
3. To modify the network mask value that corresponds to the network or host that you are defining, click the desired value in the **Mask** list.
   If you are defining a host, you must click the 255.255.255.255 value.
4. If the selected interface does not correspond to the interface from which the host or network is directly reachable, click the correct interface name in the **Interface** list.
   By default, this value is the interface selected on the **Configuration>Hosts/Networks** tab.
5. To modify the name used when referencing this host or network within access or translation rules, enter the name in the **Name (Recommended)** box.
   While this value is optional, it is recommended.
6. To retain your changes and close the **Edit host/network** dialog box, click **OK**.
7. **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

Copyright © 2001-2004, Cisco Systems, Inc.

Edit Routing

Configuration>Hosts/Networks>Edit>Edit host/network>Routing

In the **Configuration>Hosts/Networks>Edit>Edit host/network>Routing** dialog box, you can edit a static route to ensure that the firewall unit correctly forwards network packets destined to the host or network. You can also use a static route to override any dynamic routes that are discovered for this host or network by specifying a static route with a lower metric than the discovered dynamic routes. To create a static route for a host or network, you must define the IP address and metric for the hop gateway to which the firewall will forward packets destined to the selected host or network. You can also define multiple static routes for a host or network. To do so, complete your changes in the **Edit host/network>Routing** dialog box, and then add additional routes using the **Routing>Static Route** panel on the **Configuration>System Properties** tab.

The following sections are included in this Help topic:

- Field Descriptions
- Editing Static Routes

Field Descriptions

The **Edit host/network>Routing** dialog box displays the following fields:

- **Define Static Route**—Select this check box to define a static route for this host or network.
- **Gateway IP Address**—Identifies the IP addresses of the default gateway (or the next hop gateway) that forwards any network packets destined to this network or host.
- **Metric**—Identifies the priority for using a specific route. When routing network packets, a Cisco firewall unit uses the rule with the most specific network within the rule's definition. Only in cases where two routing rules have the same network is the metric used to break the tie. In the case of a tie, the lowest metric value wins. If no routing rule exists, the network packet is dropped, and if the gateway is not detected (dead), the network packet is dropped. A *metric* is a measurement of the expense of a route based on the number of hops (hop count) to the network on which a specific host resides. Hop count refers to the number of networks that a network packet must traverse, including the destination network, before it reaches its final destination. Because the hop count includes the destination network, all directly connected networks have a metric of 1. For the metric value, you can specify a number between 1 and 15.
- **OK**—Retains your changes and closes the **Edit host/network>Routing** dialog box.
- **Cancel**—Clears any changes you may have made and returns to the **Configuration>Hosts/Networks** tab.
- **Help**—Provides more information.

Editing Static Routes

Follow these steps to modify a static route for the selected host or network:

1. Select the host or network you want to modify on the **Configuration>Hosts/Networks** tab and click **Edit**. The **Edit host/network** dialog box appears.
2. Click the **Routing** tab.
3. Follow these steps to modify the static route for the selected host or network:

    1. To specify that you want to modify the static route, select the **Define Static Route** check box.
    2. To modify the default or hop gateway used to reach the selected host or network from this interface, enter or click that address in the **Gateway IP Address** list.
    3. To modify the priority for using this route, enter the number in the **Metric** box.
       Only in cases where two routing rules have the same network is the metric used to break the tie. In the case of a tie, the lowest metric value wins.
4. To retain your changes and close the **Edit host/network>Routing** dialog box, click **OK**.
5. Click **Apply** to activate your changes on the firewall.

Copyright © 2001-2004, Cisco Systems, Inc.

DHCP Client

Monitoring>DHCP Client

DHCP Client Lease Information panel displays DHCP-assigned interface parameters when DHCP addressing is configured on the outside interface of the firewall. A snapshot of the current DHCP lease information is displayed. The display is not automatically updated when the DHCP lease is renewed or rebound. To view updated DHCP client lease information, you must click **Refresh**.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

Important Notes

DHCP Client monitoring is available only when the outside interface of the firewall is configured for DHCP addressing via the **Configuration>System Properties>Interfaces** panel.

Field Descriptions

The **DHCP Client Lease Information** panel displays the following fields:

- **DHCP Client Lease Information**—Displays the parameters of the DHCP lease for the outside interface, including the assigned IP address, subnet mask, DHCP server IP address, lease time information, default gateway IP address, and other DHCP-related information.
- Refresh—Loads current DHCP client lease information from the firewall unit for display.

Copyright © 2001-2004, Cisco Systems, Inc.

PDM Log Viewer

Monitoring>PDM Log>PDM Log Viewer

PDM Log Viewer displays the syslog messages currently in the PDM Log buffer on the PIX. A snapshot of the PDM Log buffer contents on the PIX are displayed. The display is not automatically updated as new syslog messages are generated by the PIX. To view new syslog messages, you must refresh or clear the display.

The following sections are included in this Help topic:

- Field Descriptions
- Using PDM Log Viewer

Field Descriptions

The **PDM Log Viewer** panel displays the following fields:

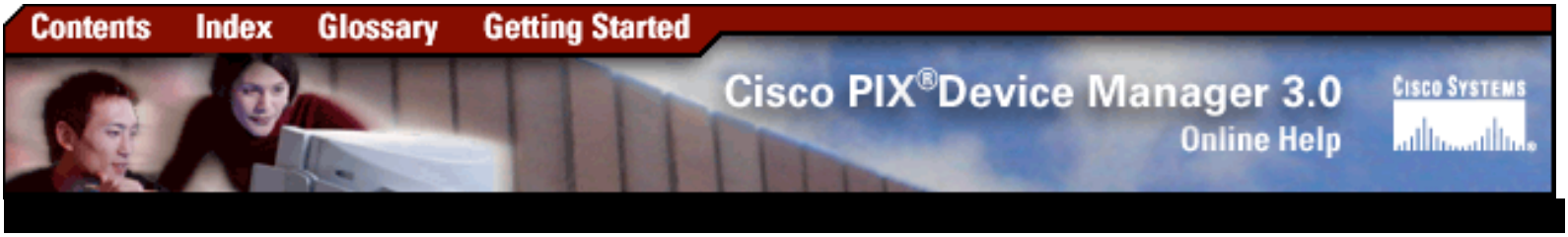
- **Severity**—Displays the severity of the condition described by the message. The lower the number, the more serious the condition. Levels are defined as follows:
  - **0 = Emergency (System unusable)**
  - **1 = Alert (Immediate action needed)**
  - **2 = Critical (Critical condition)**
  - **3 = Error (Error condition)**
  - **4 = Warning (Warning condition)**
  - **5 = Notification (Normal but significant condition)**
  - **6 = Informational (Informational message only)**
  - **7 = Debugging (Appears during debugging only)**
- **Time**—Displays the PIX date and time when the syslog message was generated.
- **Message ID: Description**—Displays the unique syslog message ID and message description. Refer to the *System Log Messages for the Cisco PIX Firewall* for more information about syslog messages.
- **Refresh**—Refreshes the current display by retrieving the syslog messages currently in the PDM Log buffer on the PIX.
- **Clear**—Clears the syslog messages currently in the PDM Log buffer on the PIX and refreshes the display. Note that ALL levels of syslog messages in the PIX buffer will be cleared, and not just the levels which have selected for viewing.
- **Close**—Closes **PDM Log Viewer**.

Using the PDM Log Viewer

Follow these steps to sort the syslog messages in the display:

1. Click one of the table column headings: **Severity**, **Time** or **Message ID:Description**. The table will be sorted in ascending or descending order each time you click on the column heading.

Copyright © 2001-2004, Cisco Systems, Inc.



PDM Log

Monitoring>PDM Log

The **PDM Log** panel lets you view syslog messages which are captured in the PDM Log buffer in Firewall memory. You may select the level of syslog messages you want to view. When you view the PDM Log, all of the buffered syslog messages at and below the logging level you choose will be displayed.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Viewing the PDM Log

Important Notes

To enable **PDM Logging**:

1. First enable logging in **Configuration>System Properties>Logging>Logging Setup**.
2. Enable PDM logging in **Configuration>System Properties>Logging>PDM Logging**.

Field Descriptions

PDM Bogging displays the following fields:

- **Logging Level**—Lets you choose the level of syslog messages to view. The available logging levels are determined by the PDM Logging Level configured using **Configuration>System Properties> Logging>PDM Logging**.
- **View**—Opens **PDM Log Viewer**.

Viewing the PDM Log

Follow these steps to view the PDM Log:

1. Click the desired logging level in the **Logging Level** list.
2. Click **View**.

Copyright © 2001-2004, Cisco Systems, Inc.

Logging Setup

Configuration>System Properties>Logging>Logging Setup

The **Logging Setup** panel lets you enable system logging on the firewall, view syslog ID levels, modify syslog ID levels, and suppress syslog messages.

The following sections are included in this Help topic:

- Field Descriptions
- Enabling System Logging
- Disabling System Logging
- Viewing Syslog IDs
- Editing Syslog IDs
- Restoring Syslog IDs to Default
- Resetting to Last Applied Settings

Field Descriptions

The **Logging Setup** panel displays the following fields:

- **Enable logging**—Turns on logging for the main PIX Firewall.
- **Enable logging on the failover Standby unit if you have one**—Turns on logging for the standby Cisco firewall unit, if available.
- **Syslog ID Table View**—Selects the information to be displayed in the Syslog ID Table. Options are defined as follows:
  - **View suppressed syslog IDs only**—Displays only those syslog IDs that have been configured as suppressed.
- **View syslog IDs with changed levels only**—Displays only those syslog IDs with logging levels that have changed from their default values.
- **View suppressed or changed level syslog IDs only**—Displays only those syslog IDs with logging levels that either have been configured as suppressed or have changed from their default values.
- **View all syslog IDs**—Displays the entire list of syslog IDs.

- **Edit**—Lets you modify the logging level or suppression setting for a syslog message.
- **Restore Defaults**—Restores the default logging level for all syslog IDs.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby

firewall unit. See Configuration Changes.

- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Enabling System Logging

Follow these steps to enable system logging on the firewall:

1. Select the **Enable logging** check box.
2. If applicable, select the **Enable logging on the failover standby unit if you have one** check box.
3. Click **Apply**.

Disabling System Logging

Follow these steps to disable system logging on the firewall:

1. Clear the **Enable logging** check box.
2. If applicable, clear the **Enable logging on the failover standby unit if you have one** check box.
3. Click **Apply**.

Viewing Syslog IDs

Follow these steps to view syslog IDs:

1. Click the **Syslog ID Table View** drop-down list.
2. Choose the option that you would like to view in the Syslog ID table.
3. Click **Apply**.

Editing Syslog IDs

Follow these steps to edit syslog ID settings:

1. In the Syslog ID table, select the syslog ID entries that you would like to edit.
2. Click **Edit**.
3. The Edit panel appears. This panel lets you modifiy syslog logging level and suppression settings.

Restoring Syslog ID Defaults

To restore syslog ID defaults, click **Restore Defaults** and then click **Apply**. All syslog IDs are restored to their default settings.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

PDM Logging

Configuration>System Properties>Logging>PDM Logging

The **PDM Logging** panel lets you set the level of logging used on the firewall and the size of the logging buffer.

The following sections are included in this Help topic:

- Field Descriptions
- Changing PDM Logging Level
- Changing PDM Logging Buffer Size
- Resetting to Last Applied Settings

Field Descriptions

The **PDM Logging** panel displays the following fields:

- **Logging Level**—Defines the level of logging messages to be retained by the system. These values range from **Debugging**, which logs all possible messages, to **Emergencies**, which only logs the subset of messages related to emergency conditions. The **Disabled** choice disables message logging.
- **Logging Buffer**—Defines the number of logging messages that will be retained. If more messages are received, the oldest existing messages will be purged from the log.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Changing PDM Logging Level

Follow these steps to change the level of PDM log messages retained by the firewall:

1. Select the desired logging level from the **Logging Level** list. **Debugging** is the most general level (which will capture the most messages), and **Emergency** is the most specific. Selecting **Disabled** turns off message logging.
2. Click **Apply**.

Changing PDM Logging Buffer Size

Follow these steps to change the size of the PDM logging buffer:

1. Enter the desired size of the buffer in **Logging Buffer** box.
2. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

PPPOE Client

Monitoring>PPPOE Client

PPPOE (Point to Point Protocol over Ethernet) allows the firewall to automatically connect users on the **inside** interface to Internet Service Providers (ISPs) via the **outside** interface. **Monitoring>PPPOE Client Information** displays information about current PPPOE client connections.

Field Descriptions

Monitoring>PPPoE Client Information displays the following fields:

- **PPPoE Client Information**—Displays information about active PPPoE client connections.
- Refresh—Loads current PPPoE client information from the firewall unit for display.

Copyright © 2001-2004, Cisco Systems, Inc.

User Licenses

Monitoring>User Licenses

Monitoring>User Licenses displays the number of current users which is subtracted from the maximum users for your firewall licensing agreement. For more information about PIX Firewall licensing, see http://www.cisco.com/go/pix.

Field Descriptions

Monitoring>User Licenses displays the following fields:

- **Licenses in Use**—Displays the number of active licenses.
- **Number of Licenses Available**—The maximum users for your firewall licensing agreement. Unlimited or a number.
- **Refresh**—Loads current user licensing information from the firewall unit for display.

Copyright © 2001-2004, Cisco Systems, Inc.

IPSec Tunnels or L2TP/PPTP New Graph

Monitoring>VPN Connection Graphs>IPSec Tunnels or L2TP/PPTP>New Graph

Monitoring>VPN Connection Graphs>IPSec Tunnels or L2TP/PPTP>New Graph displays tables or graphs that provide information about the following:

- IKE Active Tunnels
- IPSec Active Tunnels
- L2TP Active Tunnels
- L2TP Active Sessions
- PPTP Active Tunnels
- PPTP Active Sessions

The following sections are included in this Help topic: :

- Graph Tab
- Table Tab
- Export
- Print
- Bookmark

For information about getting started with PDM Graphs, see Monitoring>Building Graph Windows.

1. To view the **New Graph** window, select the tunnel or session type from **Available Graphs for:**.
2. Click **Add >>**.
3. Then select the entry that is added to the **Selected Graph(s)** list and click

.
4. The system displays the selected graph in the **New Graph** window.
5. When you are finished with the **New Graph** window, click the X control in the upper right corner of the window to close it.

Graph Tab

The **Graph** tab lets you view a line graph showing the number of active tunnels at a specific time.

View—The **View** list on the **Graph** tab lets you select the duration of the graph display and the frequency of data points on the graph. The available options include the following:

- Real-time, data every 10 sec
- Last 10 minutes, data every 10 sec
- Last 60 minutes, data every 1 min
- Last 12 hours, data every 12 min
- Last 5 days, data every 2 hours

X is the horizontal axis. Y is the vertical axis.

Tunnels/Sessions—The horizontal (X) axis of the line represents the number of active tunnels or sessions.

PIX Time—The vertical (Y) axis of the line graph represents the specific time at which the number of tunnels or sessions was recorded. This time is taken from the firewall system time and is converted to the local time zone at the site where the firewall is physically located.

Table Tab

The **Table** tab lets you view a line graph showing the number of active tunnels or sessions at each interval. Select the time between intervals from the **View** list on the **Graph** tab. You can change the size of a column by dragging the vertical separator between the two columns to a new location.

Time—The **Time** column on the **Table** tab represents the specific time at which the number of tunnels or sessions was recorded. This time is taken from the firewall system time and is converted to the local time zone at the site where the firewall is physically located.

Right column—The right column on the **Table** tab lists the number of active sessions or tunnels at each interval selected from the **View** list on the **Graph** tab.

Export

When you click **Export**, the system displays the **Save As** window, which lets you type a file name and select a folder in which to save the exported statistics.

Print

When you click **Print**, the system displays the **Print** window, which lets you select a printer for printing the selected graph or table. To print the selected graph or table, select the printer and click **OK**.

Bookmark

When you click **Bookmark**, the system displays **Cisco PIX Device Manager Bookmark**. To add a bookmark for a selected table or graph In Netscape Navigator, click the link provided and then select **Bookmarks** > **Add Bookmark** from the Netscape Navigator window. To add a a Favorite location for a selected table or graph to Internet Explorer, click the link and select **Favorites**>**Add to Favorites** from the Internet Explorer window.

Copyright © 2001-2004, Cisco Systems, Inc.

IPSec Tunnels

Monitoring>VPN Connection Graphs>IPSec Tunnels

To view the **IPSec Tunnels** panel, click the **Monitoring** tab and then select **VPN Connection Graphs**> **IPSec Tunnels** from the left frame.

The following sections are included in this Help topic:

- Available Graphs for:
- Graph Window
- Selected Graph(s)

IPSec operates in two phases. Phase 1 negotiates the security associations (SAs) used to establish a single, reusable secure tunnel between two IPSec peers. Phase 2 uses the Phase 1 tunnel to negotiate SAs and establish secure tunnels for transmitting user data. The **IPSec Tunnels** panel displays information about Phase 1 (IKE) and Phase 2 (IPSec) tunnels.

To view a graph, select the tunnel type from the **Available Graphs for:** list and click **Add >>**. Then select the entry that is added to the **Selected Graph(s)** list and click **Graph It**!. The system displays the selected graph in the **New Graph** window. When you are finished with the **New Graph** window, click the X control in the upper right corner of the window to close it.

For more information, see Monitoring>Building Graph Windows and Monitoring>Graph Windows.

Available Graphs for:

This list lets you monitor one of the following:

- IPSec Active Tunnels
- IKE Active Tunnels

Select the tunnel type and click **Add >>** to add the tunnel type to the **Selected Graph(s)** list.

IPSec Active Tunnels—This selection lets you monitor the number of currently active Phase 2 (IPSec) tunnels. Phase 2 tunnels are used for transmitting user data.

IKE Active Tunnels—This selection lets you monitor the number of currently active Phase 1 (IKE) tunnels. A single Phase 1 tunnel is used for each remote IPSec peer for negotiating the parameters used to establish Phase 2 (IPSec) tunnels.

Graph Window

The **Graph Window** list lets you select a customized graph.

Selected Graph(s)

The **Selected Graph(s)** list shows the graphs with which you are currently working. To display a graph, select an item from this list and click **Graph It!**. You can hold down the Shift key while making selections to select multiple graphs at the same time. The **New Graph** window that appears will include each selected graph for side-by-side comparison.

For more information, see Monitoring>Building Graph Windows and Monitoring>Graph Windows.

Copyright © 2001-2004, Cisco Systems, Inc.

L2TP

Monitoring>VPN Statistics>L2TP

To view the **L2TP Sessions** panel, click the **Monitoring** tab and then select **VPN Statistics**>**L2TP** from the left frame. The **L2TP Sessions** panel displays information about current L2TP sessions. Each row on the **L2TP Sessions** table represents one current L2TP session. To view details for session, select a row and click **View Details**.

The Layer Two Tunneling Protocol (L2TP) is an extension to the point-to-point protocol (PPP). L2TP merges Cisco's older Layer Two Forwarding (L2F) protocol with Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP can be used with IPSec encryption and is considered more secure against attack than PPTP. L2TP is available with Windows 2000 and Windows XP systems.

The following sections are included in this Help topic:

- Interface
- Remote IP
- Session ID
- User Name
- Pkts Sent
- Bytes Sent
- Pkts Received
- Bytes Received

Interface

The **Interface** column displays the interface name on your firewall over which the L2TP session is established.

Remote IP

The **Remote IP** column displays the IP address of the remote host that is establishing a L2TP session with the firewall.

Session Id

The **Session ID** column displays the session identifier for a specific L2TP session.

User Name

The **User Name** column displays the user name used for authentication when establishing the L2TP session.

Pkts Sent

The **Pkts Sent** column displays the number of packets sent over the L2TP session.

Bytes Sent

The **Bytes Sent** column displays the number of bytes sent over the L2TP session.

Pkts Received

The **Pkts Received** column displays the number of packets received over the L2TP session.

Bytes Received

The **Bytes Received** column displays the number of bytes received over the L2TP session.

Copyright © 2001-2004, Cisco Systems, Inc.

IKE SAs

Monitoring>VPN Statistics>IKE SAs

To view the **IKE SAs** panel, click the **Monitoring** tab and then select **VPN Statistics**>**IKE SAs** from the left frame.

The following sections are included in this Help topic:

- Source IP
- Destination IP
- State

The **IKE SAs** panel displays information about Phase 1 (IKE) security associations (SAs). A pair of IKE SAs is used to establish a single, reusable secure tunnel between two IPSec peers. This tunnel is then used to negotiate the security parameters required to establish Phase 2 (IPSec) SAs. For a list of VPN Standards supported by PIX Firewall, see More **VPN**.

Each row on the **IKE SAs** table represents one active IKE SA. You can sort the display by clicking any column heading.

Source IP

The **Source IP** column displays the IP address of the local interface on your firewall that is included in each active SA.

Destination IP

The **Destination IP** column displays the IP address of the interface on the remote IPSec peer that is included in each active SA.

State

The **State** column displays the current status of each active IKE SA.

Copyright © 2001-2004, Cisco Systems, Inc.

IPSec VPNs

Monitoring>VPN Statistics>IPSec VPNs

To view the **IPSec VPNs** panel, click the **Monitoring** tab and then select **VPN Statistics**>**IPSec VPNs** from the left frame. The **IPSec VPNs** panel displays information about Phase 2 (IPSec) security associations (SAs). A pair of IPSec SAs are required for each secure tunnel used to transmit user data.

Each row on the **IPSec VPNs** table represents one active IPSec SA. You can sort the display by clicking any column heading.

The following sections are included in this Help topic:

- Interface
- Local IP
- Service
- Remote IP
- Service
- Peer
- Encap Pkts
- Decap Pkts
- Error Pkts
- View Details

Interface

The **Interface** column displays the interface name on your firewall over which the SA is established.

Local IP

The **Local IP** column displays the IP address of the local interface on your firewall that is included in each active SA.

Service

The **Service** column displays the TCP or UDP service name or port number used by the local host on the active SA.

Remote IP

The **Remote IP** column displays the IP address of the interface on the remote host that is included in each active SA.

Service

The **Service** column displays the TCP or UDP service name or port number used by the remote host on the active SA.

Peer

The **Peer** column displays the IP address of the remote IPSec peer that established the SA.

Encap Pkts

The **Encap** column displays the number of packets encapsulated within IPSec headers over the active SA.

Decap Pkts

The **Decap Pkts** column displays the number of packets from which the IPSec headers have been removed over the active SA.

Error Pkts

The **Error Pkts** column displays the number of packets for which errors occurred during encapsulation or decapsulation.

View Details

Monitoring>VPN Statistics>IPSec VPNs>View Details shows advanced information about the VPN security associations (SAs) in the crypto maps which have been created and their related traffic statistics. The output is similar to the CLI command **show ipsec sa detail**. See the View Details and CLI command output examples which follow.

Note: Using View Details with a configuration containing several hundred SAs may produce a noticeable delay in PDM as the information provided by the PIX is parsed and displayed.

Example View Details Output

Details for jeffryp-pc-1/255.255.255.255/0/0 jeffryp-pix-prii/255.255.255.255/0/0 at Wed Mar 27 00:42:37 PST 2002

local ident (addr/mask/prot/port): (jeffryp-pc-1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (jeffryp-pix-prii/255.255.255.255/0/0)
current_peer: jeffryp-pix-prii
PERMIT, flags={origin_is_acl,}
#pkts encaps: 4989, #pkts encrypt: 4989, #pkts digest 4989
#pkts decaps: 5038, #pkts decrypt: 5038, #pkts verify 5038
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0
local crypto endpt.: 10.10.10.113, remote crypto endpt.: jeffryp-pix-prii
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 0
inbound esp sas:
inbound ah sas:
inbound pcp sas:
outbound esp sas:
outbound ah sas:
outbound pcp sas:

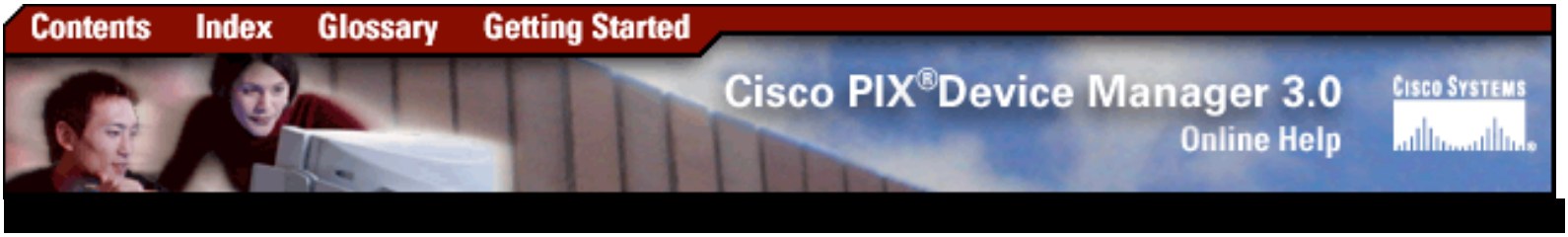
Example CLI Command Output (show ipsec sa detail)

Result of PIX command: "show ipsec sa detail"

interface: inside
Crypto map tag: inside_map, local addr. 10.10.10.113
local ident (addr/mask/prot/port): (jeffryp-pc-1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (jeffryp-pix-prii/255.255.255.255/0/0)
current_peer: jeffryp-pix-prii
PERMIT, flags={origin_is_acl,}
#pkts encaps: 4975, #pkts encrypt: 4975, #pkts digest 4975
#pkts decaps: 5024, #pkts decrypt: 5024, #pkts verify 5024
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0
local crypto endpt.: 10.10.10.113, remote crypto endpt.: jeffryp-pix-prii
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 458b13cf

inbound esp sas:
spi: 0xeb6f584e(3949942862)
transform: esp-des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: inside_map
sa timing: remaining key lifetime (k/sec): (4607998/28387)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x458b13cf(1166742479)
transform: esp-des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: inside_map
sa timing: remaining key lifetime (k/sec): (4607999/28387)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:

Copyright © 2001-2004, Cisco Systems, Inc.



PPTP

Monitoring>VPN Statistics>PPTP

To view the **PPTP Sessions** panel, click the **Monitoring** tab and then select **VPN Statistics**>**PPTP** from the left frame. The **PPTP Sessions** panel displays information about current PPTP sessions. Each row on the **PPTP Sessions** table represents one current PPTP session. To view details for the session, select a row and click **View Details**.

Point-to-Point Tunneling Protocol (PPTP) was introduced by Microsoft to provide secure remote access to Windows networks using Microsoft Point-to-Point Encryption (MPPE). Because of its vulnerability to attack, PPTP is generally only used where the greater security provided by IPSec authentication and encryption is not available or is not required. PPTP is available with Windows 95 and Windows 98 systems.

The following sections are included in this Help topic:

- Interface
- Remote IP
- Session ID
- User Name
- Pkts Sent
- Bytes Sent
- Pkts Received
- Bytes Received

Interface

The **Interface** column displays the interface name on your firewall over which the PPTP session is established.

Remote IP

The **Remote IP** column displays the IP address of the remote host that is establishing a PPTP session with the firewall.

Session Id

The **Session ID** column displays the session identifier for a specific PPTP session.

User Name

The **User Name** column displays the user name used for authentication when establishing the PPTP session.

Pkts Sent

The **Pkts Sent** column displays the number of packets sent over the PPTP session.

Bytes Sent

The **Bytes Sent** column displays the number of bytes sent over the PPTP session.

Pkts Received

The **Pkts Received** column displays the number of packets received over the PPTP session.

Bytes Received

The **Bytes Received** column displays the number of bytes received over the PPTP session.

Copyright © 2001-2004, Cisco Systems, Inc.

Welcome

Startup Wizard>Welcome

The Cisco PIX Firewall Device Manager (PDM) Startup Wizard will walk you through, step by step, the initial configuration of your firewall. As you click through the following screens, you will be prompted to enter information about your firewall and the Startup Wizard will apply these settings, so you should be able to start using your firewall right away.

The Startup Wizard will define the following in your configuration:

- A hostname for your firewall.
- A domain name for your firewall.
- A default gateway for your firewall.
- An enable password that is required to access PDM or the Command Line Interface (CLI) of the firewall.
- The speed and IP Address information of the outside interface on the firewall.
- If you are using a Auto Update Server to configure the firewall, you can specify the path to it from the wizard. This is configured in the Auto Update Server section of the Startup Wizard.
- The other interfaces of your firewall, such as the inside or DMZ interfaces, can be configured from the Startup Wizard.
- Network Address Translation (NAT) or Port Address Translation (PAT) Rules for your firewall.
- Dynamic Host Control Protocol (DHCP) settings for the inside interface, as a DHCP server.
- If you are using a PIX Firewall 501, PIX Firewall 506 or PIX Firewall 506E, the Startup Wizard will let you configure Cisco Easy VPN Remote device settings, which let the firewall act as a VPN client and to establish a VPN tunnel to the VPN headend.

more information about each of the above topics are available in the individual screens used to configure them by pressing the help button.

Before you begin using the Startup Wizard, make sure you have the following information available:

- A unique hostname to identify the firewall on your network.
- The outside interface IP address.
- The Firewall's default gateway.
- The IP addresses of your inside and other interfaces.
- The IP addresses to use for NAT or PAT configuration.
- The IP address range you will use for the DHCP server.

Remember:

- You can access the Startup Wizard at any time using the Wizards menu in PDM.
- The help button is an icon with a question mark.

- On subsequent Startup Wizard pages, you can click **Finish** to complete the wizard at any time. This sends changes made in the Startup Wizard to the firewall.

Copyright © 2001-2004, Cisco Systems, Inc.

Auto Update Configuration

Startup Wizard>Auto Update Configuration

The **Auto Update Configuration** panel lets you configure the firewall to be remotely managed from an Auto Update Server. Auto Update lets the firewall be configured and updated from a remote location, and upgrades to the software can be performed remotely as well. If you enable this feature, clicking **Next** will take you to the last page of the Startup Wizard.

The following sections are included in this Help topic:

- Field Descriptions

Field Descriptions

The **Auto Update Configuration** panel displays the following fields:

- **Enable Auto Update**—Select to enable the firewall to be configurable from an Auto Update Server.
- **Protocol**—Enter the protocol the firewall uses to communicate with the Auto Update Server. Valid values are **https** and **http**.
- **Port**—Enter the TCP or UDP port number the firewall uses to communicate to the Auto Update Server.
- **Server**—Enter the IP address or a configured name on the firewall for the Auto Update Server.
- **Path**—Enter the path on the Auto Update Server to the service that updates the firewall.
- **Interface**—Select the interface with the Auto Update Server.
- **User Name**—Enter the user name needed to access the Auto Update Server.
- **User Password**—Enter the user password for the Auto Update Server.
- **Confirm User Password**—Enter the user password for the Auto Update Server a second time.
- **Device ID Type**—Select from the list how you would like the firewall to be identified on the Auto Update Server. The values available are:
    - **Host Name**—The host name of the firewall.
    - **PIX serial number**—The serial number of the firewall.
    - **User defined name**—Type a unique identifier in the **Device ID** field for this value.
    - **IP address of interface** [***interface name***]—The IP address of the selected interface.
    - **MAC address of interface** [***interface name***]—The burned in address of the selected interface.
- **Device ID**—Depending on what you chose to identify the device in the **Device ID Type** field, this displays the unique identifier for the firewall that is used on the Auto Update Server.
- **Back**—Returns you to the previous panel.
- **Next**—Advances you to the next panel.
- **Finish**—Submits your configuration to the firewall based upon choices made in the previous panels.
- **Cancel**—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return

you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

Basic Configuration

Startup Wizard>Basic Configuration

Startup Wizard>Basic Configuration lets you configure the host name of your firewall and the Enable Password, as well as a domain name for the firewall.

The hostname can be up to 63 alphanumeric characters and mixed case.

The password is used to administer PDM or to administer the firewall from the Command Line Interface (CLI). The password is a case-sensitive password of up to 16 alphanumeric characters. If you would like to change the current password, check **Change Password** and enter the new password in the fields provided.

Field Descriptions

The **Basic Configuration** panel displays the following fields:

- **Hostname**—Lets you enter a hostname for the firewall. This is automatically determined if configured to do so using DHCP. The hostname can be up to 63 alphanumeric characters and mixed case.
- **Old Enable Password**—Enter the old enable password, if one exists, in this box.
- **New Password**—Enter the new enable password in this field. The password is a case-sensitive password of up to 16 alphanumeric characters.
- **Confirm New Password**—Reenter the new enable password in this field.
- **Domain Name**—Specify the IPSec domain name the of PIX Firewall. This can be used later for certificates. There is a 64 character limit on the domain name, and it must be alphanumeric with no special characters or spaces.
- **Back**—Returns you to the previous panel.
- **Next**—Advances you to the next panel.
- **Finish**—Submits your configuration to the firewall based upon choices made in this panel.
- **Cancel**—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

DHCP Server Configuration

Startup Wizard>DHCP Server Configuration

The **DHCP Server Configuration** panel lets you configure the firewall as a Dynamic Host Control Protocol (DHCP) server to hosts on the inside interface. Here you can configure a range of IP addresses in the address pool, then when a host on the inside interface makes a request for an IP address using DHCP, the firewall assigns it an address from this pool.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

Important Notes

- Besides passing IP addresses to hosts on the inside, DHCP has the ability to pass DNS, WINS and other information to the hosts. You can add those settings after you have completed the wizard in the **System Properties>DHCP Server** panel.
- Depending on which platform of the firewall you are using, the number of addresses allowed in the DHCP pool will vary.

Platform	License	Limit
PIX Firewall 501	10-user licenses	32
PIX Firewall 501	50-user licenses	128
PIX Firewall 501	unlimited licenses	256
All other platforms		256

- If you configure the PDM to use the DHCP server option, the firewall will use the inside IP address, add one and configure the pool based on the number of addresses available according to your license and platform. The pool size will vary, and it may be configured for less IP addresses than you are licensed to use. This is done to keep the configuration simple.

Field Descriptions

The **DHCP Server Configuration** panel displays the following fields:

- **Enable DHCP on inside interface**—Select this check box to turn on DHCP for the firewall.
- **DHCP Address Pool**
  - **Starting IP Address**—Enter the starting range of the DHCP server pool in a block of IP addresses from the lowest to highest. The PIX Firewall 506 can support up to 32 DHCP-assigned IP addresses in version 6.0; all larger PIX Firewall platforms can support 254 IP addresses.
  - **Ending IP Address**—Enter the ending range of the DHCP server pool in a block of IP addresses from the lowest to highest. The PIX Firewall 506 can support up to 32 DHCP-assigned IP addresses in version 6.0; all larger PIX Firewall platforms can support 254 IP addresses.
- **Lease Length (seconds)**—Enter the amount of time (in seconds) the client can use its allocated IP address before the lease expires. The default value is 3600 seconds (1 hour).
- **Back**—Returns you to the previous panel.
- **Next**—Advances you to the next panel.
- **Finish**—Submits your configuration to the firewall based upon choices made in the previous panels.
- **Cancel**—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

NAT and PAT Configuration

Startup Wizard>NAT and PAT Configuration

The **NAT and PAT Configuration** panel lets you configure Network Address Translation (NAT) and Port Address Translation (PAT) on your firewall.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

PAT lets you set up a single IP address to be used for the global address. With PAT, you can set multiple outbound sessions to appear as if they originate from a single IP address. When enabled, the firewall chooses a unique port number from the PAT IP address for each outbound translation slot. This feature is valuable when an Internet Service Provider (ISP) cannot allocate enough unique IP addresses for your outbound connections. An IP address that you specify for a port address cannot be used in another global address pool. PAT lets up to 65,535 hosts start connections through a single outside IP address.

If you decide to use NAT, enter the address range that is used to translate addresses on the inside interface to addresses on the outside interface. The global addresses in the pool provide an IP address for each outbound connection, and for those inbound connections resulting from outbound connections.

Important Notes

- If you use NAT, the range of IP addresses required on this panel creates a pool of addresses that is used outbound on the firewall. If you have been assigned a range of Internet-registered, global IP addresses by your Internet Service Provider, enter them here. More information about NAT is available in the glossary.
- The following are limitations when using the PAT address configuration:
  - Does not work with H.323 applications and caching name servers.
  - Do not use when multimedia applications need to be run through the firewall. Multimedia applications can conflict with port mappings provided by PAT.
  - Does not work with the **established** command.
  - When in use with a passive FTP, use the **Fixup protocol ftp strict** command statement with an **access-list** command statement to permit outbound FTP traffic.
  - A DNS server on a higher lever security interface, needing to get updates from a root name server on the outside interface, cannot use PAT.

Field Descriptions

The **NAT and PAT Configuration** panel displays the following fields:

- **Use Port Address Translation**—Select to enable PAT. You must choose one of the following if you select this option.
  - **Use the IP address on the outside interface**—The Firewall uses the IP Address of the outside interface for PAT.
  - **Specify an IP address**—Specify an IP address to be used for PAT.
- **Use Network Address Translation**—Select to enable NAT and a range of IP addresses to be used for translation.
  - **Starting Global IP Address Pool**—Enter the first IP address in a range of IP addresses to be used for translation.
  - **Ending Global IP Address Pool**—Enter the last IP address in a range of IP addresses to be used for translation.
  - **Subnet Mask**—Specify the subnet mask for the range of IP addresses to be used for translation.
- **Do not translate any addresses**—Select this so the firewall does not translate IP addresses for hosts. If you are familiar with the command line interface, this is the same as using the **nat (inside) 0 0.0.0.0 0.0.0.0** command.
- **Back**—Returns you to the previous panel.
- **Next**—Advances you to the next panel.
- **Finish**—Submits your configuration to the firewall based upon choices made in the previous panels.
- **Cancel**—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

Other Interfaces Configuration

Startup Wizard>Other Interfaces Configuration

The **Other Interfaces Configuration** panel lets you configure the IP addresses of other interfaces on the firewall. PDM automatically lists the interfaces available for configuration, and in this panel you can set the IP address, speed, interface name, and security level to make each interface unique.

If you would like to configure the outside interface, click **Back** several times until you reach the **Outside Interface Configuration** panel.

The following sections are included in this Help topic:

- Field Descriptions

Field Descriptions

The **Other Interfaces Configuration** table displays the following fields:

- **Enabled**—Displays **Yes** if the interface is enabled and **No** if the interface is disabled.
- **Hardware ID**—The hardware name for the network interface that specifies the interface's slot location on the firewall motherboard. Interface boards are numbered from the leftmost slot nearest the power supply as slot 0. The internal network interface must be in slot 1. The lowest security level external interface board is in slot 0 and the next lowest security level external interface board is in slot 2.
- **Interface Name**—Displays the name of the interface.
- **Security Level**—Displays the security level of the selected interface. Either 0 for the outside network or 100 for the inside network. Perimeter interfaces can use any number between 1 and 99. By default, PIX Firewall sets the security level for the inside interface to security100 and the outside interface to security0. The first perimeter interface is initially set to security10, the second to security15, the third to security20, and the fourth perimeter interface to security25 (a total of 6 interfaces are permitted, with a total of 4 perimeter interfaces permitted).
- **IP Address**—Displays the IP address of the selected interface.
- **Subnet Mask**—Displays the subnet mask of the selected interface.
- **Speed**—Displays the speed of the selected interface. The available values for Ethernet are:
  - **10BaseT**—10 Mbps Ethernet half-duplex communication.
  - **10baseTX**—10 Mbps Ethernet half-duplex communication.
  - **Auto**—Lets the firewall automatically determine the speed.
  - **10full**—10 Mbps Ethernet full-duplex communication.
  - **100full**—100 Mbps Ethernet full-duplex communication.

Edit—Lets you configure any of the preceding fields.

- **Back**—Returns you to the previous panel.
- **Next**—Advances you to the next panel.
- **Finish**—Submits your configuration to the firewall based upon choices made in the previous panels.
- **Cancel**—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

Outside Interface Configuration

Startup Wizard>Outside Interface Configuration

The **Outside Interface Configuration** panel lets you configure the outside interface ip address, subnet mask, and default gateway.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

Important Notes

- The Cisco PIX Device Manager recognizes which hardware interfaces already exist on your firewall. From this panel you can specify the speed at which the outside interface runs, an IP address, and the subnet mask for that address. If you use Point-to-Point Protocol over Ethernet (PPPoE) or Dynamic Host Control Protocol (DHCP) you can specify that and allow the firewall to automatically configure the settings for the outside interface.
- The default gateway is the device the firewall will send all traffic that is not directly connected to it. Normally this will be on the outside interface, and one hop away.
- If you do select PPPoE or DHCP and do not configure a default gateway, the firewall will attempt to get that setting through those protocols.
- If you do configure a default gateway and select PPPoE or DCHP, the firewall will not attempt to get that setting through those protocols.

Field Descriptions

The **Outside Interface Configuration** panel displays the following fields:

- **Speed**—Specify the speed of the outside interface.
- **IP Address**—There are three ways to configure the outside interface IP address, and they are configurable in the following fields.
  - **Use PPPoE**—If your ISP supports PPPoE, you can choose to have a PPPoE server assign your outside IP address. Ensure your ISP supports PPPoE before clicking this option.
  - **Use DHCP**—If your ISP supports DHCP, you can choose to have DHCP check your outside interface IP address and set the default route, by clicking the appropriate option.
  - **Static IP Address**—Use this to activate the following fields to be able to assign a static IP address to your firewall.

    - **IP Address**—Assign an IP address to the outside interface of your firewall. The IP address you assign must be unique for each interface. Do not use addresses previously used for routers, hosts, or any other PIX Firewall commands, such as an IP address in the global pool or for a static NAT entry.
    - **Subnet Mask**—Specify the subnet mask of your outside interface IP address, or choose one from the list.
- **Default Gateway**—The IP address of the device directly connected to the outside interface of the firewall where traffic destined for a network not directly connected is sent.
- **Back**—Returns you to the previous panel.
- **Next**—Advances you to the next panel.
- **Finish**—Submits your configuration to the firewall based upon choices made in the previous panels.
- **Cancel**—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

PPPoE Configuration

Startup Wizard>PPPoE Configuration

The **PPPoE Configuration** panel in the Startup Wizard allows you to setup the user authentication for using the Point to Point Protocol over Ethernet (PPPoE) protocol with your Internet Service Provider (ISP) or other connectivity provider. PPPoE is similar to the PPP protocol used for dial up ISP access with a modem over analog phone lines, but encapsulated within an Ethernet packet.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

Important Notes

1. PPPoE uses the Outside interface. Use Startup Wizard Outside Interface Configuration or System Properties>Interfaces to setup the outside interface.
2. Be sure your ISP or other connectivity provider supports PPPoE before choosing this option.

Field Descriptions

The **Outside Interface Configuration** panel displays the following fields:

- **PPPoE User Name**—The user name assigned by your ISP or other connectivity provider.
- **PPPoE Password**—The password assigned by your ISP or other connectivity provider
- **Confirm Password**—Confirms proper entry of the PPPoE password.
- **PPPoE Authentication**—Specify the method of user authentication to be used with PPPoE:
  - **PAP**—Password Authentication Protocol
  - **CHAP**—Challenge Handshake Authentication Protocol
  - **MSCHAP**—Microsoft Challenge Handshake Authentication Protocol
- **Back**—Returns you to the previous panel.
- **Next**—Advances you to the next panel.
- **Finish**—Submits your configuration to the firewall based upon choices made in the previous panels.
- **Cancel**—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous

panel.

Copyright © 2001-2004, Cisco Systems, Inc.

Starting Configuration

Startup Wizard>Starting Configuration

The **Startup Wizard** panel lets you begin the process of configuring your firewall using the Startup Wizard. This is only available on the PIX Firewall 501 and the PIX Firewall 506.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

From this point you can choose a starting point for the firewall. If your firewall has already been configured, you have the option from this screen to reset the configuration back to the factory defaults. If you would like, you can import the current configuration into PDM.

To reset the firewall to the factory defaults, choose **Reset the configuration to its factory default values**, and click **Next** or **Finish**. You will be prompted to verify this is what you would like to do, and the firewall will be reset to its default configuration.

To import the current configuration from the firewall into PDM, choose **Continue with the existing configuration** and click **Next**.

Important Notes

- If you choose **Reset the configuration to its factory default values**, click **Next**, then affirm at the prompt that you wish to reset the configuration, **Cancel** will not restore your previous configuration. If you choose this option the firewall will reset immediately, instead of when the Startup Wizard finishes. This cannot be undone. If you do not have a DHCP server on your network to assign an IP address to the outside interface, this may take some time to complete.
- If you do not enable **Do not change the inside interface**, the IP address on the inside interface will be changed to 192.168.1.1. If this is different than the network that you are on, you will be not be able connect back to the PIX.
- If you configure the PDM to use the DHCP server option, the firewall will use the inside IP address, add one and configure the pool based on the number of addresses available according to your license and platform. The pool size will vary, and it may be configured for less IP addresses than you are licensed to use. This is done to keep the configuration simple.

Field Descriptions

The **Starting Configuration** panel displays the following fields:

- **Back**—Returns you to the previous panel.
- **Next**—Advances you to the next panel.
- **Finish**—Submits your configuration to the firewall based upon choices made in the previous panels.
- **Cancel**—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

Startup Wizard Completed

Startup Wizard>Startup Wizard Completed

The **Startup Wizard Completed** panel lets you submit all of the settings you have made to the firewall.

- If you would like to change any of the settings you have made, click the back button. Click **Finish**, and the configuration created by the wizard is sent to the PIX and saved to flash memory.
- If you ran the Startup Wizard using https://<IP>/startup.html, a you can check **Launch PDM** to start PDM when you click **Finish**. The configuration is automatically saved to flash memory. PDM will either display a confirmation that the configuration was successful and saved to flash or else the error that occurred.
- If you ran the Startup Wizard from within PDM, you must explicitly save the configuration to flash memory just like any other configuration changes.

The following sections are included in this Help topic:

- Field Descriptions

Field Descriptions

- **Back**—Returns you to the previous panel.
- **Finish**—Submits your configuration to the firewall based upon choices made in the previous panels.
- **Cancel**—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

Easy VPN Remote Configuration

Startup Wizard>Easy VPN Remote Configuration

The **Easy VPN Remote Configuration** panel lets you configure the firewall as a Cisco Easy VPN Remote device. This means the firewall can work in conjunction with a VPN concentrator or router acting as a Cisco Easy VPN Remote device Server to use VPN and receive VPN settings from it, negotiating the parameters necessary to make a VPN tunnel active and pass encrypted traffic across a public network. This option in the Startup Wizard is only available on the PIX Firewall 501 and PIX Firewall 506 models.

The following sections are included in this Help topic:

- Field Descriptions

Field Descriptions

The **Easy VPN Remote Configuration** panel displays the following fields:

- **Enable Easy VPN Remote**—Select to enable the firewall to act as a Cisco Easy VPN Remote device.
- **Mode**—The **Mode** group box contains the following options.
  - **Client mode**—This option applies Network Address Translation (NAT) to all IP addresses of clients connected to the inside (higher security) interface of the firewall. To use this mode, you must also enable the DHCP server on the inside interface.
  - **Network extension mode**—This option does not apply NAT to any IP addresses of clients on the inside (higher security) interface of the firewall.
- **Primary Easy VPN Server IP Address**—Enter the IP address of the Easy VPN Server.
- **Secondary Easy VPN Server IP Address**—Enter the IP address of the secondary Easy VPN Server in case the primary Easy VPN Server is unavailable.
- **Group Name**—Enter the VPN group name. This must match the group name the VPN peer expects from VPN clients.
  - **Group Password**—Enter the VPN group password. This must exactly match the group password the VPN peer expects from VPN clients. It is case sensitive.
  - **Confirm Password**—Enter the VPN group password a second time. This must match the group password the VPN peer expects from VPN clients. It is case sensitive.
- **User Name**—Enter the VPN user name. This must match the user name the VPN peer expects from VPN clients. It is case sensitive.
  - **User Password**—Enter the VPN user password. This must match the user password the VPN peer expects from VPN clients. It is case sensitive.
  - **Confirm Password**—Enter the VPN user password a second time. This must match the user password the VPN peer expects from VPN clients. It is case sensitive.

- **Back**—Returns you to the previous panel.
- **Next**—Advances you to the next panel.
- **Finish**—Submits your configuration to the firewall based upon choices made in the previous panels.
- **Cancel**—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

History Metrics

Configuration>System Properties>History Metrics

The **History Metrics** panel lets you configure the firewall to keep a history of various statistics, which can be displayed by PDM through the **Monitoring** tab. The following statistics are kept when history metrics are enabled:

- Input and output bytes (per interface)
- Input and output packets (per interface)
- Input and output errors (per interface)
- Available block count (4 bytes, 80 bytes, 256 bytes and 1550 bytes)
- Memory—free and used
- Perfmon—Xlates, connections, TCP connections, UDP connections, URL filtering, WebSense, TCP fixup, TCP
- Intercept, FTP fixup, HTTP fixup, AAA Authentication, AAA Authorization, AAA Accounting
- Traffic (per interface)
- Broadcasts, No Buffer, Giants, Frame, CRC, Frame, Overrun, Underruns, Collisions, Late Collisions, Resets, Deferred, Lost Carrier (per interface)
- IDS counters
- Failover statistics—Xmit Queue, Rcv Queue, TCP rcv, TCP xmit, UDP rcv, UDP xmit, Xlate rcv, Xlate xmit
- Xlates—current and max

The following sections are included in this Help topic:

- Field Descriptions
- Disabling PDM History Metrics
- Enabling PDM History Metrics
- Resetting to Last Applied Settings

Field Descriptions

The **History Metrics** panel displays the following fields:

- **PDM History Metrics**—Selecting this check box enables the keeping of history "buckets" for each of the metrics. Clearing this check box destroys and disables the history metrics.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Disabling PDM History Metrics

This feature is enabled by default. Follow these steps to disable PDM history metrics:

1. In the **History Metrics** panel, select the **PDM History Metrics** check box. Clearing the check box disables PDM history metrics.
2. Click **Apply**.

Enabling PDM History Metrics

Follow these steps to re-enable PDM history metrics after it has been disabled:

1. Select the **PDM History Metrics** check box.
2. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Authentication Prompt

Configuration>System Properties>AAA>Authentication Prompt

The **Authentication Prompt** panel lets you provide AAA challenge text for access to the firewall. If you do not use this command, challenge text does not appear for Telnet access. Use the options to display different authentication prompts if the authentication attempt is accepted or rejected by the authentication server.

The **Authentication Prompt** panel lets you change the AAA challenge text for HTTP, FTP, and Telnet access. If configured, the prompt text displays above the username and password prompts that users view when logging in. If you do not use this feature, FTP users view FTP authentication, HTTP users view HTTP Authentication, and challenge text does not appear for Telnet access. If the user authentication occurs from Telnet, you can use the **user accepted** and **user rejected** options to display different authentication prompts if the authentication attempt is accepted or rejected by the authentication server.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Enabling When a User is Accepted
- Enabling When a User is Rejected
- Resetting to Last Applied Settings

Important Notes

Challenge text can be a string of up to 235 alphanumeric characters. Special characters should not be used, but spaces and punctuation characters are permitted. A question mark ends the string. (The question mark appears in the string.) Any characters after the question mark will be ignored.

Field Descriptions

The **Authentication Prompt** panel displays the following fields:

- **Prompt**—Select the **prompt** check box to modify the challenge text sent to request a user to enter a password.
- **User accepted**—Select the **user accepted** check box to edit the text displayed when the user is accepted into the authentication server.
- **User rejected**—Select the **user rejected** check box to edit the text displayed when the user is rejected by

the authentication server.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Enabling When a User is Accepted

Follow these steps to enter an authorization prompt when a user is accepted:

1. Select the **user accepted** check box and type a text string in the box below it.
2. To clear this text, select the **user accepted** check box a second time to clear it.
3. Click **Apply**.

Enabling When a User is Rejected

Follow these steps to enter an authorization prompt when a user is rejected:

1. Select the **user rejected** check box and type a text string in the box below it.
2. To clear this text, select the **user rejected** check box a second time to clear it.
3. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Device

Configuration>System Properties>Administration>Device

The **Device** panel lets you set the IPSec domain name and the hostname of the firewall.

Field Descriptions

- **Domain Name**—A domain name, such as `example.com`.
- **Hostname**—The hostname command changes the host name label on prompts. The default host name is `pixfirewall.` This name can be up to 63 alphanumeric characters and mixed case.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

SNMP

Configuration>System Properties>Administration>SNMP

The **SNMP** panel lets you configure the firewall for monitoring by Simple Network Management Protocol (SNMP) management stations.

SNMP defines a standard way for network management stations running or PCs on workstations to monitor the health and status of many types of devices, including switches, routers, and the firewall.

The following sections are included in this Help topic:

- SNMP Terminology
- PIX Firewall SNMP
- Field Descriptions
- Adding Management Stations
- Editing Management Stations
- Deleting Management Station
- Applying Changes

SNMP Terminology

- **Management station**—Network management stations running or PCs on workstations, use the SNMP protocol to administer standardized databases residing on the device being managed. Management stations can also receive messages about events, such as hardware failures, which require attention.
- **Agent**—In the context of SNMP, the management station is a *client* and an SNMP agent running on the firewall is a *server*.
- **OID**—The SNMP standard assigns a system object ID (OID) so that a management station can uniquely identify network devices with SNMP agents and indicate to users the source of information monitored and displayed.
- **MIB**—The agent maintains standardized data structures called Management Information Databases, or MIBs which are compiled into management stations. MIBs collect information, such as packet, connection, and error counters, buffer usage, and failover status. MIBs are defined for specific products, in addition to MIBs for the common protocols and hardware standards used by most network devices. SNMP management stations can browse MIBs or request only specific fields. In some applications, MIB data can be modified for administrative purposes.
- **Trap**—The agent also monitors alarm conditions. When an alarm condition defined in a trap occurs, such as a link up, link down, or syslog event, the agent sends notification, also known as SNMP trap, to the designated management station immediately.

PIX Firewall SNMP

For Cisco MIB files and OIDs, refer to: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

- **MIBs**—The firewall supports the following MIBs which can be browsed by management stations:
  - **MIB-II**—System and Interface groups only.
  - **Firewall MIB**—cfwSystem group only.
  - **Cisco Memory Pool MIB**.
  - **Cisco syslog MIB**—Browsing of the Cisco syslog MIB is not supported. All SNMP variables supported in the firewall are read only (RO).
- **OIDs**—The SNMP MIB mib-2.system.sysObjectID variable now provides one of the following PIX Firewall platform-specific Object IDs which can be viewed by management stations, such as CiscoView:

  PIX Firewall 506—.iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.ciscoPIXFirewall506 (same as .1.3.6.1.4.1.9.1.389)
  PIX Firewall 515—.iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.ciscoPIXFirewall515 (same as .1.3.6.1.4.1.9.1.390)
  PIX Firewall 520—.iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.ciscoPIXFirewall520 (same as .1.3.6.1.4.1.9.1.391)
  PIX Firewall 525—.iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.ciscoPIXFirewall525 (same as .1.3.6.1.4.1.9.1.392)
  PIX Firewall 535—.iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.ciscoPIXFirewall535 (same as .1.3.6.1.4.1.9.1.393)

  For other PIX Firewall platforms:
  .iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.ciscoPIXFirewall (same as .1.3.6.1.4.1.9.1.227)

- **Traps**—The firewall supports many SNMP traps. The **logging** command lets you enable or disable sending informational messages to an SNMP management station. The SNMP message level can be set with PDM or with the **logging history** command and the syslog message level is set with the **logging trap** command.

The PIX Firewall supports a maximum of 32 management stations. The **snmp-server host** command lists the IP addresses of all management stations (clients) to the firewall agent (server).

For more information about SNMP, see the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

Field Descriptions

The **SNMP** panel provides the following fields:

- **Password: (community string)**—Enter the password used by the SNMP management station when sending requests to the firewall. The SNMP community string is a shared secret among the SNMP management stations and the network nodes being managed. The firewall uses the password to determine if the incoming SNMP request is valid. The password is a case-sensitive value up to 32 characters in length. Spaces are not permitted. The default is "public".
- **System Administrator Name**—Enter the name of the firewall system administrator. The text is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
- **Firewall Location**—Specify the firewall location. The text is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
- **Send syslog messages as SNMP traps**—Select this check box to send SNMP trap notifications to the management station when syslog events occur.
- **Level**—The highest level of detail enabled for syslog messages, from 0 to 7. Level 0 is an emergency, the most important. The value specified includes all values less than itself. For example, 3 indicates that messages of level 0, 1, 2, and 3 will be logged and sent to the SNMP management station. As the value increases, more frequent, but less important messages will be generated:

  Off-**disable**—Syslog messages via SNMP will not be sent, not a message level
  ---
  0-**Emergencies**—Syslog messages that identify very serious system instabilities
  1-**Alerts**—System integrity issues which require immediate action
  2-**Critical**—Critical operational conditions
  3-**Errors**—Important operational error messages
  4-**Warnings**—Warning messages, such as configuration errors or limit conditions
  5-**Notifications**—Normal events during operation which are considered significant
  6-**Informational**—Information messages about typical of day-to-day activities
  7-**Debugging**—Configuration debugging and FTP, HTTP, URL command logs

- **SNMP management station table**
  - **Interface**—Displays the firewall interface name where the SNMP management station resides.
  - **IP Address**—Displays the IP address of an SNMP management station to which the firewall sends trap events and receive requests or polls.
  - **Poll/Trap**—Displays the method for communicating with this management station, poll only, trap only, or both trap and poll. Polling means that the firewall waits for a periodic request from the management station. The trap setting sends syslog events when they occur.

- **Add**—Opens the **Add SNMP Host Access Entry** dialog box.
- **Edit**—Opens the **Edit SNMP Host Access Entry** dialog box.
- **Delete**—Deletes the selected item.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover

standby firewall unit. See Configuration Changes.

- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

The **Add** and **Edit** buttons provide these fields:

- **Interface Name**—Select the interface on which the management station resides.
- **IP Address**—Specify the IP address of the management station.
- **Server Poll/Trap Specification**—Select **Poll**, **Trap** or both.
- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

For more information about SNMP, see the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

Adding SNMP Management Stations

Follow these steps to add SNMP Management Stations:

1. Click **Add** to open the **SNMP Host Access Entry** dialog box.
2. From **Interface Name**, select which interface the SNMP management station resides.
3. Enter the IP address of that management station in **IP Address**.
4. Click to select **Poll**, **Trap**, or both.
5. To return to the previous panel click:
   - **OK**—Accepts changes and returns to the previous panel.
   - **Cancel**—Discards changes and returns to the previous panel.
   - **Help**—Provides more information.

Editing SNMP Management Stations

Follow these steps to edit SNMP Management Stations:

1. Select a list item from the SNMP management station table on the **SNMP** panel.
2. Click **Edit** to open the **Edit SNMP Host Access Entry** dialog box.
3. From Interface Name, select which interface the SNMP management station resides.
4. Enter the IP address of that management station in **IP Address**.
5. Click to select **Poll**, **Trap**, or both.
6. To return to the previous panel click:
   -

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Deleting SNMP Management Stations

Follow these steps to delete an SNMP management station from the table:

1. Select a list item from the SNMP management station table on the **SNMP** panel.
2. Click **Delete**.

Applying Changes

Changes to the table made by **Add**, **Edit**, or **Delete** are not immediately applied to the running configuration. Click one of the following buttons to apply or discard changes:

1. **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
2. **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Anti-Spoofing

Configuration>System Properties>Advanced>Anti-Spoofing

The **Anti-Spoofing** panel lets you specify which interfaces to protect from an IP spoofing attack using network ingress and egress filtering.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Enabling or Disabling Anti-Spoofing
- Resetting to Last Applied Settings

Important Notes

This feature provides Unicast RPF (Reverse Path Forwarding) functionality for the firewall and is disabled by default. Due to the danger of IP spoofing in the IP protocol, measures need to be taken to reduce this risk when possible. Unicast RPF, or reverse route lookups, prevents such manipulation under certain circumstances.

Caution: Before using this feature, add static routes for every network that can be accessed on the interfaces you wish to protect. Only enable this feature if routing is fully specified. Otherwise, the firewall will stop traffic on the interface you specify if routing is not in place.

Up to 100 VLAN (Virtual LAN) interfaces may be listed in the table.

Field Descriptions

The **Anti-Spoofing** panel displays the following fields:

- **Interface table**—The network interfaces which were configured in Configuration>System Properties>Interfaces are listed.
  - **Interface**—The interface on which anti-spoofing is enabled or disabled.
  - **Proxy ARP Enabled**—Displays if anti-spoofing is enabled or disabled.
- **Enable**—Click to enable anti-spoofing for the selected interface.

- **Disable**—Click to disable anti-spoofing for the selected interface.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Enabling or Disabling Anti-Spoofing

To enable or disable anti-spoofing, follow these steps:

1. Select the interface in the interface table on which you want to enable or disable anti-spoofing. To select multiple interfaces at a time, select an interface, and then hold down the CTRL key while you click other interfaces that you want to select.
2. Click **Enable** to enable anti-spoofing, or **Disable** to disable anti-spoofing.
3. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

CTIQBE

Configuration>System Properties>Advanced>Fixup>CTIQBE

The **CTIQBE** panel lets you enable or disable the use of Computer Telephony Integration Quick Buffer Encoding (CTIQBE) protocol through the firewall. The default CTIQBE port number is 2748 and cannot be changed.

The **CTIQBE** panel lets you enable or disable support in the firewall for CTIQBE protocol. CTIQBE protocol is used for Cisco IP SoftPhone or other Cisco TAPI/JTAPI applications to communicate successfully with Cisco CallManager across the firewall with NAT, PAT, or Bi-directional NAT configured.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Enabling CTIQBE Fixup
- Disabling CTIQBE Fixup
- Resetting to Last Applied Settings

Important Notes

For more information about the protocols used in the **Fixup** panels, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

Field Descriptions

The **CTIQBE** panel displays the following fields:

- **Enable**—Enables CTIQBE fixup for a firewall. Clearing this check box disables CTIQBE fixup.

  Note: The default **CTIQBE** port number is 2748 and cannot be changed.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use

the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Enabling CTIQBE Fixup

This feature is disabled by default. Follow these steps to enable CTIQBE fixup:

1. In the **CTIQBE** panel, select the **Enable** check box.
2. Click **Apply**.

Disabling CTIQBE Fixup

Follow these steps to disable CTIQBE fixup after it has been enabled:

1. In the **CTIQBE** panel, clear the **Enable** check box.
2. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

H.323 RAS

Configuration>System Properties>Advanced>Fixup>H.323 RAS

The **H.323** panel lets you enable or disable the firewall to look into the payload of H.323 signal channels and apply the Adaptive Security Algorithm (ASA). H.323 RAS fixup is enabled for UDP ports 1718 and 1719 by default.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Disabling H.323 Fixup
- Enabling H.323 Fixup
- Changing the H.323 Fixup Port Numbers
- Resetting to Last Applied Settings

Important Notes

H.323 is a suite of protocols defined by the International Telecommunication Union (ITU) for multimedia conferences over LANs. H.323 also supports VoIP gateways and VoIP gatekeepers. The Firewall supports H.323 version 2. The H.323 fixup feature provides support for Intel InternetPhone, CU-SeeMe, CU-SeeMe Pro, MeetingPoint, and MS NetMeeting. H.323 RAS uses a single UDP connection for registration, admissions, and status.

For more information about the protocols used in the **Fixup** panels, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

For a list of applications and protocols supported, see IP.

Field Descriptions

The **H.323** panel displays the following fields:

- **H.323 table**
  - **Low Port**—Displays the UDP port number or lower port number range for the H.323 RAS fixups.
  - **High Port**—Displays the upper port number range for the H.323 RAS fixups.
- **Add**—Copies the new entry into the H.323 table.

- **Low Port**—Lets you enter a port number or lower port number range for addition to the H.323 table.
- **High Port (optional)**— Lets you enter an upper port number range for addition to the H.323 table.
- **Delete**—Deletes the selected item.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Disabling H.323 Fixup

This feature is enabled by default. Follow these steps to disable H.323 fixup:

1. Select any row displayed in the H.323 table.
2. Click **Delete**. The port or port range is deleted from the H.323 table.
3. Click **Apply**.

Enabling H.323 Fixup

Follow these steps to re-enable H.323 fixup after it has been disabled:

1. Enter **1720** or a lower port number range in the **Low Port** box.
2. Enter an upper port number range (if applicable) in the **High Port** box.
3. Click **Add**.
4. Repeat steps 1 through 3 if necessary.
5. Click **Apply**.

Changing the H.323 Fixup Port Numbers

Follow these steps to change the H.323 fixup ports:

1. Select the port or port range you want to change in the H.323 table.
2. Click **Delete**.
3. Enter a port number or a lower port number range in the **Low Port** box.
4. Enter an upper port number range (if applicable) in the **High Port** box.
5. Click **Add**.
6. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

ICMP Error

Configuration>System Properties>Advanced>Fixup>ICMP Error

The **ICMP Error** panel lets you enable or disable Network Address Translation (NAT) of Internet Control Message Protocol (ICMP) error messages that are generated by intermediate hops between the inside host and the PIX. By default, the firewall does not create xlates for intermediate nodes that generate ICMP error messages.

When NAT is enabled for ICMP error messages, the firewall creates xlates for intermediate nodes that generate ICMP error messages. It is helpful to enable this feature when tracing a route for troubleshooting purposes.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Enabling ICMP Error
- Disabling ICMP Error

Important Notes

For more information about the protocols used in the **Fixup** panels, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

Field Descriptions

The **ICMP Error** panel displays the following fields:

- **Enable NAT for ICMP error messages**—Lets you enable or disable NAT for ICMP error messages.

Enabling ICMP Error

Select the **Enable NAT for ICMP error messages** check box to enable the firewall to NAT for ICMP error messages. When NAT is enabled for ICMP error messages, the firewall creates xlates for intermediate nodes that

generate ICMP error messages. This feature is helpful when tracing a route for troubleshooting purposes. For example, you can trace the route from an outside host, using a tool like the **traceroute** router command, to trace the hops back to the destination on the inside of the firewall.

Disabling ICMP Error

Clear the **Enable NAT for ICMP error messages** check box to disable the firewall to NAT for ICMP error messages. That is, the firewall does not create xlates for intermediate nodes that generate ICMP error messages. ICMP error messages generated by intermediate nodes between the inside host and the firewall reach the outside host without consuming any additional NAT resources.

Copyright © 2001-2004, Cisco Systems, Inc.

MGCP

Configuration>System Properties>Advanced>Fixup>MGCP

The **MGCP** panel lets you enable or disable the firewall to inspect Media Gateway Control Protocol (MGCP) messages between Call Agent and media gateway. You can specify the port(s) at which the firewall listens for MGCP traffic. Typically, a Call Agent is configured to send commands to port 2427 (the default MGCP port for gateways) and a gateway is configured to send commands to port 2727 (the default MGCP port for Call Agents).

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Enabling MGCP Fixup
- Disabling MGCP Fixup
- Changing the MGCP Fixup Port Number
- Configuring MGCP Fixup
- Resetting to Last Applied Settings

Important Notes

For more information about the protocols used in the **Fixup** panels, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

For a list of applications and protocols supported, see **more IP.**

Field Descriptions

The **MGCP** panel displays the following fields:

- **MGCP table**
  - **Low Port**—Displays the port number or lower port number range for the MGCP. Typically, a Call Agent is configured to send commands to port 2427 (the default MGCP port for gateways) and a gateway is configured to send commands to port 2727 (the default MGCP port for Call Agents).
  - **High Port**—Displays the upper port number range (if applicable) for the MGCP fixup.

- **Add**—Copies the **Low** and **High** port values into the MGCP table**.**

- **Low port**—Lets you enter a port number or lower port number range for addition to the MGCP table.
- **High port (optional)**—Lets you enter an upper port number range for addition to the MGCP table.
- **Delete**—Deletes the selected item.
- **Configure MGCP—**Lets you specify the maximum MGCP command queue size and set up groups consisting of Call Agents and gateways.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Enabling MGCP Fixup

This feature is disabled by default. Follow these steps to enable MGCP fixup:

1. Enter **2427** (typically, for a gateway) or **2727** (typically, for a Call Agent) or a lower port number range in the **Low port** box.
2. Enter an upper port number range (if applicable) in the **High port** box.
3. Click **Add**.
4. Repeat Steps 1 through 3 if necessary.
5. Click **Apply**.

Disabling MGCP Fixup

Follow these steps to disable MGCP fixup:

1. Select the row you want to delete in the MGCP table.
2. Click **Delete**.
3. Click **Apply**.

Changing the MGCP Fixup Port Numbers

Follow these steps to change the MGCP fixup ports:

1. Select the port or port range you want to change in the MGCP table.
2. Click **Delete**.
3. Enter a port number or a lower port number range in the **Low port** box.
4. Enter an upper port number range (if applicable) in the **High port** box.
5. Click **Add**. The port or port number range appears in the MGCP table.
6. Click **Apply**.

Configuring MGCP Fixup

To configure MGCP, click **Configure MGCP**. The Configure MGCP panel appears. This panel lets you specify the

maximum MGCP command queue size and set up groups consisting of Call Agents and gateways.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Configure MGCP

Configuration>System Properties>Advanced>Fixup>MGCP>Configure MGCP

The **Configure MGCP** panel lets you specify the MGCP command queue size and set up Call Agent and gateway groups. An MGCP group may consist of any number of Call Agents or gateways. However, it must contain at least one Call Agent or gateway.

The following sections are included in this Help topic:

- Field Descriptions
- Adding an MGCP Group
- Editing an MGCP Group
- Deleting an MGCP Group
- Resetting to Last Applied Settings

Field Descriptions

The **Configure MGCP** panel displays the following fields:

- **Command Queue Size**—Specifies the maximum number of MGCP commands that will be queued. When the limit is reached and a new command arrives, the command that has been in the queue for the longest time will be removed. The range is from 1 to 4,294,967,295. The default value is 200.
- **MGCP Group table**
  - #—Displays the group ID for Call Agents and gateway groups. An MGCP group may consist of any number of Call Agents or gateways. However, it must contain at least one Call Agent or gateway. The initial default value is 0, and it increments by 1 with each new group entry. This value can be configured from 0 to 4,294,967,295.
  - **Gateway(s)**—Displays the IP address of the gateway(s). A gateway may only belong to one group.
  - **Call Agent(s)**—Displays the IP address of the Call Agent(s). A Call Agent may belong to more than one group.
- **Add**—Clicking this button opens the **Add MGCP Group** dialog box, which lets you add gateway and Call Agent IP addresses.
- **Edit**—Select a group from the table and click this button to open the **Edit MGCP Group** dialog box, which lets you edit the properties of the selected group.
- **Delete**—Clicking this button deletes the highlighted group definition.
- **OK**—Accepts changes and returns to the previous panel.

- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Adding an MGCP Group

Follow these steps to add a new group:

1. In the **Configure MGCP** panel, click **Add**. The **Add MGCP Group** dialog box appears.
2. Change the group ID number or accept the default.
3. Enter the IP address of the desired gateway or Call Agent and click **Add**.
4. Repeat Step 3 for multiple gateway or Call Agent IP addresses.
5. In the **Add MGCP Group** dialog box, click **OK**.
6. In the **Configure MGCP** panel, click **OK**.
7. In the **MGCP** panel, click **Apply**.

Editing an MGCP Group

Follow these steps to change the settings of an existing group:

1. In the **Configure MGCP** panel, select the number of the group that you want to change and click **Edit**. The **Edit MGCP Group** dialog box appears.
2. Change the group settings as desired and click **OK**.
3. In the **Configure MGCP** panel, click **OK**.
4. In the **MGCP** panel, click **Apply**.

Deleting an MGCP Group

Follow these steps to remove an existing group:

1. In the **Configure MGCP** panel, select the number of the group that you want to delete and click **Delete**.
2. Click **OK**.
3. In the **MGCP** panel, click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Add MGCP Group

Configuration>System Properties>Advanced>Fixup>MGCP>MGCP Config>Add MGCP Group

The **Add MGCP Group** dialog box lets you create MGCP Call Agent and gateway groups. An MGCP group may consist of any number of Call Agents or gateways. However, it must contain at least one Call Agent or gateway.

The following sections are included in this Help topic:

- Field Descriptions
- Adding an MGCP Group
- Editing an MGCP Group

Field Descriptions

The **Add MGCP Group** dialog box displays the following fields:

- **Group ID**—Displays the group ID for Call Agents and gateway groups. An MGCP group may consist of any number of Call Agents or gateways. However, it must contain at least one Call Agent or gateway. The initial default value is 0, incrementing by 1 with each new group entry. This value can be configured from 0 to 4,294,967,295.
- **Gateways IP Address Table**—Displays the IP addresses of the gateways associated with the group. A gateway may only belong to one group.
- **Gateway to Add**—Enter the IP address of the gateway that you wish to add.
- **Add**—Clicking this button adds the IP address of the gateway that you entered to the IP address table.
- **Delete**—Clicking this button deletes the highlighted gateway IP address entry from the IP address table.
- **Call Agents IP Address Table**—Displays the IP addresses of the Call Agents associated with the group. A Call Agent may belong to more than one group.
- **Call Agent to Add**—Enter the IP address of the Call Agent that you wish to add.
- **Add**—Clicking this button adds the IP address of the Call Agent that you entered to the IP address table.
- **Delete**—Clicking this button deletes the highlighted Call Agent IP address entry from the IP address table.

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Adding an MGCP Group

Follow these steps to add a new group:

1. You may change the group ID number or accept the default. Enter the IP address of the desired gateway or Call Agent and click **Add**.
2. Repeat Step 1 for multiple gateway or Call Agent IP addresses.
3. In the **Add MGCP Group** dialog box, click **OK**.
4. In the **Configure MGCP** panel, click **OK**.
5. In the **MGCP** panel, click **Apply**.

Editing an MGCP Group

Follow these steps to change the settings of an existing group:

1. Change the group settings as desired.
2. Click **Add** to add a new IP address to the IP address table, or highlight an existing IP address, and click **Delete** to remove the entry from the IP address table.
3. Repeat Step 2 for multiple gateway or Call Agent IP addresses.
4. In the **Edit MGCP Group** dialog box, click **OK**.
5. In the **Configure MGCP** panel, click **OK**.
6. In the **MGCP** panel, click **Apply**.

Copyright © 2001-2004, Cisco Systems, Inc.

Edit MGCP Group

Configuration>System Properties>Advanced>Fixup>MGCP>MGCP Config>Edit MGCP Group

The **Edit MGCP Group** dialog box lets you edit MGCP Call Agent and gateway groups. An MGCP group may consist of any number of Call Agents or gateways. However, it must contain at least one Call Agent or gateway.

The following sections are included in this Help topic:

- Field Descriptions
- Editing an MGCP Group

Field Descriptions

The **Edit MGCP Group** dialog box displays the following fields:

- **Group ID**—Displays the group ID for Call Agents and gateway groups. An MGCP group may consist of any number of Call Agents or gateways. However, it must contain at least one Call Agent or gateway. The initial default value is 0, incrementing by 1 with each new group entry. This value can be configured from 0 to 4,294,967,295.
- **Gateways IP Address Table**—Displays the IP addresses of the gateways associated with the group. A gateway may only belong to one group.
- **Gateway to Add**—Enter the IP address of the gateway that you wish to add.
- **Add**—Clicking this button adds the IP address of the gateway that you entered to the IP address table.
- **Delete**—Clicking this button deletes the highlighted gateway IP address entry from the IP address table.
- **Call Agents IP Address Table**—Displays the IP addresses of the Call Agents associated with the group. A Call Agent may belong to more than one group.
- **Call Agent to Add**—Enter the IP address of the Call Agent that you wish to add.
- **Add**—Clicking this button adds the IP address of the Call Agent that you entered to the IP address table.
- **Delete**—Clicking this button deletes the highlighted Call Agent IP address entry from the IP address table.
- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Editing an MGCP Group

Follow these steps to change the settings of an existing group:

1. Change the group settings as desired.
2. Click **Add** to add a new IP address to the IP address table, or highlight an existing IP address, and click **Delete** to remove the entry from the IP address table.
3. Repeat Step 2 for multiple gateway or Call Agent IP addresses.
4. In the **Edit MGCP Group** dialog box, click **OK**.
5. In the **Configure MGCP** panel, click **OK**.
6. In the **MGCP** panel, click **Apply**.

Copyright © 2001-2004, Cisco Systems, Inc.

PPTP

Configuration>System Properties>Advanced>Fixup>PPTP

The **PPTP** panel lets you enable or disable the firewall to permit Point-to-Point Tunneling Protocol (PPTP) traffic which is a tunneling protocol for Point-to-Point Protocol (PPP). You can specify the port(s) at which the firewall listens for PPTP traffic. The default PPTP port number is 1723.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Enabling PPTP Fixup
- Disabling PPTP Fixup
- Changing the PPTP Fixup Port Number
- Resetting to Last Applied Settings

Important Notes

For more information about the protocols used in the **Fixup** panels, refer to the *Cisco PIX Firewall and VPN Configuration Guide* for your version of software.

For a list of applications and protocols supported, see IP.

▲

Field Descriptions

The **PPTP** panel displays the following fields:

- **PPTP table**
  - **Low Port**—Displays the port number or lower port number range for the PPTP fixup. The default is **1723**.
  - **High Port**—Displays the upper port number range (if applicable) for the PPTP fixup.

- **Add**—Copies the **Low** and **High** port values into the PPTP table**.**
- **Low port**—Lets you enter a port number or lower port number range for addition to the PPTP table.
- **High port (optional)**—Lets you enter an upper port number range for addition to the PPTP table.
- **Delete**—Deletes the selected item.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Enabling PPTP Fixup

This feature is disabled by default. Follow these steps to enable PPTP fixup:

1. Enter **1723** or a lower port number range in the **Low port** box.
2. Enter an upper port number range (if applicable) in the **High port** box.
3. Click **Add**.
4. Repeat Steps 1 through 3 if necessary.
5. Click **Apply**.

Disabling PPTP Fixup

Follow these steps to disable PPTP fixup:

1. Select the row you want to delete in the PPTP table.
2. Click **Delete**.
3. Click **Apply**.

Changing the PPTP Fixup Port Numbers

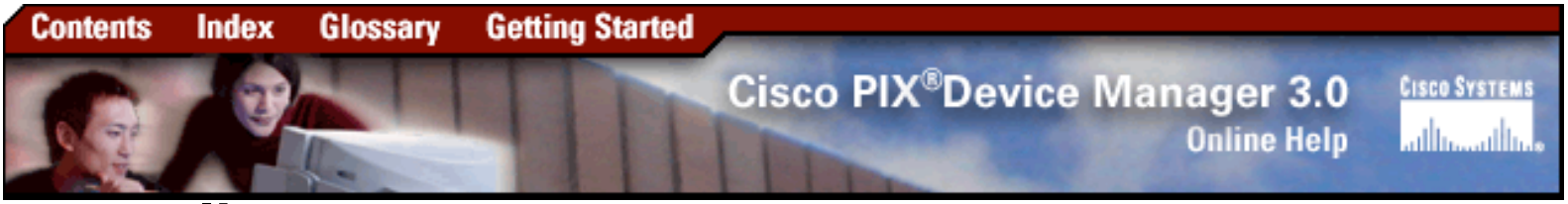
Follow these steps to change the PPTP fixup ports:

1. Select the port or port range you want to change in the PPTP table.
2. Click **Delete**.
3. Enter a port number or a lower port number range in the **Low port** box.
4. Enter an upper port number range (if applicable) in the **High port** box.
5. Click **Add**. The port or port number range appears in the PPTP table.
6. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.



IDS Policy

Configuration>System Properties>Intrusion Detection>IDS Policy

The **IDS Policy** panel lets you define Intrusion Detection System (IDS) policies. By defining IDS policies, you instruct the firewall to audit IP traffic going through the firewall, looking for pre-defined attack and informational signatures. For each IDS policy, you can instruct the firewall to send an alarm (syslog), drop the offending packet and/or reset the offending connection. You can also selectively enable your IDS policies on one or more of the firewall interfaces.

Auditing is performed by looking at the IP packets as they arrive at an input interface. If a packet triggers a signature and the configured action does not drop the packet, then the same packet can trigger other signatures. The firewall supports both inbound and outbound auditing. For a complete list of supported Cisco Secure IDS signatures, their wording, and whether they are attack or informational messages, refer to the *Cisco PIX Firewall System Log Messages* guide for your version of software.

The following sections are included in this Help topic:

- Related Information
- Field Descriptions
- Add
- Edit
- Delete
- Selecting IP Attack and IP Informational Actions
- Resetting to Last Applied Settings

Related Information

- Design Guide for implementing netForensics v2.1 with Cisco PIX Firewall, Cisco Intrusion Detection System
- *Cisco PIX Firewall System Log Messages* guide for your version of software

---

Field Descriptions

The **IDS Policy** panel displays the following fields:

- **Intrusion Detection Policy table**

    - **Name**—Displays the names of IDS rules you have defined.
    - **Type**—Describes the type of rule: Info or Attack.
    - **Action**—Defines the action taken when this rule is triggered. **Alarm** indicates that when a signature match is detected, PIX Firewall reports the event to all configured syslog servers. **Drop** drops the offending packet. **Reset** drops the offending packet and closes the connection if it is part of an active connection.

- **Add**—Opens the **Add** dialog box.
- **Edit**—Opens the **Edit** dialog box.
- **Delete**—Deletes the selected item.

- **Policy-to-Interface Mappings table**
    - **Interface**—Lists the interfaces on which your IDS policy can be enabled.
    - **Attack Policy**—Displays the specific attack policy, if any, for that interface.
    - **Info Policy**—Displays the specific info policy, if any, for that interface.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Adding IDS Policy Settings

Follow these steps to add a new IDS policy:

1. In the **IDS Policy** panel, click **Add**. The **Add IDS Policy** dialog box appears.
2. Define the new policy's name, type, and action(s), and click **OK**.
3. In the **IDS Policy** panel, click **Apply**.

Editing IDS Policy Settings

Follow these steps to modify an existing IDS policy:

1. In the **IDS Policy** panel, select the rule you want to change and click **Edit**. The **Edit IDS Policy** dialog box appears.
2. Change the policy settings as desired and click **OK**.
3. In the **IDS Policy** pane, click **Apply**.

Deleting an IDS Policy Setting

Follow these steps to remove an IDS policy:

1. In the **IDS Policy** panel, select the IDS rule you want to delete.
2. Click **Delete**.

3. Click **Apply**.

Selecting IP Attack and IP Informational Actions

Follow these steps to change the attack or informational policy for a firewall interface:

1. For the desired interface, choose an attack or info policy from the list in the **Policy-to-Interface Mappings** table.
2. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

IDS Signatures

Configuration>System Properties>Intrusion Detection>IDS Signatures

The **IDS Signatures** panel lets you select which signatures the firewall IDS system searches for. When a signature is enabled, the firewall audits the appropriate traffic and logs a message or takes other action if that signature is found. Note that enabling or disabling IDS signatures is only meaningful when you have enabled one or more IDS policies, using the **IDS Policy** panel.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Enabling or Disabling Signatures
- Resetting to Last Applied Settings

Important Notes

Auditing is performed by looking at the IP packets as they arrive at an input interface. If a packet triggers a signature and the configured action does not drop the packet, then the same packet can trigger other signatures. The PIX Firewall supports both inbound and outbound auditing. For a complete list of supported Cisco Secure IDS signatures, their wording, and whether they are attack or informational messages, refer to the *Cisco PIX Firewall System Log Messages* guide for your version of software.

Field Descriptions

The **IDS Signatures** panel displays the following fields:

- **IDS Signatures table**
  - **Enabled**—Lists the IDS signatures that are currently enabled.
  - **Disabled**—Lists the IDS signatures that are currently disabled.
- **Disable**—Select an enabled signature and click this button to disable it.
- **Enable**—Select a disabled signature and click this button to enable it.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Enabling or Disabling Signatures

Follow these steps to enable or disable IDS signatures:

1. Select one or more IDS signatures in the **Enabled** or **Disabled** column, and click the appropriate button to move them to the other column.
2. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Others

Configuration>System Properties>Logging>Others

The **Others** panel lets you define where syslog messages are sent for debugging purposes. You must have logging enabled in the **Logging Setup** panel to use these options.

The following sections are included in this Help topic:

- Field Descriptions
- Displaying Syslog Messages
- Resetting to Last Applied Settings

Field Descriptions

The **Others** panel displays the following fields:

- **Send to PIX Firewall console**—Selects a logging level from this list to send syslog messages of that level or lower to your PIX console. Levels are defined as follows:
  - Disabled (no logging)
  - Emergency (level 0, system unusable)
  - Alert (level 1, immediate action needed)
  - Critical (level 2, critical condition)
  - Error (level 3, error condition)
  - Warning (level 4, warning condition)
  - Notification (level 5, normal but significant condition)
  - Informational (level 6, informational message only)
  - Debugging (level 7, appears during debugging only)
- **Send to Telnet**—Selects a logging level from this list to send syslog messages to all the Telnet sessions connected to the firewall. Logging levels are defined in the preceding list.
- **Send to buffer**—Selects a logging level from this list to send syslog messages to an internal buffer for later review. Logging levels are defined in the preceding list.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Displaying Syslog Messages

1. Ensure that logging is enabled in the **Logging Setup** panel.
2. Choose a logging level in one or more of the lists to send syslog messages of that level or lower to the firewall console, all Telnet sessions, and/or an internal buffer, as desired.
3. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Rate Limit

Configuration>System Properties>Logging>Rate Limit

The **Rate Limit** panel lets you specify the number of syslog messages that the firewall can send to your syslog server. To make use of the syslog server(s) you must also enable logging using the **Logging Setup** panel. You can specify a rate limit for syslog logging levels, or be more specific and specify the rate of messages limited to a specific syslog message.

The following sections are included in this Help topic:

- Field Descriptions
- Specifying a Message Rate Limit Logging Level
- Specifying a Message Rate Limit Logging by Syslog Message ID
- Resetting to Last Applied Settings

Field Descriptions

The **Rate Limit** panel displays the following fields:

- **Rate Limit for syslog logging levels**
  - **Logging Level**—Displays syslog logging level. Levels are defined as follows:
    - Disabled (no logging)
    - Emergency (level 0, system unusable)
    - Alert (level 1, immediate action needed)
    - Critical (level 2, critical condition)
    - Error (level 3, error condition)
    - Warning (level 4, warning condition)
    - Notification (level 5, normal but significant condition)
    - Informational (level 6, informational message only)
    - Debugging (level 7, appears during debugging only)
  - **No of Messages**—Displays the number of messages sent to the syslog server.
  - **Time (Seconds)**—Displays the amount of time, in seconds, the syslog server is updated with syslog level messages.

- **Edit**—Select a server from the table and click this button to open the **Edit Rate Limit** dialog box, where you can edit the properties of the selected logging level.
- **Individually rate limited syslog messages**

- **Message ID**—Enter the syslog message ID for the syslog message you wish to limit.
- **No of Messages**—Displays the number of messages sent to the syslog server.

- **Time (Seconds)**—Displays the amount of time, in seconds, the syslog server is updated with syslog level messages.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Specifying a Message Rate Limit Logging Level

Follow these steps to specify a message rate limit logging level:

1. In the **Rate Limit for syslog logging levels** area, select the logging level you wish to modify. The **Edit Rate Limit** dialog box appears.
2. Configure the new rate limit settings as desired and click **OK**.
3. In the **Rate Limit** panel, click **Apply**.

Specifying a Message Rate Limit Logging by Syslog Message ID

Follow these steps to specify a message rate limit logging by syslog message ID:

1. In the **Individually rate limited syslog messages** area, select the logging level you wish to modify. The **Edit Rate Limit** dialog box appears.
2. Configure the new rate limit settings as desired and click **OK**.
3. In the **Rate Limit** panel, click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Edit Rate Limit

Configuration>System Properties>Logging>Edit Rate Limit

The **Edit Rate Limit** box lets you specify the number of messages the firewall can send to a syslog server, and the amount of time between updates to that server.

Field Descriptions

The **Edit Rate Limit** box displays the following fields:

- **Rate Limit for syslog logging levels**
  - **Logging Level**—Displays the selected syslog logging level. If you are modifying a specific syslog message ID rate limit, you may specify the logging level. Levels are defined as follows:
    - Disabled (no logging)
    - Emergency (level 0, system unusable)
    - Alert (level 1, immediate action needed)
    - Critical (level 2, critical condition)
    - Error (level 3, error condition)
    - Warning (level 4, warning condition)
    - Notification (level 5, normal but significant condition)
    - Informational (level 6, informational message only)
    - Debugging (level 7, appears during debugging only)
- **No of Messages**—Specifies the number of messages sent to the syslog server.
- **Time (Seconds)**—Specifies the amount of time, in seconds, the syslog server is updated with syslog level messages.

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Syslog

Configuration>System Properties>Logging>Syslog

The **Syslog** panel lets you specify the syslog servers to which the firewall will send syslog messages. To make use of the syslog server(s) you define on this panel, you must also enable logging using the **Logging Setup** panel.

The following sections are included in this Help topic:

- Field Descriptions
- Adding a Syslog Server
- Editing a Syslog Server
- Deleting a Syslog Server
- Resetting to Last Applied Settings

Field Descriptions

The **Syslog** panel displays the following fields:

- **Syslog Servers table**
  - **Interface**—Displays the firewall interface used to communicate with the syslog server.
- **IP Address**—Displays the IP address of the syslog server.
- **Protocol/Port**—Displays the protocol and port used by the syslog server.

- **Add**—Clicking this button will open the **Add Syslog Server** dialog box, where you can define the properties of a new syslog server.
- **Edit**—Select a server from the table and click this button to open the **Edit Syslog Server** dialog box, where you can edit the properties of the selected server.
- **Delete**—Clicking this button deletes the highlighted syslog server definition.
- **Facility**—Select a syslog facility for the host to use as a basis to file the messages. The default is LOCAL(4) 20, which is what most UNIX systems expect. However, because your network devices share the eight available facilities, you may need to change this value for syslog.
- **Level**—Select the level of logging messages to be sent to the syslog server. Levels are defined as follows:

  - Disabled (no logging)

- Emergency (level 0, system unusable)
- Alert (level 1, immediate action needed)
- Critical (level 2, critical condition)
- Error (level 3, error condition)
- Warning (level 4, warning condition)
- Notification (level 5, normal but significant condition)
- Informational (level 6, informational message only)
- Debugging (level 7, appears during debugging only)

- **Include Timestamp**—Select this check box to attach a timestamp to each syslog message saved.
- **Message Queue**—Enter the number of messages that are allowed to be queued on the firewall when the syslog server is busy. A zero value means an unlimited number of messages may be queued.

Adding a Syslog Server

Follow these steps to add a new syslog server:

1. In the **Syslog** panel, click **Add**. The **Add Syslog Server** dialog box appears.
2. Configure the new server settings as desired and click **OK**.
3. In the **Syslog** panel, click **Apply**.

Editing a Syslog Server

Follow these steps to change the settings of an existing syslog server:

1. In the **Syslog** panel, select the server definition you want to change and click **Edit**. The **Edit Syslog Server** dialog box appears.
2. Change the server settings as desired and click **OK**.
3. In the **Syslog** panel, click **Apply**.

Deleting a Syslog Server

Follow these steps to remove a syslog server:

1. In the **Syslog** panel, select the syslog server you want to delete.
2. Click **Delete**.
3. Click **Apply**.

Resetting to Last Applied Settings

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Advanced Syslog Configuration

Configuration>System Properties>Logging>Syslog>Advanced

The **Advanced Syslog Configuration** dialog box lets you configure syslog messages to include a device ID. If this feature is enabled, the device ID will be included in all non-EMBLEM (Enterprise Management BaseLine Embedded Manageability) formatted syslog messages. This feature is disabled by default.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Disabling Syslog Device ID

Important Notes

- The device ID is sent with the non-EMBLEM messages to the syslog server and is only visible from a syslog server, not from the PIX Firewall itself. Therefore, you will not see the device ID on the PIX Firewall console when issuing the "sh logg" command.

Field Descriptions

The **Syslog Advanced Configuration** panel displays the following fields:

- **Enable Syslog Device ID**—Enable this feature to include the device ID in all non-EMBLEM formatted syslog messages. This feature does not affect syslog messages in EMBLEM format. The default value is disabled.
- **Hostname**—Select this radio button to use the host name as the device ID.
- **IP Address**—Select this radio button to use the IP address as the device ID.
    - **Interface Name**—This box is enabled when the IP Address radio button is selected. Select an interface name from the drop-down list that contains all of the interface names that are configured on the device. The device ID will be the specified PIX Firewall interface IP address, regardless of the interface from which the message was sent. This provides a consistent device ID for all messages sent from a device. If an interface that does not have an IP address is chosen as the device ID, then 0.0.0.0 will be used.
- **String**—Select this radio button to use a user-defined string as the device ID.
    - **User-defined ID**—This box is enabled when the String radio button is selected. Specify a string that

does not exceed 16 characters or contain a space or &, ', ", or ? characters.

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Disabling Syslog Device ID

Follow these steps to exclude a Syslog Device ID:

1. In the **Advanced Syslog Configuration** panel, clear the **Enable Syslog Device ID** check box.
2. Click **OK**.

Copyright © 2001-2004, Cisco Systems, Inc.

Multicast

Configuration>System Properties>Multicast

The **Multicast** panel lets you configure the firewall to support multicast routing based on the Stub Multicast Routing (SMR) standard. SMR provides dynamic host registration and facilitates multicast routing by acting as an Internet Group Management Protocol (IGMP) proxy agent. When an IGMP report is received, the packet is multicast to the interface associated with the IGMP helper for processing according to the configured multicast routing protocol.

The following sections are included in this Help topic:

- Multicast Addressing
- Important Notes About Multicast
- Field Descriptions
  - Stub Multicast Routing
  - IGMP
    - Protocol
    - Access Group
    - Join Group
  - MRoute
- Enabling Multicast
- Enabling a Static Multicast Route
- Applying Changes

Important Notes About Multicast

- The firewall supports IGMP versions 1 and 2.
- To change IGMP settings, you must first enable multicast on a chosen interface under **Multicast>Stub Multicast Routing**.
- To change static multicast routes, use the **Multicast>MRoute** panel.
- You can permit or deny multicast access to and from particular networks using the **Multicast>IGMP>Access Groups** panel. If these access groups are applied, this function is performed before the packet is translated. These multicast access group rules act the same way as other access rules for other other types of packets. For more information about how access rules work, see Access Rules Help.
- The firewall does not pass multicast packets. Many routing protocols use multicast packets to transmit their data. If you need to send routing protocols across the firewall, configure the routers with the **neighbor** command. We consider it inherently dangerous to send routing protocols across the firewall. If the routes on the unprotected interface are corrupted, the routes transmitted to the protected side of the firewall will pollute routers there as well.
- For a primer on multicast on other Cisco equipment, see the Multicast Overview at http://www.cisco.com.

Multicast Addressing

Multicast addressing allows a source to transmit packets to multiple destinations, a multicast group, simultaneously.

Multicast addresses range from **224.0.0.0** to **239.255.255.255**, however only the range **224.0.1.0** to **239.255.255.255** is available.

The first part of the multicast address range, **224.0.0.0** to **224.0.0.255**, is reserved and referred to as the **Reserved Link Local Addresses** (RLLA). These addresses are unavailable.

See **Multicast** and **IP Addressing** for more information.

Field Descriptions

The **Multicast** panel provides the following fields:

Stub Multicast Routing

- The **Stub Multicast Routing** table displays the following columns:
  - **Interface**—Displays the interfaces available for multicast on the firewall
  - **multicast Enabled**—Displays the value **yes** if multicast is enabled on the interface listed in the column to the left, and the value **no** if multicast is disabled on that interface.
  - **Max Groups**—Displays the configured maximum number of groups enabled for multicast. This is an editable field with a value of 0 to 2000.
  - **Forward Interface**—Displays the interface that IGMP packets are forwarded to if IGMP forwarding is enabled.
- **Edit**—Opens the **Edit Enable Multicast Interface** box, where you can set up multicast on a selected interface.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

IGMP

The **IGMP** panel provides the following fields:

- **Protocol**—Lets you configure the IGMP Protocol settings for a selected interface.
  - The **Configure IGMP Protocol Settings** table displays the following columns:
    - **Interface**—Displays the interface name of the selected interface.
    - **Query Interval**—Displays the amount of time, in seconds, the firewall waits before querying for IGMP information.
    - **Response Time**—Displays the amount of time, in seconds, the firewall waits before responding with IGMP updates.
    - **Version**—Displays the version of IGMP the firewall is configured to use on the selected interface. The firewall supports both IGMP versions 1 and 2. The default is IGMP version 2.
  - **Edit**—Lets you configure the IGMP protocol settings previously listed on the selected interface.
- **Access Group**—Lets you permit or deny multicast packets for a selected network.
  - The **Access Groups** table displays the following columns:
    - **Action**—Displays whether multicast traffic is permitted or denied on the selected interface.
    - **Interface**—Displays the name of the interface on which the access rule is applied.
    - **Multicast** Group—Displays the IP address of the network the rule is applied to.
    - **Netmask**—Displays the netmask of the network the rule is applied to.

    The following buttons listed open a box that lets you configure the preceding values:

  - **Insert Before**—Lets you insert a multicast access rule above another previously configured rule.
  - **Insert After**—Lets you insert a multicast access rule below another previously configured rule.
  - **Add**—Lets you add a new multicast access rule.
  - **Edit**—Lets you edit an existing multicast access rule.
  - **Delete**—Lets you delete a multicast access rule.
- **Join Group**—Lets you join a multicast group. Multicast must be enabled for groups to be added.
  - The **Join Group** table displays the following columns:
    - **Interface**—Displays the interface on which the multicast group join rule is configured.
    - **Join Group Address**—Displays the group network IP addresses the firewall joins over the selected interface.

    The following buttons listed open a box that lets you configure the preceding values:

  - **Add**—Lets you join a multicast group on a selected interface by adding a multicast group join rule.
  - **Edit**—Lets you edit an existing multicast group join rule on a specified interface.
  - **Delete**—Lets you delete a multicast access group join rule.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

MRoute

The **MRoute** panel lets you configure static multicast routes.

- The **MRoute** table displays the following columns from left to right:
  - **Source Interface**—Displays the interface name of the source interface, where the firewall receives multicast packets.
  - **IP Address**—Displays the IP address of the of the source router, where the firewall receives multicast packets.
  - **Group Interface**—Displays the interface that the firewall forwards multicast information to.
  - **IP Address**—Displays the IP address of the configured network on which the firewall sends multicast packets. This can be any multicast (sp) IP address (224.0.0.0 - 239.255.255.255) for the group with the exception of RLLA addresses.
- **Edit**—Lets you edit an existing multicast static route.
- **Delete**—Lets you delete an existing multicast static route.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Enabling Multicast

Follow these steps to enable multicast:

1. Select **Multicast>Stub Multicast Routing**.
2. Select the interface you want to enable multicast on, then click **Edit**.
3. Check **Enable Multicast**, and select the maximum number of groups for this interface.
4. Optionally, you can enable IGMP forwarding by selecting **Enable IGMP Forwarding**, and specifying the interface on which to forward IGMP packets.
5. Click **OK**, then on the **Stub Multicast Routing** panel, click **Apply**.

Enabling a Static Multicast Route

Follow these steps to enable a static multicast route:

1. Select **Multicast>MRoute**.
2. Select the interface you want to create a static multicast route on, then click **Add**.
3. Enter the IP address your firewall receives static multicast packets from in the **Source IP Address** box, and then select or type the netmask of that host or network in the **Source Mask** box.
4. Select the interface you want the firewall to send the multicast packets to in the **Group Interface** list.
5. Specify the group that is to receive the multicast packets in the **Group IP Address** field. This must be a Reserved Link Local Address (RLLA) multicast IP address, in the range of 224.0.0.0-224.0.0.255.

6. Specify the group netmask in **Group Mask** box. If you are not sure which masks are valid, select one from the list.
7. Click **OK**, then in the Stub Multicast Routing panel, click **Apply**.

Applying Changes

If you do not wish to apply your recent change to the configuration click:

> **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Changes are not immediately applied to the running configuration. To apply your changes:

> **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

Copyright © 2001-2004, Cisco Systems, Inc.

Access Group

Configuration>System Properties>Multicast>IGMP>Access Group

The **Access Group** panel lets you configure the access groups, which control the multicast groups that hosts on the subnet serviced by an interface can join.

The following sections are included in this Help topic:

- Important Notes About Multicast
- Field Descriptions
  - Access Groups
  - Inserting an Access Group
- Applying Changes

Important Notes About Multicast

- The firewall supports IGMP versions 1 and 2.
- To change IGMP settings, first enable multicast on a chosen interface under **Multicast>Stub Multicast Routing**.
- To change static multicast routes, use the **Multicast>MRoute** panel.
- You can permit or deny multicast access to and from particular networks using the **Multicast>IGMP>Access Groups** panel. If these access groups are applied, this function is performed before the packet is translated. These multicast access group rules act the same way as other access rules for other other types of packets. For more information about how access rules work, see Access Rules Help.
- For a primer on multicast on other Cisco equipment, please see the Multicast Overview on http://www.cisco.com.

▲

Field Descriptions

Access Groups—Lets you permit or deny multicast packets for a selected network.

The **Access Groups** table displays the following columns:

- **Action**—Displays whether multicast traffic is permitted or denied on the selected interface.
- **Interface**—Displays the name of the interface to which the access rule is applied.
- **Multicast Group**—Displays the IP address of the network to which the rule is applied.
- **Netmask**—Displays the netmask of the network to which the rule is applied.

Inserting an Access Group

The following buttons open a box that lets you configure the preceding values:

- **Insert Before**—Lets you insert a multicast access rule above another previously configured rule.
- **Insert After**—Lets you insert a multicast access rule below another previously configured rule.
- **Add**—Lets you add a new multicast access rule.
- **Edit**—Lets you edit an existing multicast access rule.
- **Delete**—Lets you delete a multicast access rule.

Applying Changes

If you do not wish to apply your recent change to the configuration click:

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Changes are not immediately applied to the running configuration. To apply changes:

Apply—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

Copyright © 2001-2004, Cisco Systems, Inc.

Add/Edit IGMP Access Group

Configuration>System Properties>Multicast>IGMP>Access Group>Add/Edit IGMP Access Group

The **Add/Edit IGMP Access Group** box lets you modify the selected access groups.

The following sections are included in this Help topic:

- Important Notes About Multicast
- Add/Edit IGMP Access Group

Important Notes About Multicast

1. The firewall supports IGMP versions 1 and 2.
2. To change IGMP settings, you must first enable multicast on a chosen interface under **Multicast>Stub Multicast Routing**.
3. To change static multicast routes, use the **Multicast>MRoute** panel.
4. You can permit or deny multicast access to and from particular networks using the **Multicast>IGMP>Access Groups** panel. If these access groups are applied, this function is performed before the packet is translated. These multicast access group rules act the same way as other access rules for other other types of packets. For more information about how access rules work, see Access Rules Help.
5. For a primer on multicast on other Cisco equipment, see Multicast Overview on http://www.cisco.com.

Add/Edit IGMP Access Group—Lets you permit or deny multicast packets for a selected network.

The **Access Groups** table displays the following columns:

- **Interface Name**—Displays the name of the interface to which the access rule is applied.
- **Action**—Displays whether multicast traffic is permitted or denied on the selected interface.
- **Multicast Group**—Displays the IP Address of the network to which the rule is applied.
- **Netmask**—Displays the netmask of the network to which the rule is applied.
- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

Join Group

Configuration>System Properties>Multicast>IGMP>Join Group

The **Join Group** panel lets you join a multicast group.

The following sections are included in this Help topic:

- Important Notes About Multicast
- Field Descriptions
- Applying Changes

Important Notes About Multicast

- The firewall supports IGMP versions 1 and 2.
- To change IGMP settings, you must first enable multicast on a chosen interface under **Multicast>Stub Multicast Routing**.
- To change static multicast routes, use the **Multicast>MRoute** panel.
- You can permit or deny multicast access to and from particular networks using the **Multicast>IGMP>Access Groups** panel. If these access groups are applied, this function is performed before the packet is translated. These multicast access group rules act the same way as other access rules for other other types of packets. For more information about how access rules work, see Access Rules Help.
- For a primer on multicast on other Cisco equipment, see the Multicast Overview on http://www.cisco.com.

▲

Field Descriptions

Join Group—Lets you join a multicast group. multicast must be enabled for groups to be added.

The **Join Group** table displays the following columns:

- **Interface**—Displays the interface on which the multicast group join rule is configured.
- **Join Group Address**—Displays the group network IP addresses the PIX Firewall joins over the selected interface.

The buttons listed below open a box that lets you configure the preceding values:

- **Add**—Lets you join a multicast group on a selected interface by adding a multicast group join rule.
- **Edit**—Lets you edit an existing multicast group join rule on a specified interface.
- **Delete**—Lets you delete a multicast access group join rule.

Applying Changes

If you do not wish to apply your recent change to the firewall configuration click:

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Changes are not immediately applied to the running configuration. To apply changes:

Apply—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

Copyright © 2001-2004, Cisco Systems, Inc.

Add/Edit Join Group

Configuration>System Properties>Multicast>IGMP>Join Group>Add/Edit Join Group

The **Add/Edit IGMP Join Group** box lets you add or edit an IGMP join group.

The following sections are included in this Help topic:

- Important Notes About Multicast
- Field Descriptions

Important Notes About Multicast

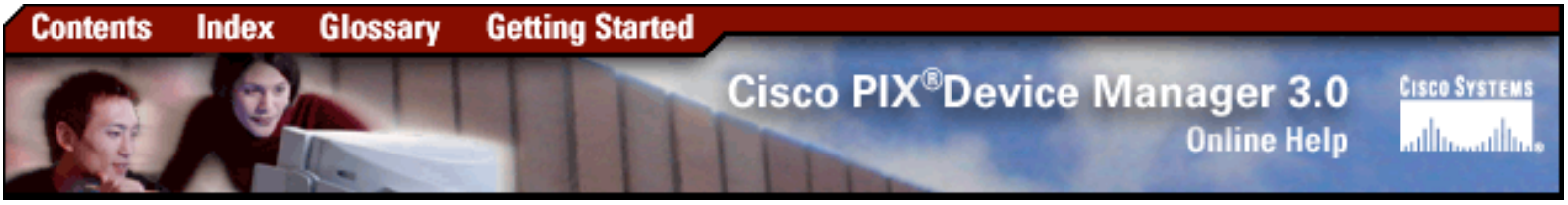
- The firewall supports IGMP versions 1 and 2.
- To change IGMP settings, you must first enable multicast on a chosen interface under **Multicast>Stub Multicast Routing**.
- To change static multicast routes, use the **Multicast>MRoute** panel.
- You can permit or deny multicast access to and from particular networks using the **Multicast>IGMP>Access Groups** panel. If these access groups are applied, this function is performed before the packet is translated. These multicast access group rules act the same way as other access rules for other other types of packets. For more information about how access rules work, see Access Rules Help.
- For a primer on multicast on other Cisco equipment, see the Multicast Overview on http://www.cisco.com.

Field Descriptions

The **Add/Edit Join Group** box displays the following fields:

- **Interface Name**—Lets you configure which interface the multicast group join rule is configured.
- **Join Group Address**—Lets you configure the group network IP addresses the firewall joins over the selected interface.

Copyright © 2001-2004, Cisco Systems, Inc.



MRoute

Configuration>System Properties>Multicast>MRoute

The **MRoute** panel lets you configure static multicast routes (SMR).

IP multicast static routes (mroutes) allow you to have multicast paths diverge from the unicast paths. When using multicast, the firewall expects to receive packets on the same interface where it sends unicast packets back to the source. This expectation is beneficial if your multicast and unicast topologies are congruent. However, you might want to configure unicast packets and multicast packets to take different paths.

The following sections are included in this Help topic:

- Important Notes About Multicast
- Field Descriptions
  - MRoute
- Enabling a Static Multicast Route
- Applying Changes

Routers send IGMP query messages through their attached local networks. Host members of a multicast group respond to a query by sending IGMP reports noting the multicast groups to which they belong. The multicast router takes responsibility for forwarding multicast datagrams from one multicast group to all other networks that have members in the group.

Important Notes About Multicast

1. The firewall supports IGMP versions 1 and 2.
2. To change IGMP settings, you must first enable multicast on a chosen interface under **Multicast>Stub Multicast Routing**.
3. To change static multicast routes, use the **Multicast>MRoute** panel.
4. You can permit or deny multicast access to and from particular networks using **Multicast>IGMP>Access Groups**. If these access groups are applied, this function is performed before the packet is translated. These multicast access group rules act the same way as other access rules for other other types of packets. For more information about how access rules work, see Access Rules Help.
5. For a primer on multicast on other Cisco equipment, see the Multicast Overview on http://www.cisco.com.

Field Descriptions

MRoute

The **MRoute** panel lets you configure static multicast routes.

- The **MRoute** table displays the following columns from left to right:
  - **Source Interface**—Displays the interface name of the source interface, where the PIX Firewall receives multicast packets.
  - **IP Address**—Displays the IP address of the of the source router, where the firewall receives multicast packets.
  - **Group Interface**—Displays the interface that the firewall forwards multicast information to.
  - **IP Address**—Displays the IP address of the configured network the PIX Firewall sends multicast packets. This can be any multicast IP address (224.0.0.0 - 239.255.255.255) for the group with the exception of RLLA addresses.
- **Add**—Lets you add a multicast static route.
- **Edit**—Lets you edit an existing multicast static route.
- **Delete**—Lets you delete an existing multicast static route.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Enabling a Static Multicast Route

Follow these steps to enable a static multicast route:

1. Select **Multicast>MRoute**.
2. Select the interface you want to create a static multicast route on, then click **Add**.
3. Enter the IP Address your firewall receives static multicast packets from in the **Source IP Address** field, and then select or type the netmask of that host or network in the **Source Mask** field.
4. Select the interface you want the PIX Firewall to send the multicast packets to in the **Group Interface** field.
5. Specify the group that is to receive the multicast packets in the **Group IP Address** field. This can be any multicast IP address (224.0.0.0 - 239.255.255.255) for the group with the exception of RLLA addresses.
6. Specify the group netmask in **Group Mask** field. If you are not sure which masks are valid, select one from the list.
7. Click **OK**, then on the Stub Multicast Routing panel, click **Apply**.

Applying Changes

If you do not wish to apply your recent change to the firewall configuration click:

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Changes are not immediately applied to the running configuration. To apply changes:

Apply—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

Copyright © 2001-2004, Cisco Systems, Inc.

Stub Multicast Routing

Configuration>System Properties>Multicast>Stub Multicast Routing

The technology used for multicast routing on the firewall is called Stub Multicast Routing (SMR). SMR provides dynamic host registration and facilitates multicast routing by acting as an Internet Group Management Protocol (IGMP) proxy agent. When an IGMP report is received, the packet is multicast to the interface associated with the IGMP helper for processing according to the configured multicast routing protocol.

When you use multicast routing in a large network, there are often stub regions over which the administrator has limited control. To reduce the configuration and administration burden, you can configure a subset of multicast functionality that provides the stub region with connectivity, but does not allow it to participate in or potentially complicate any routing decisions.

Stub IP multicast routing allows simple multicast connectivity and configuration at stub networks. It eliminates periodic flood-and-prune behavior across slow-speed links (ISDN and below) using dense mode. It eliminates that behavior by using forwarded IGMP reports as a type of join message and using selective multicast message filtering.

Stub IP multicast routing allows stub sites to be configured quickly and easily for basic multicast connectivity, without the flooding of multicast packets and subsequent group pruning that occurs in dense mode, and without excessive administrative burden at the central site.

The following sections are included in this Help topic:

- Important Notes About Multicast
- Field Descriptions
- Enabling multicast Routing
- Enabling a Static Multicast Route
- Applying Changes

Important Notes About Multicast

- The firewall supports IGMP versions 1 and 2.
- To change IGMP settings, you must first enable multicast on a chosen interface under **Multicast>Stub Multicast Routing**.
- To change static multicast routes, use the **Multicast>MRoute** panel.
- You can permit or deny multicast access to and from particular networks using the **Multicast>IGMP>Access Groups** panel. If these access groups are applied, this function is performed before the packet is translated. These multicast access group rules act the same way as other access rules

for other other types of packets. For more information about how access rules work, see Access Rules Help.

- For a primer on multicast on other Cisco equipment, see the Multicast Overview at http://www.cisco.com.

Field Descriptions

The **Multicast** panel provides the following fields:

Stub Multicast Routing

- The **Stub Multicast Routing** table displays the following columns:
  - **Interface**—Displays the interfaces available for multicast on the firewall.
  - **multicast Enabled**—Displays the value **yes** if multicast is enabled on the interface listed in the column to the left, and the value **no** if multicast is disabled on that interface.
  - **Max Groups**—Displays the configured maximum number of groups enabled for multicast. This is an editable field with a value of 0 to 2000.
  - **Forward Interface**—Displays the interface that IGMP packets are forwarded to if IGMP forwarding is enabled.
- **Edit**—Opens the **Edit Enable Multicast Interface** box, where you can set up multicast on a selected interface.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Enabling Multicast

Follow these steps to enable multicast:

1. Select **Multicast>Stub Multicast Routing**.
2. Select the interface you want to enable multicast on, then click **Edit**.
3. Select the **Enable Multicast** check box, and select the maximum number of groups for this interface.
4. Optionally, you can enable IGMP forwarding by selecting **Enable IGMP Forwarding**, and specifying the interface on which to forward IGMP packets.
5. Click **OK**, then in the Stub Multicast Routing panel, click **Apply**.

Applying Changes

If you do not wish to apply your recent change to the configuration click:

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Changes are not immediately applied to the running configuration. To apply changes:

Apply—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

Copyright © 2001-2004, Cisco Systems, Inc.

Add/Edit Mroute

Configuration>System Properties>Multicast>MRoute>Add/Edit Mroute

The **Add/Edit Multicast Route** panel lets you configure static multicast routes. Multicast addressing allows a source to transmit packets to multiple destinations, a multicast group, simultaneously.

The following sections are included in this Help topic:

- Multicast Addressing
- Field Descriptions
- Enabling a Static Multicast Route

Multicast Addressing

Multicast addressing allows a source to transmit packets to multiple destinations, a multicast group, simultaneously.

Multicast addresses range from **224.0.0.0** to **239.255.255.255**, however only the range **224.0.1.0** to **239.255.255.255** is available to us.

The first part of the multicast address range, **224.0.0.0** to **224.0.0.255**, is reserved and referred to as the **Reserved Local Link Addresses** (RLLA). These addresses are unavailable.

See **Multicast** and **IP Addressing** for more information.

▲

Note: The firewall does not pass multicast packets. Many routing protocols use multicast packets to transmit their data. If you need to send routing protocols across the firewall, configure the routers with the **neighbor** command. We consider it inherently dangerous to send routing protocols across the firewall. If the routes on the unprotected interface are corrupted, the routes transmitted to the protected side of the firewall will infect routers there as well.

Field Descriptions

Add Multicast Route provides the following fields:

- **Source Interface**—Displays the interface name of the source interface, where the firewall receives multicast packets. See **Configuration>System Properties>Interfaces**.
- **Source IP Address**—Displays the IP Address of the source router, where the firewall receives multicast packets. It must be a unicast, not multicast, IP address.
- **Source Mask**—The mask for the Source IP address

  Note: To avoid routing problems, the firewall defaults to 255.255.255.255 for the network mask. IP addresses and masks are usually provided together by your ISP or network administrator. Set the correct mask for the number of static IP addresses assigned to you by your ISP or network administrator. For more information, see Uses for Subnet Masks.

- **Group Interface**—Displays the interface that the firewall forwards multicast information to.
- **Group IP Address**—Displays the Group IP address of the configured network the firewall sends multicast packets. This can be any multicast IP address (224.0.0.0 - 239.255.255.255) for the group with the exception of RLLA addresses. See Multicast Addressing.
- **Group Mask**—The mask for the Group IP address of the interface

  Note: To avoid routing problems, the firewall defaults to 255.255.255.255 for the network mask. IP addresses and masks are usually provided together by your ISP or network administrator. Set the correct mask for the number of static IP addresses assigned to you by your ISP or network administrator. For more information, see Uses for Subnet Masks.

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

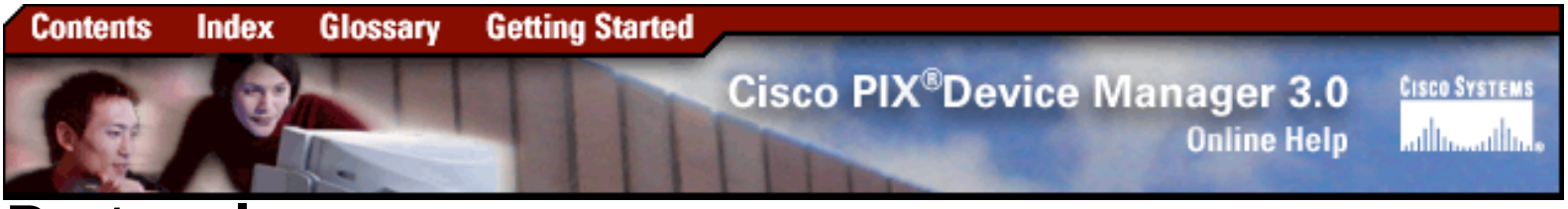
▲

Enabling a Static Multicast Route

Follow these steps to enable a static multicast route:

1. Select **Multicast>MRoute**.
2. Select the interface you want to create a static multicast route on, then click **Add**.
3. Enter the IP address your firewall receives static multicast packets from in **Source IP Address** , and then select or type the netmask of that host or network in **Source Mask**.
4. Select the interface you want the firewall to send the multicast packets to in **Group Interface**.
5. Specify the group that is to receive the multicast packets in **Group IP Address**. This must be a multicast IP address in the range of 224.0.1.0-239.255.255.255. See Multicast Addressing.
6. Specify the group netmask in **Group Mask**. If you are not sure which masks are valid, select one from the list.
7. Click **OK** to return to Stub Multicast Routing.
8. Click **Apply** to send changes to the firewall.

Copyright © 2001-2004, Cisco Systems, Inc.



Protocol

Configuration>System Properties>Multicast>IGMP>Protocol

The **Protocol** panel lets you configure the firewall to support multicast routing. The technology used for this on the firewall is called Stub Multicast Routing (SMR). SMR provides dynamic host registration and facilitates multicast routing by acting as an Internet Group Management Protocol (IGMP) proxy agent. When an IGMP report is received the packet is multicast to the interface associated with the IGMP helper for processing according to the configured multicast routing protocol.

IP hosts use IGMP to report their group membership to directly connected multicast routers. IGMP is an integral part of IP. RFC 2236 defines Internet Group Management Protocol Version 2.

IGMP uses group addresses, which are Class D IP addresses. The high-order four bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is guaranteed not to be assigned to any group. The address 224.0.0.1 is assigned to all systems on a subnet. The address 224.0.0.2 is assigned to all devices acting as multicast routers on a subnet.

The following sections are included in this Help topic:

- Important Notes About Multicast
- Field Descriptions
- Applying Changes

Important Notes About Multicast

1. The firewall supports IGMP versions 1 and 2.
2. To change IGMP settings, you must first enable multicast on a chosen interface under **Multicast>Stub Multicast Routing**.
3. To change static multicast routes, use the **Multicast>MRoute** panel.
4. You can permit or deny multicast access to and from particular networks using the **Multicast>IGMP>Access Groups** panel. If these access groups are applied, this function is performed before the packet is translated. These multicast access group rules act the same way as other access rules for other other types of packets. For more information about how access rules work, see Access Rules Help.
5. For a primer on multicast on other Cisco equipment, see the Multicast Overview on http://www.cisco.com.

▲

Field Descriptions

The **Protocol** panel provides the following fields:

IGMP

- **Protocol**—Lets you configure the IGMP Protocol settings for a selected interface.
  - The **Configure IGMP Protocol Settings** table displays the following columns:
    - **Interface**—Displays the interface name of the selected interface.
    - **Query Interval**—Displays the amount of time in seconds the firewall waits before querying for IGMP information.
    - **Response Time**—Displays the amount of time in seconds the firewall waits before responding with IGMP updates.
    - **Version**—Displays the version of IGMP the firewall is configured to use on the selected interface. The firewall supports both IGMP versions 1 and 2. The default is IGMP version 2.
  - **Edit**—Lets you configure the IGMP protocol settings listed above on the selected interface.

Applying Changes

If you do not wish to apply your recent change to the configuration click:

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Changes are not immediately applied to the running configuration. To apply changes:

Apply—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

Copyright © 2001-2004, Cisco Systems, Inc.

Edit IGMP Protocol Settings

Configuration>System Properties>Multicast>IGMP>Protocol>Edit IGMP Protocol Settings

The **Edit IGMP Protocol Settings** panel lets you enable Stub Multicast Routing on an interface and edit IGMP protocol settings.

The following sections are included in this Help topic:

- Field Descriptions

Field Descriptions

The **Edit IGMP Protocol Settings** panel provides the following fields:

- **Interface Name**—Displays the interface name of the selected interface.
- **Version**—Displays the version of IGMP the firewall is configured to use on the selected interface. The Firewall supports both IGMP versions 1 and 2. The default is IGMP version 2.
- **Query Interval**—Displays the amount of time in seconds the firewall waits before querying for IGMP information.
- **Response Time**—Displays the amount of time in seconds the firewall waits before responding with IGMP updates.
- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

Edit Enable Multicast Interface

Configuration>System Properties>Multicast>Stub Multicast Routing>Edit Enable Multicast Interface

The **Edit Enable Multicast Interface** dialog box lets you enable Stub Multicast Routing on an interface and enable IGMP forwarding.

Field Descriptions

The **Edit Enable Multicast Interface** box provides the following fields:

- **Enable Multicast on 'inside' interface**—Enables multicast on the selected interface. If you selected the outside interface when you clicked **Edit**, this check box is labeled **Enable Multicast on 'outside' interface**.
- **Max Groups**—Displays the configured maximum number of groups enabled for multicast. You can enter a value in the range of 0 to 2000.
- **Forward Interface**—Displays the interface that IGMP packets are forwarded to if IGMP forwarding is enabled.
- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

RIP

Configuration>System Properties>Routing>RIP

The **RIP** panel lets you display and edit the Routing Information Protocol (RIP) settings displayed in the **RIP** table.

The following sections are included in this Help topic:

- Field Descriptions
- Adding a RIP Interface
- Editing a RIP Interface
- Deleting RIP Interface
- Applying Changes

The default configuration enables IP routing table updates from RIP broadcast packets received from routers and other devices. However, the firewall unit cannot pass RIP updates between its own interfaces. The **RIP** panel provides additional control over the configuration, including selection of version 1 or 2. If you specify RIP version 2, authentication can be enabled and RIP updates can be encrypted using MD5 encryption.

RIP Version 2 Notes

1. Ensure that the key and key ID are the same as those used by any other device in your network that makes RIP version 2 updates.
2. In passive mode, PIX Firewall version 5.3 and higher accepts RIP version 2 multicast updates with an IP destination of 224.0.0.9.
3. In the RIP version 2 default mode, the firewall transmits default route updates using an IP destination of 224.0.0.9.
4. Configuring RIP version 2 registers the multicast address 224.0.0.9 on the respective interface to accept multicast RIP version 2 updates.
5. When the RIP version 2 commands for an interface are removed, the multicast address is unregistered from the interface card.

Field Descriptions

The **RIP** panel displays the following fields:

- **Interface**—The network interface name configured in Configuration>System Properties>Interfaces.
- **Action**—The action, **Broadcast default route** or **Passive RIP**, configured for each interface using the **Add RIP Configuration** dialog box.
- **Version**—The version of RIP, **1** or **2**, enabled for this interface. Version 2 is recommended. Use version 1 when backward compatibility is required.
- **Auth Type**—The type of authentication, **clear text** or **MD5**, to use when RIP version 2 is enabled. We recommend using MD5.
- **Authentication Key**—The encryption **Key**, a 16-character text string, shared with routers and other RIP version 2 devices communicating with the firewall.
- **Key ID**—The Key **ID** (identification), a number between 1 and 255, which must be shared with routers and other version 2 devices communicating with the firewall.

- **Add**—Opens the **Add** dialog box.
- **Edit**—Opens the **Edit** dialog box.
- **Delete**—Deletes the selected item.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Adding a RIP Interface

Follow these steps to add interfaces to the **RIP** table:

1. Click **Add** to open the **Add RIP Configuration** dialog box.
2. Select the interface that you want to add from the **interface** list of interfaces enabled in Configuration>System Properties>Interfaces.
3. Click the action option you want RIP to use, **broadcast/multicast default route** or **passive RIP**.
4. Under **version**, click the RIP version you want to use, **1** or **2**. If you select version 2, see RIP Version 2 Notes.
5. If you selected RIP version 2, you may enable authentication by selecting the **Enable Authentication** check box.
6. Enter the **Authentication Key** that will encrypt RIP updates and shared with other version 2 devices.
7. Enter the Key ID value to be shared with other version 2 devices in the **Key ID value** box.
8. Click **OK** to approve the addition and return to the **RIP** panel, the **Cancel** button to exit with no changes, or **Help** for more information.

Editing a RIP Interface Configuration

Follow these steps to **edit** the RIP configuration of interfaces in the **RIP Table**:

1. Select an interface from the **RIP** table by clicking the line beginning with the name of the interface.
2. Click **Edit** to open the **Edit RIP Configuration** dialog box.
3. Select the interface that you want to edit from the list of interfaces enabled in Configuration>System Properties>Interfaces.
4. Click the action option you want RIP to use, **broadcast/multicast default route** or **passive RIP**.
5. Under **version**, click the RIP version you want to use, **1** or **2**. If you select version 2, see RIP Version 2 Notes.
6. If you selected RIP version 2, you may enable authentication by selecting the **Enable Authentication** check box.
7. Enter the Authentication Key that will encrypt RIP updates and shared with other version 2 devices.
8. Enter the Key ID value to be shared with other version 2 devices in the **Key ID value** box.
9. To return to the previous panel click one of the following buttons:
   - **OK**—Accepts changes and returns to the previous panel.
   - **Cancel**—Discards changes and returns to the previous panel.
   - **Help**—Provides more information.

▲

Deleting RIP Interface Configurations

Follow these steps to delete RIP configurations from interfaces:

1. Select an interface from the **RIP Table** by selecting the interface in the **Interface** list.
2. Click **Delete**.

▲

Applying Changes

Changes to the table made by **Add**, **Edit**, or **Delete** are not immediately applied to the running configuration. You must click on one of the following buttons to apply or discard changes:

1. **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
2. **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last

time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Proxy ARPs

Configuration>System Properties>Proxy ARPs

The **Proxy ARPs** panel lets you enable or disable Proxy ARPs on each network interface.

The following sections are included in this Help topic:

- PIX Firewall and Proxy ARPs
- Field Descriptions
- Enabling or Disabling Proxy ARPs
- Applying Changes

ARP (Address Resolution Protocol) is a layer two protocol that resolves an IP address to a physical address, also called a Media Access Controller (MAC) address. A host sends an ARP request asking "Who is this IP?" The device owning the IP should reply with "Hey, I am the one, here's my MAC address."

Proxy ARP refers to a gateway device, in this case, the firewall, "impersonating" an IP address and returning its own MAC address to answer an ARP request for another device.

PIX Firewall and Proxy ARPs

The firewall builds a table from responses to ARP requests to map physical addresses to IP addresses. A periodic ARP function is enabled in the default configuration. The presence of entries in the ARP cache indicates that the firewall has network connectivity. The **show arp** command lists the entries in the ARP table. Usually, administrators do not need to manually manipulate ARP entries on the firewall. This is done only when troubleshooting or solving network connectivity problems.

The **arp** command is used to add an entry for new hosts on a network or when an existing host is exchanged for another. Alternatively, you can wait for the duration specified with the **arp timeout** command to expire and the ARP table rebuilds itself automatically with the new host information.

It is desirable to turn off the ARP function on interfaces connected to networks that do not change often and, in general, to improve performance, stability and general security. The **sysopt noproxyarp** command is used to disable Proxy ARPs on an interface from the command-line interface. For more information, see the *Cisco PIX Firewall Command Reference* for your version of software.

The **Proxy ARPs** panel provides a simple interface to disable Proxy ARPs on any of the firewall network interfaces.

With the use of VLANs in FWSM you can have up to 100 interfaces listed in the table.

Field Descriptions

The **Proxy ARPs** panel provides the following display:

- **Interface table**—The network interfaces which were configured in Configuration>System Properties>Interfaces are listed.
  - **Interface**—The interface on which Proxy ARP is enabled or disabled.
  - **Proxy ARP Enabled**—Displays if Proxy ARP is enabled or disabled.
- **Enable**—Click to enable Proxy ARPs for the selected interface.
- **Disable**—Click to disable Proxy ARPs for the selected interface.

Enabling and Disabling Proxy ARPs

Follow these steps to enable or disable Proxy ARPs:

1. Select the interface in the interface table on which you want to enable or disable Proxy ARPs. To select multiple interfaces at a time, select an interface, and then hold down the CTRL key while you click other interfaces that you want to select.
2. Click **Enable** to enable Proxy ARPs, or **Disable** to disable Proxy ARPs.

Applying Changes

Changes to the table made by **Add**, **Edit**, or **Delete** are not immediately applied to the running configuration. You must click one of the following buttons to apply or discard changes:

1. **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
2. **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Filtering

Configuration>System Properties>Routing>OSPF>Filtering

The **Filtering** panel lets you display and configure filter rules advertised in type 3 link-state advertisements (LSAs) between Open Shortest Path First (OSPF) areas of an Area Border Router (ABR).

The following sections are included in this Help topic:

- Field Descriptions
- Applying Changes to the Firewall

Field Descriptions

When a filter is configured, the following fields are populated in the table on the **Filtering** panel:

- **OSPF Process**—Displays the OSPF process ID for the selected filter.
- **Area ID**—Displays the area ID used by the selected filter.
- **Filtered Network**—Displays the filtered network used by the selected filter.
- **Traffic Direction**—Displays the direction traffic is filtered for the selected filter.
- **Sequence #**—Displays the sequence number for the filter entry.
- **Action**—Displays the action applied to the selected filter. Options available are **permit** and **deny**.
- **Lower Range**—Displays the lower range of the filtered network. This determines the lower range of the lengths of the netmasks that the filtering applies to.
- **Upper Range**—Displays the upper range of the filtered network. This determines the upper range of the lengths of the netmasks that the filtering applies to.

- **Add**—Click to add a filter.
- **Edit**—Click to edit an existing filter.
- **Delete**—Select a filter and click to delete a configured filter.

Applying Changes to the Firewall

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Add or Edit OSPF Filtering Entry

Configuration>System Properties>Routing>OSPF>Filtering>Add or Edit OSPF Filtering Entry

The **Add OSPF Filtering Entry** or **Edit OSPF Filtering Entry** panel lets you configure filter rules advertised in type 3 link-state advertisements (LSAs) between Open Shortest Path First (OSPF) areas of an Area Border Router (ABR).

ABR type 3 LSA filtering extends the capability of an ABR that is running OSPF to filter type 3 LSAs between different OSPF areas. This filtering is based on a rule defined by you. Once configured, only the specified networks are sent from one area to another area, or are restricted to their OSPF area. This type of area filtering can be applied to traffic going into or coming out of an OSPF area, or to both the incoming and outgoing traffic for that area.

The following sections are included in this Help topic:

- Field Descriptions
- Applying Changes to the Firewall

Field Descriptions

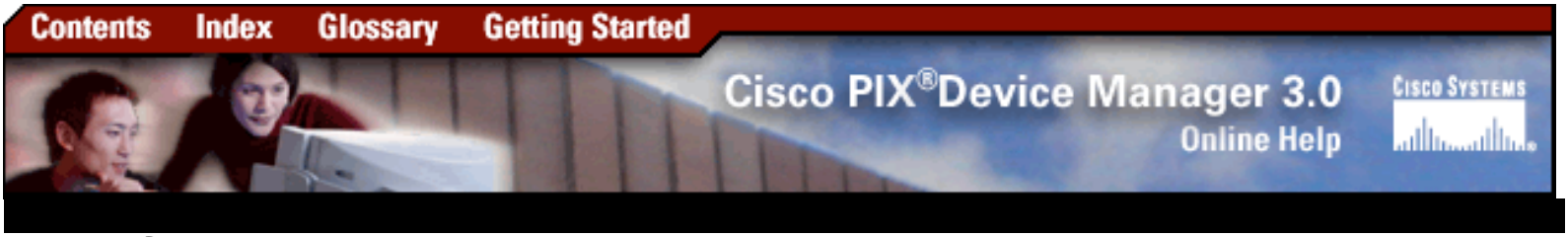
When a filter is configured, the following fields are populated in the table on the **Filtering** panel:

- **OSPF Process**—Select the OSPF process ID for the filter.
- **Area ID**—Select the area ID used by the filter.
- **Filtered Network**—Enter the network to be filtered. The format must be *network/subnet mask bits*. For example, 192.168.1.0/24, where the *network* is 192.168.1.0, and the *subnet mask bits* is 24. This would mean 192.168.1.0 is the network, and the subnet mask is 255.255.255.0.
- **Traffic Direction**—Select the direction that traffic is filtered, based on the selected filter. Options available are **inbound** and **outbound**.
- **Sequence #**—Enter the sequence number for the filter entry, between 1 and 4294967295.
- **Action**—Select the action applied to the selected filter. Options available are **permit** and **deny**.
- **Lower Range**—Enter the lower range of the filtered network, in subnet mask bits. The lower range must be less than or equal to the upper range, and greater than the subnet mask bits for the filtered network. For example, if you configure 172.100.1.0/24 to be the filtered network, the subnet mask bits are 24. The lower range must be greater than 24, that is 25-32.
- **Upper Range**—Select the upper range of the filtered network, in subnet mask bits. The upper range must be greater than or equal to the lower range.

Applying Changes to the Frewall

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.



Interface

Configuration>System Properties>Routing>OSPF>Interface

The **Interface** panel lets you configure interface specific OSPF routing parameters for all interfaces that are not disabled or shutdown.

The following sections are included in this Help topic:

- Field Descriptions
  - Authentication
  - Properties
- Applying Changes to the Firewall

Field Descriptions

Authentication

Displays the OSPF authentication properties for each interface. Select an interface in the table, and click **Edit** to edit the authentication properties for that interface. You can select no authentication, password authentication, or MD5 authentication.

Properties

Displays the OSPF routing properties for each interface. Select an interface in the table, and click **Edit** to edit the properties for that interface.You can change the cost and priority of the interface, and other advanced features.

Applying Changes to the Firewall

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Edit OSPF Interface Authentication

Configuration>System Properties>Routing>OSPF>Interface>Edit OSPF Interface Authentication

The **Edit OSPF Interface Authentication** dialog box lets you configure interface specific OSPF routing parameters.

Authentication should be used with all routing protocols when possible because route redistribution between OSPF and other protocols (like RIP) can potentially be used by attackers to subvert routing information. If MD5 authentication is used on all segments, security should not be an issue with OSPF.

Message Digest 5 (MD-5) authentication uses key-ids. Key-ids are used to determine the order that keys are tried. Key-ids are used when moving from an old key to a new key, and all OSPF routers may not have received the new key. Those routers that have not received the new key-id can use the old key until all the routers in the area have the new key.

The following sections are included in this Help topic:

- Field Descriptions
  - Interface
  - Authentication
    - Use Area authentication, if defined
    - No Authentication
    - Password Authentication
    - MD5 Authentication
- Applying Changes to the Firewall

Field Descriptions

Interface

Displays the interface changes that will be applied to when changes are made in this dialog box.

Authentication

- **Use Area authentication, if defined**—If an area has been defined for a specific interface, then Area authentication is used by default. If authentication is changed to something other than **Area authentication** for an interface that has an area defined, the specified area authentication is overridden. For more information on setting up areas, see Configuration>System Properties>OSPF>Setup>

Area / Networks. This is the default.

- **No Authentication**—Select to require no authentication between the PIX Firewall and neighboring or adjacent routers.
- **Password Authentication**—Select to assign a password to be used by neighboring routers that are using the OSPF simple password authentication. The variable password can be any continuous string of characters that can be entered from the keyboard, up to 8 bytes in length.
- **MD5 Authentication**—Select to enable OSPF Message Digest 5 (MD5) authentication. The key-id variable is a numerical identifier, from 1 to 255, for the authentication key, and the key variable is an alphanumeric password of up to 16 bytes.
    - **Add**—Click **Add** to add the entry to the **Key ID** table.
    - **Delete**—Highlight an entry in the **Key ID** table and click **Delete** to remove.

Applying Changes to the Firewall

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

Add or Edit an Area

Configuration>System Properties>Routing>OSPF>Setup>Area/Networks>Add an Area

The **Add an Area** and **Edit an Area** dialog box lets you add an OSPF area. The three types of OSPF areas are normal areas, stub areas, and not so stubby areas (NSSA).

The following sections are included in this Help topic:

- Overview
  - Normal Areas
  - Stub Areas
  - NSSA
- Field Descriptions
  - Area Type
    - Normal
    - Stub
    - NSSA
  - Area Networks
    - Enter IP Address and Mask
  - Authentication
    - None
    - Password
    - MD5
  - Default Cost
- Applying Changes to the Firewall

Overview

Normal Areas

Normal areas are areas which have no summary or redistribution attributes defined. A normal area can use password authentication, MD5 authentication, or no authentication.

Stub Areas

Stub areas are areas into which information on external routes is not sent. Instead, there is a default external route generated by the ABR into the stub area for destinations outside the autonomous system. To take advantage of the OSPF stub area support, default routing must be used in the stub area.

Not So Stubby Areas (NSSA)

The OSPF implementation of NSSA is similar to an OSPF stub area. NSSA does not flood type 5 external LSAs from the core into the area, but it can import autonomous system external routes in a limited fashion within the area.

NSSA allows importing of type 7 autonomous system external routes within NSSA area by redistribution. These type 7 LSAs are translated into type 5 LSAs by NSSA ABRs, which are flooded throughout the whole routing domain. Summarization and filtering are supported during the translation.

Use NSSA to simplify administration if you are an Internet service provider (ISP) or a network administrator that must connect a central site using OSPF to a remote site that is using a different routing protocol.

Prior to NSSA, the connection between the corporate site border router and the remote router could not be run as an OSPF stub area because routes for the remote site could not be redistributed into stub area, and two routing protocols needed to be maintained. A simple protocol like RIP was usually run and handled the redistribution. With NSSA, you can extend OSPF to cover the remote connection by defining the area between the corporate router and the remote router as an NSSA.

Field Descriptions

Area Type

- **Normal**—Displays the interface that changes will be applied to when changes are made in this dialog box.
- **Stub**—An OSPF area that carries a default route and intra- and inter-area routes but does not carry external routes. Virtual links cannot be configured across a stub area, and they cannot contain an Autonomous System Boundary Router (ASBR).
    - **Summary**—Clear this check box to reduce the number of summary link-state advertisements (LSAs type 3) sent into a stub area.
- **NSSA**—Select to configure an area as a not so stubby area (NSSA).
    - **Redistribute**—When the OSPF router is an NSSA Area Border Router (ABR) and you want the redistribute command to import routes only into the normal areas, and not into the NSSA area, select this check box.
    - **Summary**—Clear this check box to reduce the number of summary link-state advertisements sent into an NSSA.
    - **Default Information Originate**—Select to generate a Type 7 default in the NSSA area. This only takes effect on an NSSA ABR or an NSSA Autonomous System Boundary Router (ASBR).

Area Networks

- **Enter IP Address and Mask**—Enter the IP address and subnet mask of the network to be used by OSPF in this area, then click **Add**. To remove a network, select it from the IP Address table and click **Delete**.

Authentication

- **None**—Select to require no authentication between OSPF areas. This is the default.

- **Password**—Select to assign a password to be used by neighboring routers that are using the OSPF simple password authentication. The variable password can be any continuous string of characters that can be entered from the keyboard, up to 8 bytes in length.
- **MD5**—Select to enable OSPF Message Digest 5 (MD5) authentication. The key-id variable is a numerical identifier, from 1 to 255, for the authentication key, and the key variable is an alphanumeric password of up to 16 bytes.

Default Cost

The cost for the default summary route used for a stub or NSSA. The acceptable value is 0 to 65535. The default value for cost is 1.

Applying Changes to the Firewall

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

Edit OSPF Interface Advanced Properties

Configuration>System Properties>Routing>OSPF>Setup>Edit OSPF Interface Advanced Properties

The **Edit OSPF Interface Advanced Properties** dialog box lets you edit the OSPF intervals on a selected interface.

The following sections are included in this Help topic:

- Field Descriptions
  - Intervals (in seconds)
    - Hello Interval
    - Retransmit Interval
    - Transmit Delay
    - Dead Interval
- Applying Changes to the Firewall

Field Descriptions

Intervals (in seconds)

- **Hello Interval**—Enter a number to specify the interval between hello packets that the firewall sends on the interface. The default is 10 seconds, with a range from 1 to 65535.
- **Retransmit Interval**—Enter a number to specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The default value is 5 seconds, with a range from 1 to 65535.
- **Transmit Delay**—Enter a number to set the estimated time required to send a link-state update packet on the interface. The default value is 1 second, with a range from 1 to 65535.
- **Dead Interval**—Enter a number to set the dead interval before neighbors declare the router down (the length of time during which no hello packets are seen). The variable seconds specifies the dead interval and must be the same for all nodes on the network. The default for seconds is four times the interval set by the hello interval, from 1 to 65535.

Applying Changes to the Firewall

OK—Accepts changes and returns to the previous panel.

Cancel—Discards changes and returns to the previous panel.
Help—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

Edit OSPF Interface Properties

Configuration>System Properties>Routing>OSPF>Interface>Edit OSPF Interface Properties

The **Edit OSPF Interface Properties** dialog box lets you configure interface specific OSPF properties, such as cost cost of sending a packet on an interface, and router priority, which helps determine the designated router for this network.

The following sections are included in this Help topic:

- Field Descriptions
  - Interface
  - Cost
  - Priority
  - MTU Ignore
  - Database Filter
  - Advanced
- Applying Changes to the Firewall

Field Descriptions

- **Interface**—Displays the interface changes that will be applied to when changes are made in this dialog box.
- **Cost**—Enter a value from 1 to 65535 to explicitly specify the cost of sending a packet on an interface. The cost parameter is an unsigned integer value from 1to 65535, expressed as the link-state metric.
- **Priority**—A positive integer from 0 to 255 that specifies the priority of the router. The default is 1. The router priority helps determine the designated router for this network. Setting the priority to zero means the PIX Firewall will not become the designated router.
- **MTU Ignore**—Disables OSPF MTU mismatch detection on receiving DBD packets and is enabled by default.
- **Database Filter**—Select this check box to filter outgoing link-state advertisements (LSAs) to an OSPF interface.
- **Advanced**—Opens the **Edit OSPF Interface Advanced** dialog box, where you can edit intervals.

Applying Changes to the Firewall

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.

- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

Redistribution

Configuration>System Properties>Routing>OSPF>Redistribution

Routes that originate from other routing protocols (or different OSPF processes) and that are injected into OSPF through redistribution are called external routes. There are two forms of external metrics: type 1 and type 2. These routes are represented by O E2 (for type 2) or O E1 (for type 1) in the IP routing table, and they are examined after the firewall is done building its internal routing table. After they are examined, they are flooded throughout the autonomous systems (AS), unaltered. (Autonomous systems are a collection of networks, subdivided by areas, under a common administration sharing a common routing strategy.)

OSPF type 1 metrics result in routes adding the internal OSPF metric to the external route metric; they are also expressed in the same terms as an OSPF link-state metric. The internal OSPF metric is the total cost of reaching the external destination, including whatever internal OSPF network costs are incurred to get there. These costs are calculated by the device wanting to reach the external route.

OSPF type 2 metrics do not add the internal OSPF metric to the cost of external routes and are the default type used by OSPF. The use of OSPF type 2 metrics assumes that you are routing between autonomous systems (AS); therefore, the cost is considered greater than any internal metrics. This eliminates the need to add the internal OSPF metrics.

The following sections are included in this Help topic:

- Field Descriptions
- Applying Changes to the Firewall

Field Descriptions

When redistribution is configured, the following fields are populated in the table on the **Redistribution** panel:

- **OSPF Process**—Displays the OSPF process ID for the selected virtual link.
- **Protocol**—The protocol used by for redistribution.
- **Match**—Displays the match for route matching.
- **Subnets**—Displays the OSPF authentication properties for the virtual link.
- **Metric Value**—The metric value for a routing protocol. The value is an integer from -2147483647 to 2147483647.
- **Metric Type**—OSPF metric type for default routes, either type 1 or 2. The default is type 2.
- **Tag Value**—The value to match (for controlling redistribution with route maps). The valid range is 0 to 4294967295.
- **Route Map**—The name of an access control list (ACL) used for route mapping.

- **Add**—Click to add a redistribution entry.
- **Edit**—Click to edit an existing redistribution entry.
- **Delete**—Select a virtual link and click to delete a configured redistribution entry.

Applying Changes to the firewall

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Add or Edit Redistribution Entry

Configuration>System Properties>Routing>OSPF>Redistribution>
Add or Edit Redistribution Entry

The **Add Redistribution Entry** or **Edit Redistribution Entry** dialog box lets you configure parameters related to redistribution of routes within an OSPF area.

The following sections are included in this Help topic:

- Field Descriptions
- Applying Changes to the Firewall

Field Descriptions

When redistribution is configured, the following fields are populated in the table on the **Redistribution** panel:

- **OSPF Process**—Displays the OSPF process ID for which redistribution is defined.
- **Protocol**—The protocol used by for redistribution.
  - **Static**—Select to use a static route for redistribution.
  - **Connect**—Select to use a connected route for redistribution.
  - **OSPF**—Select an OSPF area ID for redistribution.
- **Match**—Select the appropriate check box for route matching.
- **Use Subnets**—Select to redistribute subnets. The default is redistribute only classful networks.
- **Metric Value**—The metric value for a routing protocol. The value is an integer from 1 to 65535.
- **Metric Type**—OSPF metric type for default routes, either type 1 or 2. The default is type 2.
- **Tag Value**—The value to match (for controlling redistribution with route maps). The valid range is 0 to 4294967295.
- **Route Map**—The name of the route map.

Applying Changes to the Firewall

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

Add a Route Summarization Entry

Configuration>System Properties>Routing>OSPF>Setup>Route Summarization>
Add a Route Summarization Entry

The **Add a Route Summarization Entry** dialog box lets you configure route summarization information for a selected OSPF process. Route summarization is the consolidation of advertised addresses. This feature causes a single summary route to be advertised to other areas by an ABR. In OSPF, an ABR will advertise networks in one area into another area. If the network numbers in an area are assigned in a way such that they are contiguous, you can configure the ABR to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

The following sections are included in this Help topic:

- Field Descriptions
  - Process ID
  - Area ID
  - IP Address
  - Netmask
  - Advertise
- Applying Changes to the Firewall

Field Descriptions

- **Process ID**—Select the process ID for route summarization.
- **Area ID**—Select the area ID for route summarization.
- **IP Address**—Enter the IP address of the network to have its routes summarized.
- **Netmask**—Enter the subnet mask of the network to have its routes summarized.
- **Advertise**—Check to advertise summarized routes with Type 3 summary LSAs. If this check box is cleared, Type 3 summary LSAs are suppressed, and the component networks remain hidden from other networks.

Applying Changes to the Firewall

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

Summary Address

Configuration>System Properties>Routing>OSPF>Summary Address

The **Summary Address** panel lets you display, add, edit, or delete OSPF summary address information. Summary addresses create aggregate addresses for OSPF.

Route summarization is the consolidation of advertised addresses. This feature causes a single summary route to be advertised to other areas by an ABR. In OSPF, an ABR will advertise networks in one area into another area. If the network numbers in an area are assigned in a way such that they are contiguous, you can configure the ABR to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

The following sections are included in this Help topic:

- Field Descriptions
- Applying Changes to the Firewall

Field Descriptions

When a summary addressing is configured, the following fields are populated in the table on the **Summary Address** panel.

- **OSPF Process**—Displays the OSPF process ID for the selected summary address entry.
- **IP Address**—The summary address designated for a range of addresses used by the selected summary address entry.
- **Netmask**—The IP subnet mask used for the summary route by the selected summary address entry.
- **Advertise**—Diplays whether or not the summary should be advertised.
- **Tag**—The value to match (for controlling redistribution with route maps).

- **Add**—Click to add a summary address entry.
- **Edit**—Click to edit an existing summary address entry.
- **Delete**—Select a summary address entry and click to delete a summary address entry.

Applying Changes to the Firewall

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use

the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Add or Edit OSPF Summary Address Entry

Configuration>System Properties>Routing>OSPF>Summary Address>
Add or Edit OSPF Summary Address Entry

The **Add OSPF Summary Address Entry or Edit OSPF Summary Address Entry** dialog box lets you configure OSPF summary address information. Summary addresses create aggregate addresses for OSPF.

The following sections are included in this Help topic:

- Field Descriptions
- Applying Changes to the Firewall

Field Descriptions

When summary addressing is configured, the following fields are populated in the table on the **Summary Address** panel.

- **OSPF Process**—Select the OSPF process ID for the summary address entry.
- **IP Address**—Enter the summary address designated for a range of addresses for use by the summary address entry.
- **Netmask**—Select the IP subnet mask used for the summary route.
- **Advertise**—If the network numbers in an area are assigned in a way such that they are contiguous, you can configure the firewall to advertise a summary route that covers all the individual networks within the area that fall into the specified range by selecting this check box.
- **Tag**—A tag value that can be used as a "match" value for controlling redistribution via route-maps.

Applying Changes to the Firewall

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

Virtual Links

Configuration>System Properties>Routing>OSPF>Virtual Links

The **Virtual Link** panel lets you add, edit or delete a virtual link.

In OSPF, all areas must be connected to a backbone area. If there is a break in backbone continuity, or the backbone is purposefully partitioned, you can establish a virtual link. The two endpoints of a virtual link are ABRs. The virtual link must be configured in both routers. The configuration information in each router consists of the other virtual endpoint (the other ABR) and the non-backbone area that the two routers have in common (called the transit area). Note that virtual links cannot be configured through stub areas.

The following sections are included in this Help topic:

- Field Descriptions
- Applying Changes to the Firewall

Field Descriptions

When a virtual link is configured, the following fields are populated in the table on the **Virtual Link** panel.

- **OSPF Process**—Displays the OSPF process ID for the selected virtual link.
- **Area ID**—Displays the area ID used by the selected virtual link.
- **Peer Router ID**—Displays the peer router ID used by the selected virtual link.
- **Authentication**—Displays the OSPF authentication properties for the virtual link.

- **Add**—Click to add a virtual link.
- **Edit**—Click to edit an existing virtual link.
- **Delete**—Select a virtual link and click to delete a configured virtual link.

Applying Changes to the Firewall

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last

time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Add or Edit a Virtual Link

Configuration>System Properties>Routing>OSPF>Virtual Links>Add or Edit a Virtual Link

The **Add a Virtual Link or Edit a Virtual Link** dialog box lets you configure the parameters available for virtual links.

The following sections are included in this Help topic:

- Field Descriptions
- Applying Changes to the Firewall

Field Descriptions

- **OSPF Process**—Select the OSPF process ID for the virtual link.
- **Area ID**—Select the area ID used by the virtual link.
- **Peer Router ID**—Enter the peer router ID used by the virtual link.
- **Advanced**—Opens the Edit Virtual Link Advanced Properties dialog box, where you can configure authentication and intervals.

Applying Changes to the Firewall

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

Edit Virtual Link Advanced Properties

Configuration>System Properties>Routing>OSPF>Virtual Links>Add or Edit a Virtual Link>
Edit Virtual Link Advanced Properties

The **Edit Virtual Link Advanced Properties** dialog box lets you configure authentication and intervals available for virtual links.

The following sections are included in this Help topic:

- Field Descriptions
  - Authentication
    - No Authentication
    - Password Authentication
    - MD5 Authentication
  - Intervals (in seconds)
    - Hello Interval
    - Retransmit Interval
    - Transmit Delay
    - Dead Interval
- Applying Changes to the Firewall

Field Descriptions

Authentication

- **No Authentication**—Select to require no authentication between OSPF areas. This is the default.
- **Password Authentication**—Select to assign a password to be used by neighboring routers that are using the OSPF simple password authentication. The variable password can be any continuous string of characters that can be entered from the keyboard, up to 8 bytes in length.
- **MD5 Authentication**—Select to enable OSPF Message Digest 5 (MD5) authentication. The key-id variable is a numerical identifier, from 1 to 255, for the authentication key, and the key variable is an alphanumeric password of up to 16 bytes.
  - **Add**—Click **Add** to add the entry to the **Key ID** table.
  - **Delete**—Highlight an entry in the **Key ID** table and click **Delete** to remove.

Intervals (in seconds)

- **Hello Interval**—Enter a number to specify the interval between hello packets that the firewall sends on the interface. The default is 10 seconds, with a range from 1 to 65535.
- **Retransmit Interval**—Enter a number to specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The default value is 5 seconds, with a range from 1 to 65535.
- **Transmit Delay**—Enter a number to set the estimated time required to send a link-state update packet on the interface. The default value is 1 second, with a range from 1 to 65535.
- **Dead Interval**—Enter a number to set the dead interval before neighbors declare the router down (the length of time during which no hello packets are seen), use the ospf dead-interval seconds subcommand. The variable seconds specifies the dead interval and must be the same for all nodes on the network. The default for seconds is four times the interval set by the **ospf hello-interval** command, from 1 to 65535.

Applying Changes to the Firewall

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

Add AAA Server

VPN Wizard>Add AAA Server

AAA Server Group lets you define the location of the authentication, authorization, and accounting (AAA) server, the group name and the protocol used for AAA.

To change other AAA server settings or add up to 14 additional AAA servers, use the **AAA** category on the **System Properties** tab.

The following sections are included in this Help topic:

- Field Descriptions

Field Descriptions

The **AAA Server Group** window displays the following fields:

- **AAA Server Group Name**—An alphanumeric string which is the name of the server group.
- **Protocol**—Select the protocol used for a configured AAA server. The options are **TACACS+** and **RADIUS**.
- **Server IP Address**—The IP address of the TACACS+ or RADIUS server.
- **Interface**—The interface on which the AAA server resides.
- **Key**—A case-sensitive, alphanumeric keyword of up to 127 characters that is the same value as the key on the TACACS+ server. Any characters entered past 127 are ignored. The key is used between the client and server for encrypting data between them. The key must be the same on both the client and server systems. Spaces are not permitted in the key, but other special characters are.
- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

Attributes Pushed to Client (Optional)

VPN Wizard>Attributes Pushed to Client (Optional)

You have the option to push additional attributes to your VPN clients using the **VPN Wizard>Attributes Pushed to Client (Optional)** panel. These attributes will only work with a Cisco VPN Client v3.x or higher.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

The attributes you can include are DNS, WINS, and default domain name to be pushed to the Cisco VPN Client v3.x.

To change other optional VPN client attributes that are pushed to the client, use the **Remote Access>Cisco VPN Client** category on the **VPN** tab.

Important Notes

- If you are using Cisco VPN 3000 Client version 2.5, use the **Remote Access>Cisco VPN Client>Add** category on the **VPN** tab to configure these options, and select the **Select if you are using Version 2.5** check box.
- Any attribute field you leave blank will not be pushed to VPN clients.

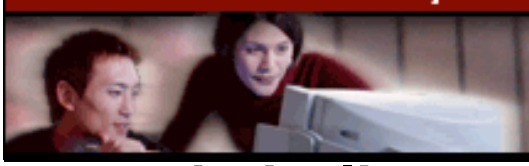
Field Descriptions

The **VPN Wizard>Attributes Pushed to Client (Optional)** panel displays the following fields:

- **Primary DNS Server**—The IP address of the primary DNS server.
- **Secondary DNS Server**—The IP address of the secondary DNS server.
- **Primary WINS Server**—The IP address of the primary WINS server.
- **Secondary WINS Server**—The IP address of the secondary WINS server.
- **Default Domain Name**—The default domain name.
- **Back**—Returns you to the previous panel.
- **Next**—Advances you to the next panel.
- **Finish**—Submits your configuration to the firewall based upon choices made in the previous panels. This button is dimmed until all necessary steps have been completed in the Wizard.
- **Cancel**—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard**

dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.



Extended Client Authentication

VPN Wizard>Extended Client Authentication

Use the **Extended Client Authentication** panel to require Virtual Private Network (VPN) client users to authenticate from an authentication, authorization, and accounting (AAA) server for access to the private network on your firewall.

Extended Client Authentication is optional, and is not required for VPN client access to the private network.

Extended Authentication (Xauth) is a feature within the IKE protocol. Xauth lets you deploy IPSec VPNs using TACACS+ or RADIUS, or LOCAL as your user authentication method.

This feature, which is designed for VPN clients, provides user authentication by prompting the user for username and password and verifies them with the information stored in your TACACS+ or RADIUS database. Xauth is negotiated between IKE Phase 1 (IKE device authentication phase) and IKE Phase 2 (IPSec SA negotiation phase). If the Xauth fails, the IPSec security association will not be established and the IKE security association will be deleted.

A AAA server must be defined before Xauth will work on the firewall. You can define the AAA server using the **New** button. This will open the **AAA Server Group** panel where you can define the location of the AAA server, the group name and the protocol used for AAA.

To change other AAA server settings, use the **AAA** category on the **System Properties** tab.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

Important Notes

- The IKE Mode Config feature also is negotiated between these IKE Phase 1 and 2. If both features are configured, Xauth is performed first.
- The VPN client remote user should be running the Cisco Secure VPN Client version 1.1, Cisco VPN 3000 Client version 2.5, or Cisco VPN 3000 Client version 3.0. We recommend Cisco VPN 3000 Client version 3.0 or later.

Field Descriptions

The **Enable Extended Client Authentication** panel displays the following fields:

- **Enable Extended Client Authentication**—Check to enable Xauth on your firewall.
- **Extended Authentication for group [name]**—Displays the group name you specified on a previous panel.
- **AAA Server Group**—Select which protocol is used for a configured AAA server. The options are TACACS+ and RADIUS, and LOCAL. If LOCAL authentication is selected, **AAA server uses one time password** check box will not be selectable.
- **New**—Click to open the **AAA Server Group** panel where you can define the location of the AAA server, the group name and the protocol used for AAA.
- **AAA server uses one time password**—Check to enable Xauth to require a one time password for users. An example of this would be a hardware or software token password generating mechanism.
- **Back**—Returns you to the previous panel.
- **Next**—Advances you to the next panel.
- **Finish**—Submits your configuration to the firewall based upon choices made in the previous panels. This button is dimmed until all necessary steps have been completed in the Wizard.
- **Cancel**—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

IPSec Traffic Selector (continued)

VPN Wizard>IPSec Traffic Selector (continued)

Use the **IPSec Traffic Selector (continued)** panel to identify the traffic that you want to protect using the current IPSec tunnel. The current IPSec tunnel will protect packets that are sent to or received from the hosts or networks that you select on this panel. Use this panel to identify the hosts and networks protected by protected by the remote IPSec peer. Use the previous panel, (**IPSec Traffic Selector)** to identify hosts and networks protected by your local PIX Firewall.

Select the appropriate button on this panel for identifying hosts and networks using an IP address, a host name, or a group.To define a group of hosts or networks, use the **Hosts/Networks** tab.

The following sections are included in this Help topic:

- IP Address
- Name
- Group
- Selected

IP Address

Enable this button to identify hosts or networks by their IP address, using the controls described in this section.

Interface—Use this field to identify the firewall interface connected to the hosts or networks that you want to protect.

IP address—Use this field to enter the IP address in dotted-decimal notation for the hosts or networks that you want to protect. After entering each address, click **->** to add the address to the **Selected** list.

Mask—Use this list to select the subnet mask of the hosts or networks that you want to protect and click **->** to add the address to the **Selected** list.

Browse—Click this button to display the **Select host/network** panel. Choose the hosts or networks you want to protect from the **Select host/network** panel and click **OK**.

Name

Enable this button to identify hosts by their host names. Enter the fully qualified domain name of each host in the **Name** field and click **->** to add each host to the **Selected** list.

Group

Enable this button to identify hosts or networks by a predefined group name, using the controls described in this section.

Interface—Use this field to identify the firewall interface connected to the hosts or networks that you want to protect.

Group—Use this list to select the predefined group name containing the hosts or networks that you want to protect.

To define a new group of hosts or networks, use the **Hosts/Networks** tab from the PDM main window.

Selected

This list shows the hosts, networks, or groups of hosts and networks that are selected to be protected by the current VPN tunnel. To add hosts, networks, or groups to this list, select the appropriate button, identify the host, network, or group using the controls on the left side of the panel, and click **->**. To remove hosts, networks, or groups from this list, select them and click **<-**.

Back—Returns you to the previous panel.

Next—Advances you to the next panel.

Finish—Submits your configuration to the firewall based upon choices made in the previous panels. This button is dimmed until all necessary steps have been completed in the Wizard.

Cancel—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

IPSec Traffic Selector

VPN Wizard>IPSec Traffic Selector

Use the **IPSec Traffic Selector** panel to identify the traffic that you want to protect using the current IPSec tunnel. The current IPSec tunnel will protect packets that are sent to or received from the hosts or networks that you select on this panel. Use this panel to identify the hosts and networks protected by your local PIX Firewall. Use the **IPSec Traffic Selector (continued)** panel, which follows, to identify hosts and networks protected by the remote IPSec peer.

Select the appropriate button on this panel for identifying hosts and networks using an IP address, a host name, or a group.To define a group of hosts or networks, use the **Hosts/Networks** tab.

The following sections are included in this Help topic:

- IP Address
- Name
- Group
- Selected

IP Address

Enable this button to identify hosts or networks by their IP address, using the controls described in this section.

Interface—Use this field to identify the firewall interface connected to the hosts or networks that you want to protect.

IP address—Use this field to enter the IP address in dotted-decimal notation for the hosts or networks that you want to protect. After entering each address, click **->** to add the address to the **Selected** list.

Mask—Use this list to select the subnet mask of the hosts or networks that you want to protect and click **->** to add the address to the **Selected** list.

Browse—Click this button to display the **Select host/network** panel. Choose the hosts or networks you want to protect from the **Select host/network** panel and click **OK**.

Name

Enable this button to identify hosts by their host names. Enter the fully qualified domain name of each host in the **Name** field and click **->** to add each host to the **Selected** list.

Group

Enable this button to identify hosts or networks by a predefined group name, using the controls described in this section.

Interface—Use this field to identify the firewall interface connected to the hosts or networks that you want to protect.

Group—Use this list to select the predefined group name containing the hosts or networks that you want to protect.

To define a new group of hosts or networks, use the **Hosts/Networks** tab from the PDM main window.

Selected

This list shows the hosts, networks, or groups of hosts and networks that are selected to be protected by the current VPN tunnel. To add hosts, networks, or groups to this list, select the appropriate button, identify the host, network, or group using the controls on the left side of the panel, and click **->**. To remove hosts, networks, or groups from this list, select them and click **<-**.

Back—Returns you to the previous panel.

Next—Advances you to the next panel.

Finish—Submits your configuration to the firewall based upon choices made in the previous panels. This button is dimmed until all necessary steps have been completed in the Wizard.

Cancel—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

L2TP and IPSec

VPN Wizard>L2TP and IPSec

Use **VPN Wizard>L2TP and IPSec** to configure L2TP on your firewall for remote client authentication.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

Layer Two Tunneling Protocol (L2TP) is a VPN tunneling protocol which allows remote clients to use the public IP network to securely communicate with private corporate network servers. L2TP uses PPP over UDP (port 1701) to tunnel the data. L2TP protocol is based on the client/server model. The function is divided between the L2TP Network Server (LNS), and the L2TP Access Concentrator (LAC). The LNS typically runs on a network gateway such as a router, while the LAC can be a dial-up Network Access Server (NAS), or a PC with a bundled L2TP client such as Microsoft Windows 2000.

PIX Firewall with L2TP/IPSec support provides the capability to deploy and administer an L2TP VPN solution alongside the IPSec VPN and PIX Firewall services in a single platform.

To change other L2TP settings, use the use the **Remote Access>L2TP/PPTP>Add** category on the **VPN** tab.

Important Notes

- L2TP will not work independently of IPSec on the firewall. IPSec must be configured to make L2TP work. The VPN Wizard will walk you through the steps to configure IPSec, so you can use L2TP for authentication.

Field Descriptions

The **Authentication** group box displays the following fields:

- **Pre-shared key (Wild-card Key)**—Enter an alphanumeric pre-shared key to be used by the VPN client.
- **Re-enter key**—Retype the pre-shared key in this box.
- **Certificate**—Select to use certificates issued by a trusted certification authority (CA) to authenticate the VPN client.

- **Back**—Returns you to the previous panel.
- **Next**—Advances you to the next panel.
- **Finish**—Submits your configuration to the firewall based upon choices made in the previous panels. This button is dimmed until all necessary steps have been completed in the Wizard.
- **Cancel**—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

Local Username Password Database

VPN Wizard>Local Username Password Database

Use the **VPN Wizard>Local Username Password Database** to define local usernames and passwords for authentication with PPTP clients.

Field Descriptions

The **VPN Wizard>Local Username Password Database** panel displays the following fields:

- **Username**—Enter a local username to be used for authentication with PPTP clients.
- **Password**—Enter the password associated with the username.
- **Re-enter Password**—Retype the password associated with the username.
- **Add**—Click to add the username to the firewall local username database.
- **Username** and **Password** table—Displays the configured usernames and passwords available on the firewall.
- **Back**—Returns you to the previous panel.
- **Next**—Advances you to the next panel.
- **Finish**—Submits your configuration to the firewall based upon choices made in the previous panels. This button is dimmed until all necessary steps have been completed in the Wizard.
- **Cancel**—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

MPPE Encryption

VPN Wizard>MPPE Encryption

The **VPN Wizard>MPPE Encryption** panel lets you determine if Microsoft Point-To-Point Encryption (MPPE) is not used, optional or required.

PIX Firewall PPTP VPN supports standard PPP CCP negotiations with Microsoft Point-To-Point Encryption (MPPE) extensions using RSA/RC4 algorithm. MPPE currently supports 40-bit and 128-bit session keys. MPPE generates an initial key during user authentication and refreshes the key regularly. To use a 128-bit key, your firewall must be licensed for 3DES encryption.

To change other MPPE settings, use the **Remote Access>L2TP/PPTP>Add** category on the **VPN** tab.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

Important Notes

- The length of the session key can be either 40 or 128 bits, depending on whether you are using a US Domestic or International version of the Windows client. You can specify **auto** in the **Remote Access>L2TP/PPTP>Add** category on the **VPN** tab to accommodate both.

Field Descriptions

The **Enable Extended Client Authentication** panel displays the following fields:

- **Do not use MPPE**—Click to not require the use of MPPE.
- **MPPE is optional**—Click to make the use of MPPE optional.
- **MPPE is required**—Click to require the use of MPPE.
- **Back**—Returns you to the previous panel.
- **Next**—Advances you to the next panel.
- **Finish**—Submits your configuration to the firewall based upon choices made in the previous panels. This button is dimmed until all necessary steps have been completed in the Wizard.
- **Cancel**—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous

panel.

Copyright © 2001-2004, Cisco Systems, Inc.

PPTP/L2TP Authentication

VPN Wizard>PPTP/L2TP Authentication

PIX Firewall provides support for Microsoft Point-to-Point Tunneling Protocol (PPTP), which is an alternative to IPSec handling for VPN clients. While PPTP is less secure than IPSec, PPTP is easier to implement and maintain.

The **vpdn** command implements the PPTP feature for inbound connections between the firewall and a Windows client. PPTP is a layer two tunneling protocol which lets a remote client use a public IP network to communicate securely with servers at a private corporate network. PPTP tunnels the IP protocol. RFC 2637 describes the PPTP protocol.

Support is provided for only inbound PPTP and only one firewall interface can have the protocol enabled.

Supported authentication protocols include: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) using external authentication, authorization, and accounting (AAA) (RADIUS or TACACS+) servers or the firewall local username and password database. Through the PPP IP Control Protocol (IPCP) protocol negotiation, PIX Firewall assigns a dynamic internal IP address to the PPTP client allocated from a locally defined IP address pool.

PIX Firewall PPTP VPN supports standard PPP CCP negotiations with Microsoft Point-To-Point Encryption (MPPE) extensions using RSA/RC4 algorithm. MPPE currently supports 40-bit and 128-bit session keys. MPPE generates an initial key during user authentication and refreshes the key regularly.

When you specify MPPE, use the MS-CHAP PPP authentication protocol. If you are using an external AAA server, the protocol should be RADIUS and the external RADIUS server should be able to return the Microsoft MSCHAP_MPPE_KEY attribute to the firewall in the RADIUS Authentication Accept packet. See RFC 2548, "Microsoft Vendor Specific RADIUS Attributes," for more information on the MSCHAP_MPPE_KEY attribute.

Cisco Secure ACS 2.5 and later releases support the MS-CHAP/MPPE encryption.

PIX Firewall PPTP VPN has been tested with the following Microsoft Windows products: Windows 95 with DUN1.3, Windows 98, Windows NT 4.0 with SP6, and Windows 2000.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

Important Notes

- If you configure PIX Firewall for 128-bit encryption and if a Windows 95 or Windows 98 client does not support 128-bit or greater encryption, then the connection to the firewall is refused. When this occurs, the Windows client moves the dial-up connection menu down to the screen corner while the PPP negotiation is in progress. This gives the appearance that the connection is accepted when it is not. When the PPP negotiation completes, the tunnel terminates and PIX Firewall ends the connection. The Windows client eventually times out and disconnects.

Field Descriptions

The **VPN Wizard>PPTP Authentication** panel displays the following fields:

- **PAP**—Select this check box to enable Password Authentication Protocol (PAP) on your firewall.
- **CHAP**—Select this check box to enable Challenge Handshake Authentication Protocol (CHAP) on your firewall.
- **MSCHAP (required for use of MPPE)**—Select this check box to enable Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) on your firewall. This is available only if you select PPTP authentication.
- **New**—Click to open the **AAA Server Group** panel where you can define the location of the AAA server, the group name and the protocol used for AAA.
- **Authenticate using VPDN local username/password database**—Click to use the local usernames and passwords on your firewall for PPTP.
- **Authenticate using AAA server group**—Click to use a AAA server to authenticate users on your firewall for PPTP, and to optionally specify an accounting server.
    - **Authentication**—Choose the AAA server group from the list to authenticate users.
    - **Accounting**—Choose the AAA server group from the list to log accounting information.
- **New**—Click to open the **AAA Server Group** panel where you can define the location of the AAA server, the group name and the protocol used for AAA.
- **Back**—Returns you to the previous panel.
- **Next**—Advances you to the next panel.
- **Finish**—Submits your configuration to the firewall based upon choices made in the previous panels. This button is dimmed until all necessary steps have been completed in the Wizard.
- **Cancel**—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

Remote Access Client

VPN Wizard>Remote Access Client

Use the **Remote Access Client** panel to identify the type of remote access client that will use the current VPN tunnel to connect to your local PIX Firewall.

The following sections are included in this Help topic:

- Cisco VPN Client, Release 3.x or Higher, or other Easy VPN Remote product
- Cisco VPN 3000 Client, Release 2.5/2.6
- Microsoft Windows client using PPTP
- Microsoft Windows client using L2TP

Cisco VPN Client, Release 3.x or Higher, or other Easy VPN Remote product

Click to support remote access clients using Cisco VPN Client v3.x (Cisco Unified VPN Client Framework) software, or to support a connection to another Cisco Easy VPN Server.

Cisco VPN 3000 Client, v2.5/2.6

Click to support remote access clients using Cisco VPN 3000 Client, Release 2.5/2.6 software.

Microsoft Windows Client using PPTP

Click to support remote access clients Microsoft Windows client using Point-to-Point Tunneling Protocol (PPTP).

Microsoft Windows Client using L2TP

Click to support remote access clients Microsoft Windows client using Layer Two Tunneling Protocol (L2TP).

Back—Returns you to the previous panel.

Next—Advances you to the next panel.

Finish—Submits your configuration to the firewall based upon choices made in the previous panels. This button is dimmed until all necessary steps have been completed in the Wizard.

Cancel—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

Address Pool

VPN Wizard>Remote Access Client>Address Pool

The **Address Pool** panel lets you create a pool of local addresses that can be used for assigning dynamic addresses to remote VPN clients (Mode Config).

The following sections are included in this Help topic:

- Name
- Range Start Address
- Range End Address

Pool Name

Enter a descriptive identifier for the address pool.

Range Start Address

Enter the starting IP address in the address pool.

Range End Address

Enter the ending IP address in the address pool.

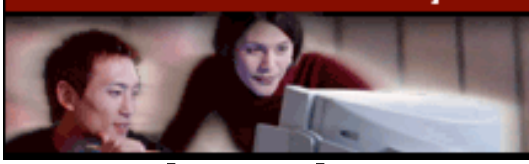
Back—Returns you to the previous panel.

Next—Advances you to the next panel.

Finish—Submits your configuration to the firewall based upon choices made in the previous panels. This button is dimmed until all necessary steps have been completed in the Wizard.

Cancel—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.



Pre-Shared Keys

Configuration>VPN>IKE>Pre-Shared Keys

To view the **Configure Pre-shared Keys** panel, click the **VPN** tab and then select **IKE**>**Pre-shared Keys** from the Categories tree.

The following sections are included in this Help topic:

- Field Descriptions
- Adding a Pre-Shared Key
- Changing a Pre-Shared Key
- Deleting a Pre-Shared Key

The **Configure Pre-shared Keys** panel lets you configure a pre-shared authentication key, called a public key or a Internet Security Association and Key Management Protocol (ISAKMP) key. This panel also lets you associate this key with an IPSec peer or security gateway address or host. Your configuration edits are captured by PDM but are not sent to the firewall unit until you click **Apply**.

When you cannot use Internet Key Exchange (IKE) to establish security associations (SAs) between your firewall and a remote IPSec peer, you can manually configure the pre-shared key used for establishing the Phase 1 SA. This is only practical with a limited number of IPSec peers having known IP addresses (or DNS host names). This method of configuration is most practical for site-to-site VPNs. Whenever a new peer is added to the network, you must configure pre-shared keys for that peer and any PIX Firewall or other VPN headend using pre-shared keys. Also, you cannot use SA lifetimes or perfect forward secrecy (PFS) when using pre-shared keys.

For more information, see VPN>IKE Policies, VPN, More VPN.

Field Descriptions

Pre-Shared Keys displays the following fields:

- **Peer Name/IP**—This identifies the IP address or DNS host name of the remote peer for which a pre-shared key has been configured.
- **Netmask**—This identifies the subnet mask of the remote peer for which a pre-shared key has been configured.
- **XAuth**—This identifies if extended authentication (XAuth) is enabled or disabled for the specified remote peer. Xauth lets you deploy IPSec VPNs using TACACS+ or RADIUS as your user authentication method. This feature provides user authentication by prompting the user for a username and password and verifying

these with information stored in a TACACS+ or RADIUS database.

Note: Xauth is negotiated after IPSec Phase 1 (IKE device authentication phase) and before IPSec Phase 2 (IPSec SA negotiation phase). If Xauth authentication fails, the IPSec SA is not established and the IKE SA is deleted.

- **Config Mode**—This option allows a security gateway (in this case a PIX Firewall) to download an IP address and other network level configuration to a VPN client peer as part of IKE (Phase 1) SA negotiation. Using this exchange, the firewall gives an IP address to the VPN client to be used as an “inner” IP address encapsulated with the IPSec packet. This provides a known IP address for the VPN client, which can be matched against the IPSec rules. To implement this feature, it must also be supported by any routers handling the IPSec traffic.
- **Key**—Displays the first few bytes of the pre-shared authentication key, called a public key or an Internet Security Association and Key Management Protocol (ISAKMP) key.

- **Add**—Opens the Add Pre-shared Key dialog box.
- **Edit**—Opens the Edit Pre-shared Key dialog box.
- **Delete**—Deletes the selected item.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Adding a Pre-shared Key

Follow these steps to define a new pre-shared key configuration:

1. Click **Add**.
2. In the **Add ISAKMP Key** dialog box that appears, enter the information required.
3. Click **OK**.
4. Click **Apply.**

Changing a Pre-Shared Key Configuration

You will need to change an existing pre-shared key configuration when the IP address of the remote peer changes or if you wish to periodically change the public key used to establish a secure tunnel with the remote peer. Follow these steps to change an existing pre-shared key configuration:

1. Select a pre-shared key entry.
2. Click **Edit**.
3. In the **Edit ISAKMP Key** dialog box that appears, change the information as required.
4. Click **OK**.
5. Click **Apply**.

Deleting a Pre-shared Key

1. Select a pre-shared key entry.
2. Click **Delete**.
3. Confirm the operation.
4. Click **Apply**.

Copyright © 2001-2004, Cisco Systems, Inc.

VPN Client Group

VPN Wizard>Remote Access Client>VPN Client Group

Use the **VPN Client Group** panel to group remote access users who are using Cisco VPN Client. The attributes associated with a group will be applied and downloaded to the client(s) that are part of a given group. The group password is a pre-shared key to be used for IKE authentication.

The following sections are included in this Help topic:

- Group Name
- Pre-shared key (Group Password)
- Certificate

Group Name

Use this field to enter the group name that includes any remote access clients using the current VPN tunnel to connect to your local PIX Firewall. Make sure that this group name is configured in the client remote access software to ensure that appropriate group attributes are downloaded.

Pre-shared key (Group Password)

Enable this button if you want remote access clients in this group to use pre-shared keys for authentication when accessing your local PIX Firewall. A pre-shared key is a quick and easy way to set up communication with a limited number of remote peers. To use this method of authentication, exchange the pre-shared key with the remote access user through some secure and convenient method, such as an encrypted e-mail message.

Note: pre-shared keys must be exchanged between each pair of IPSec peers that need to establish secure tunnels. This authentication method is appropriate for a stable network with a limited number of IPSec peers. It may cause scalability problems in a network with a large or increasing number of IPSec peers.

Group Password—Use this field to enter the pre-shared key that will be used by remote access clients belonging to this group for accessing your local PIX Firewall.

Re-enter Password—Use this field to re-enter the pre-shared key that will be used by remote access clients belonging to this group for accessing your local PIX Firewall.

Certificate

Enable this button if you want remote access clients in this group to use certificates for authentication when accessing your local PIX Firewall.

Digital certificates (also known as public key certificates) are an efficient way to manage the security keys used for establishing an IPSec tunnel. A digital certificate contains information that identifies a user or device, such as a name, serial number, company, department or IP address. A digital certificate also contains a copy of the owner's public key.

With digital certificates, each peer is enrolled with a CA and when two peers wish to communicate, they exchange certificates and digitally sign data to authenticate each other. When a new peer is added to the network, it simply enrolls with a CA, and none of the other peers need any additional configuration. Using manual configuration of pre-shared keys, each IPSec peer has to be configured for every peer with which it communicates.

Remote access clients obtain certificate from a certificate authority (CA), which is responsible for managing certificate requests and issuing digital certificates. A CA can be a trusted third-party, such as VeriSign, or a private (in-house) CA that you establish within your organization.

Back—Returns you to the previous panel.

Next—Advances you to the next panel.

Finish—Submits your configuration to the firewall based upon choices made in the previous panels. This button is dimmed until all necessary steps have been completed in the Wizard.

Cancel—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

Address Translation Exemption (Optional)

VPN Wizard>Remote Access Client>Address Translation Exemption (Optional)

Use the **Address Translation Exemption (Optional)** panel to identify local hosts/networks which are to be exempted from address translation. By default, the firewall hides the real IP address of internal networks from outside hosts by dynamic or static Network Address Translation (NAT). The security provided by NAT is essential to minimize the risk of being attacked by untrusted outside hosts, but may be improper for those who have been authenticated and protected by VPN.

For example, using dynamic NAT, an inside host would be translated to the outside using a randomly selected an address from a pool. Remote VPN clients would not be able to connect to these hosts, unless you configure a NAT exemption rule that dictates that traffic between VPN clients and these inside hosts is not to be translated. You can specify which networks will be seen by connecting VPN clients using this exemption rule.

Select the appropriate button on this panel for identifying hosts and networks using an IP address, a host name, or a group. To define a group of hosts or networks, use the **Hosts/Networks** tab.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
  - IP Address
  - Name
  - Group
  - Enable split tunneling
  - Selected

Important Notes

If you do not select any traffic for exemption and leave the **Selected** list empty, all networks on the inside of the firewall are exposed to remote VPN client connections and exempted from NAT.

Field Descriptions

Host/Network Exempted From NAT

The **Host/Network Exempted From NAT** group box contains the **Host/Network** box and the **Selected** list. The content in **Host/Network** can change depending on what option you click.

IP Address

Click to identify hosts or networks by their IP address, using the controls described in this section.

- **Interface**—Use this field to identify the firewall interface connected to the hosts or networks that you want to protect.
- **IP address**—Use this field to enter the IP address in dotted-decimal notation for the hosts or networks that you want to protect. After entering each address, click to add the address to the **Selected** list.
- **Mask**—Use this list to select the subnet mask of the hosts or networks that you want to protect and click to add the address to the **Selected** list.
- **Browse**—Click to display the **Select host/network** panel. Choose the hosts or networks you want to protect from the **Select host/network** panel and click **OK**.

Name

Click to identify hosts by their host names. Enter the fully qualified domain name of each host in the **Name** field and click to add each host to the **Selected** list.

Group

Click to identify hosts or networks by a predefined group name, using the controls described in this section.

- **Interface**—Use this field to identify the firewall interface connected to the hosts or networks that you want to protect.
- **Group**—Use this list to select the predefined group name containing the hosts or networks that you want to protect.

To define a new group of hosts or networks, use the **Hosts/Networks** tab from the PDM main window.

Enable split tunneling

Check if you want your local PIX Firewall to allow traffic from remote access clients destined for the public Internet to be sent unencrypted. Split tunneling causes traffic for protected networks to be sent encrypted, while traffic for unprotected networks is sent unencrypted.

This option is only available if you are using Cisco VPN Client, and is not available if you are using Microsoft Windows PPTP or L2TP client. Once enabled, the firewall will push a list of IP addresses to the remote VPN client after Internet Key Exchange (IKE) authentication. When sending the packet to an IP address included in the list, the remote VPN client will encrypt it and tunnel it to PIX Firewall. Otherwise, the packet is sent unencrypted to the Internet and the packet will not reach PIX Firewall because it is routed by the Internet service provider (ISP) that provides the Internet connection to the remote client.

Selected

This list shows the hosts, networks, or groups of hosts and networks that are selected to be protected by the current VPN tunnel. To add hosts, networks, or groups to this list, select the appropriate button, identify the host, network, or group using the controls on the left side of the panel, and click

. To remove hosts, networks, or groups from this list, select them and click

.

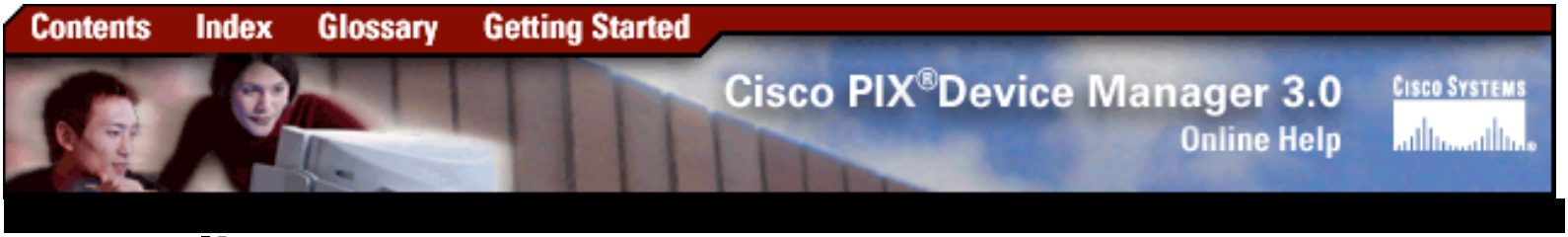
Back—Returns you to the previous panel.

Next—Advances you to the next panel.

Finish—Submits your configuration to the firewall based upon choices made in the previous panels. This button is dimmed until all necessary steps have been completed in the Wizard.

Cancel—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.



IKE Policy

VPN Wizard>Site to Site VPN>IKE Policy

Use the **IKE Policy** panel to specify the encryption and authentication algorithms used by the IKE (Phase 1) VPN Tunnel.

The following sections are included in this Help topic:

- Encryption
- Authentication
- DH Group

Encryption

Use this list to select the encryption option you want to use with the current VPN tunnel. This encryption algorithm is used to encrypt and decrypt user information transmitted over the current VPN tunnel. A symmetric encryption protocol uses the same key to encrypt and decrypt user information.

DES—(Data Encryption Standard) is a symmetric encryption protocol developed in 1975 by the U. S. Department of Defense and standardized by ANSI in 1981 as ANSI X.3.92. DES is widely considered secure enough for most business purposes and is faster than 3-DES.

3-DES—(triple DES) is another symmetric encryption protocol that performs encryption three times with the same 56-bit key, making it more secure than DES. No successful attack has been demonstrated against 3-DES but it is slower than DES.

AES—(Advanced Encryption Standard) is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits.

Note: Not all VPN client software supports AES encryption. Make sure your VPN client software supports this feature before you enable it on PDM.

Authentication

Use this list to select the authentication (has/message digest?) option that you want to use with the current VPN tunnel. A message digest algorithm is used to make sure that no change is made to a message during transmission. This guarantees the integrity of user data and the validity of authentication information.

MD5—(Message Digest 5) produces a 128-bit message digest and may be slightly faster than SHA-1.

SHA-1—(Secure Hash Algorithm 1) produces a 160-bit message digest for which no known attacks or partial attacks have yet been demonstrated.

DH Group

Use this list to select a Diffie Hellman (DH) group to use with the current VPN tunnel. Diffie Hellman is a public key cryptography protocol that allows two parties to establish a shared secret over insecure communications channels. Diffie-Hellman is used within Internet Key Exchange (IKE) to establish session keys.

Group 1 (768-bit)—Use this option when the remote IPSec peer uses Group 1.

Group 2 (1024-bit)—Use this option when the remote IPSec peer uses Group 2.

Group 5 (1536-bit)—Use this option when the remote IPSec peer uses Group 5.

Back—Returns you to the previous panel.

Next—Advances you to the next panel.

Finish—Submits your configuration to the firewall based upon choices made in the previous panels. This button is dimmed until all necessary steps have been completed in the Wizard.

Cancel—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

Remote Site Peer

VPN Wizard>Site to Site VPN>Remote Site Peer

Use the **Remote Site Peer** panel to identify the IP address of the remote IPSec peer that will terminate the VPN tunnel that you are configuring. Also, use this panel to identify which of the following methods of authentication you want to use:

- Pre-shared Keys
- Certificates

The following sections are included in this Help topic:

- Peer IP Address
- Authentication

Peer IP Address

Use this field to identify the IP address of the remote IPSec peer that will terminate the VPN tunnel you are configuring. The remote IPSec peer might be another PIX Firewall, a VPN concentrator, or any other gateway device that supports IPSec. Enter the IP address in dotted-decimal notation (such as 192.168.100.1).

Authentication

Use the controls in this region to identify the type of authentication that is used by the remote site peer.

Pre-shared key—Select this button to use a pre-shared key and enter the pre-shared key into the field provided. A pre-shared key is a quick and easy way to set up communication with a limited number of remote peers. To use this method of authentication, exchange the pre-shared key with the administrator of the remote site through some secure and convenient method, such as an encrypted e-mail message.

Note: pre-shared keys must be exchanged between each pair of IPSec peers that need to establish secure tunnels. This authentication method is appropriate for a stable network with a limited number of IPSec peers. It may cause scalability problems in a network with a large or increasing number of IPSec peers.

Re-enter key—Use this field to re-enter the pre-shared key into the field provided.

Certificate—Select this button to use certificates for authentication between your local PIX Firewall and the remote IPSec peer.

Digital certificates (also known as public key certificates) are an efficient way to manage the security keys used for establishing an IPSec tunnel. A digital certificate contains information that identifies a user or device, such as a name, serial number, company, department or IP address. A digital certificate also contains a copy of the owner's public key.

With digital certificates, each peer is enrolled with a CA and when two peers wish to communicate, they exchange certificates and digitally sign data to authenticate each other. When a new peer is added to the network, it simply enrolls with a CA, and none of the other peers need any additional configuration. Using manual configuration of pre-shared keys, each IPSec peer has to be configured for every peer with which it communicates.

You obtain a certificate from a certificate authority (CA), which is responsible for managing certificate requests and issuing digital certificates. A CA can be a trusted third-party, such as VeriSign, or a private (in-house) CA that you establish within your organization.

FQDN (Fully Qualified Domain Name)—When you use the certificate method of authentication, select this button if your local PIX Firewall is identified by its fully qualified domain name (FQDN), such as cisco.example.com Enter the FQDN in the field provided.

IP Address—When you use the certificate method of authentication, select this button if your local Firewall is identified by its IP address. In this case, you do not have to identify the IP address because it is automatically determined by the VPN Wizard.

Back—Returns you to the previous panel.

Next—Advances you to the next panel.

Finish—Submits your configuration to the firewall based upon choices made in the previous panels. This button is dimmed until all necessary steps have been completed in the Wizard.

Cancel—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

Transform Set

VPN Wizard>Transform Set

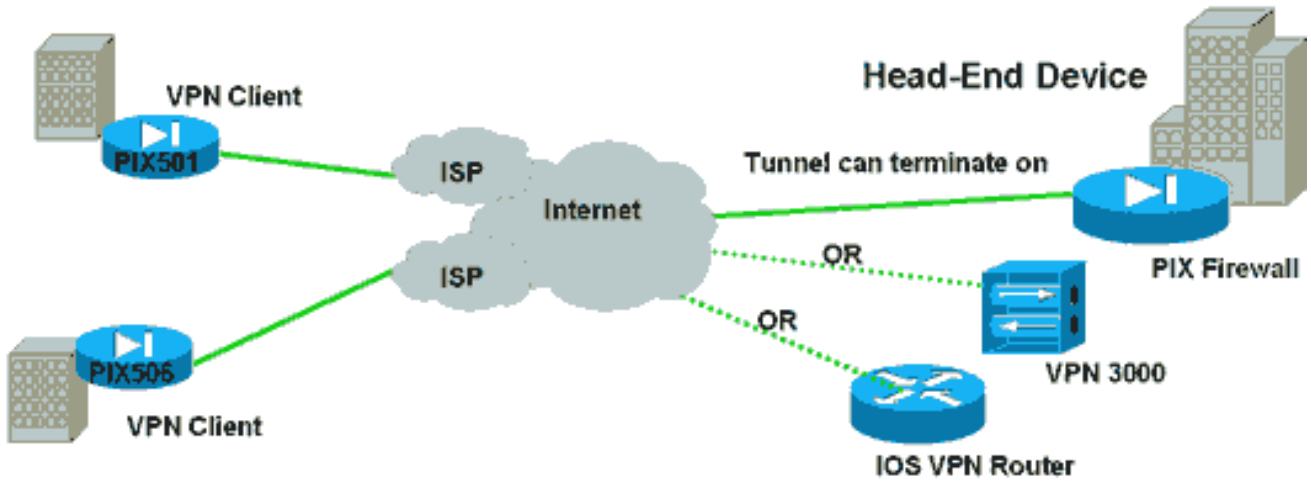
Use the **Transform Set** panel to specify the encryption and authentication algorithms used by the IPSec (Phase 2) VPN Tunnel.

The following sections are included in this Help topic:

- Introduction
- Encryption
- Authentication

Introduction

IPSec provides secure communication over an insecure network, such as the public Internet, by encrypting traffic between two IPSec peers, such as your local PIX Firewall and a remote Firewall or VPN concentrator.



IPSec operates in two phases:

- Phase 1 negotiates the security associations (SAs) used to establish a single, reusable secure tunnel between two IPSec peers.
- Phase 2 uses the Phase 1 tunnel to negotiate SAs and establish secure tunnels for transmitting user data.

To establish a secure tunnel, either in Phase 1 or Phase 2, both peers must agree on the encryption algorithm and other security parameters to use. Once negotiation is completed, each peer establishes an SA that defines the

security parameters to use with the other peer.

The IPSec protocol used in almost all transform sets is the Encapsulating Security Protocol (ESP), which provides both encryption and authentication. If ESP is not supported by the remote IPSec peer, use the option **VPN**>**Tunnel Policy**>**Advanced**>**Select Transform Set** to change the protocol to Authentication Header (AH), which is an older IPSec protocol, providing authentication without encryption.

See **VPN**, More ▸ **VPN**.

Encryption

Use this list to select the encryption option you want to use with the current VPN tunnel. This encryption algorithm is used to encrypt and decrypt user information transmitted over the current VPN tunnel. A symmetric encryption protocol uses the same key to encrypt and decrypt user information.

- **DES**—(Data Encryption Standard) is a symmetric encryption protocol developed in 1975 by the U. S. Department of Defense and standardized by ANSI in 1981 as ANSI X.3.92. DES is widely considered secure enough for most business purposes and is faster than 3DES.
- **3DES**—(Triple DES) is another symmetric encryption protocol that performs encryption three times with the same 56-bit key, making it more secure than DES. No successful attack has been demonstrated against 3DES but it is slower than DES.
- **AES**—(Advanced Encryption Standard) is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits.

Authentication

Use this list to select the authentication option that you want to use with the current VPN tunnel. A message digest algorithm is used to make sure that no change is made to a message during transmission. This guarantees the integrity of user data and the validity of authentication information.

- **MD5**—(Message Digest 5) has a smaller digest and is considered to be slightly faster than SHA-1.
- **SHA-1**—(Secure Hash Algorithm 1) produces a 160-bit message digest for which no known attacks or partial attacks have yet been demonstrated.

For more information about IPSec cryptography standards see More ▸ **VPN.**

Back—Returns you to the previous panel.

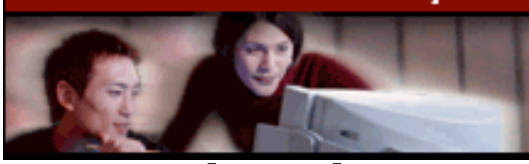
Next—Advances you to the next panel.

Finish—Submits your configuration to the firewall based upon choices made in the previous panels. This button is

dimmed until all necessary steps have been completed in the Wizard.

Cancel—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.



VPN Wizard Start

VPN Wizard>VPN Wizard Start

Use this panel to select the type of Virtual Private Network (VPN) tunnel that you are defining and to identify the interface on which the tunnel will be enabled. A VPN tunnel provides secure communication over an insecure network, such as the public Internet, by encrypting traffic between two IPSec peers, such as your local PIX Firewall and a remote Firewall or VPN concentrator.

To configure a secure tunnel, first decide if you are using your firewall to provide remote access to your local area network (LAN), or to provide connectivity to a LAN in another geographic location. Next, identify the interface to use to connect to the remote IPSec peer. If your firewall has only two interfaces, this will always be the lower security interface, which is named "outside" by default. If your firewall has multiple interfaces, you should plan your VPN configuration before running this wizard and identify the interface to use for each remote IPSec peer with which you need to establish secure connectivity.

To set up your firewall as a remote access client in relation to another PIX Firewall or Cisco VPN Concentrator, select the **Startup Wizard** from the Wizards menu. **More**

The following sections are included in this Help topic:

- Site to Site VPN
- Remote Access VPN
- Select Interface

Site to Site VPN

Click to create a site-to-site VPN configuration. This configuration is used between two IPSec security gateways, which can include firewalls, VPN concentrators, or other devices that support site-to-site IPSec connectivity. When you select this option, a series of panels are displayed that allow you to enter the configuration required for this type of VPN. With a site-to-site VPN, your local PIX Firewall provides secure connectivity between your LAN and a LAN in a different geographic location.

Remote Access VPN

Click to create a remote access VPN configuration. This configuration is used to allow secure remote access for VPN clients, such as mobile users. A remote access VPN lets remote users securely access centralized network resources. When you select this option, the system displays a series of panels that let you enter the configuration required for this type of VPN. With a remote access VPN, your local PIX Firewall provides secure connectivity between individual remote users and the LAN resources protected by your local Firewall.

Select Interface

Use the selection list to select the interface on which the current VPN tunnel will be enabled. The **outside** interface is the lower security interface on your firewall, while the **inside** interface is the higher security interface.

Back—Returns you to the previous panel.

Next—Advances you to the next panel.

Finish—Submits your configuration to the firewall based upon choices made in the previous panels. This button is dimmed until all necessary steps have been completed in the Wizard.

Cancel—Discards any changes without applying them. The Wizard will prompt you with the **Exit Wizard** dialog box when **Cancel** is clicked. Clicking **Exit** will close the Wizard, and clicking **Cancel** again will return you to the Wizard panel. Remember at any time in the Wizard you can click **Back** to return to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.

Authentication

Configuration>VPN>IKE>Certificate>Authentication

The **Certificate Authentication** panel allows authenticate its certification authority (CA) the CA's self-signed certificate, which contains the CA's public key.

To authenticate a peer's certificate(s), a PIX Firewall must obtain the CA certificate containing the CA public key. Because the CA certificate is a self-signed certificate, the key should be authenticated manually by contacting the CA administrator.

The authenticate information is not saved to the firewall configuration. However, the public keys embedded in the received CA certificates are saved in the configuration as part of the RSA public key record (called the "RSA public key chain"). To save the public keys permanently to Flash memory, go to the **VPN>Certificate>Configuration** panel and click **Advanced**. More information about VPN technology is available here.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

Important Notes

- The fingerprint option is not available through PDM. If your CA requires the use of fingerprints, you must use the command-line interface (CLI) to configure them.
- You must complete the **VPN>Certificate>Configuration** before you attempt to authenticate the CA.

Field Descriptions

- **Nickname**—Type the nickname of the CA.
- **Authenticate the CA**—Click to authenticate the CA.

Copyright © 2001-2004, Cisco Systems, Inc.

Advanced Options

Configuration>VPN>IKE>Certificate>Configuration>Advanced Options

Advanced Options lets you save or clear saved certificate and key information from the flash memory, view certificate revocation list (CRL) information, and make a request for the CRL.

When certificates are revoked, they are added to a certificate revocation list (CRL). When you implement authentication using certificates, you can choose to use CRLs or not. Using CRLs lets you easily revoke certificates before they expire, but the CRL is generally only maintained by the CA or its authorized registration authority (RA). If you are using CRLs and the connection to the CA or RA is not available when authentication is requested, the authentication request will fail.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

Important Notes

- Be sure that the firewall clock is set to GMT, month, day, and year before configuring CA. Otherwise, the CA may reject or allow certificates based on an incorrect timestamp. Cisco's PKI protocol uses the clock to make sure that a CRL is not expired. The lifetime of a certificate and CRL is checked in GMT time. If you are using IPSec with certificates, set the firewall clock to GMT to ensure that CRL checking works correctly.
- If your firewall has a CRL which has not yet expired, but you suspect that the CRL's contents are out of date, select the **Request for CRL (Certificate Revocation List)** check box to request that the latest CRL be immediately downloaded to replace the old CRL.

Field Descriptions

The **Advanced Options** dialog box contains the following fields:

- **Save certificates and keys to the PIX flash**—Click to save your certificates and pre-shared keys to the Flash memory.
- **Remove previously saved certificates and keys from the PIX flash**—Click to remove any previously saved certificates from Flash memory.

- **Show CRL Info**—Click to list the CRL information in the **CRL Info** area.
- **CRL Info**—Lists the CRL information on the firewall.
    - A CRL lists all the network's devices' certificates that have been revoked. The firewall will not accept revoked certificates; therefore, any peer with a revoked certificate cannot exchange IPSec traffic with your firewall.
    - The first time your firewall receives a certificate from a peer, it will download a CRL from the CA. your firewall then checks the CRL to make sure the peer's certificate has not been revoked. (If the certificate appears on the CRL, it will not accept the certificate and will not authenticate the peer.)
    - A CRL can be reused with subsequent certificates until the CRL expires. When the CRL does expire, the firewall automatically updates it by downloading a new CRL and replacing the expired CRL with the new CRL.
- **Request for CRL (Certificate Revocation List)**—If your firewall has a CRL which has not yet expired, but you suspect that the CRL's contents are out of date, use the **ca crl request** command to request that the latest CRL be immediately downloaded to replace the old CRL.

Copyright © 2001-2004, Cisco Systems, Inc.

Certificate Configuration

Configuration>VPN>IKE>Certificate>Certificate Configuration

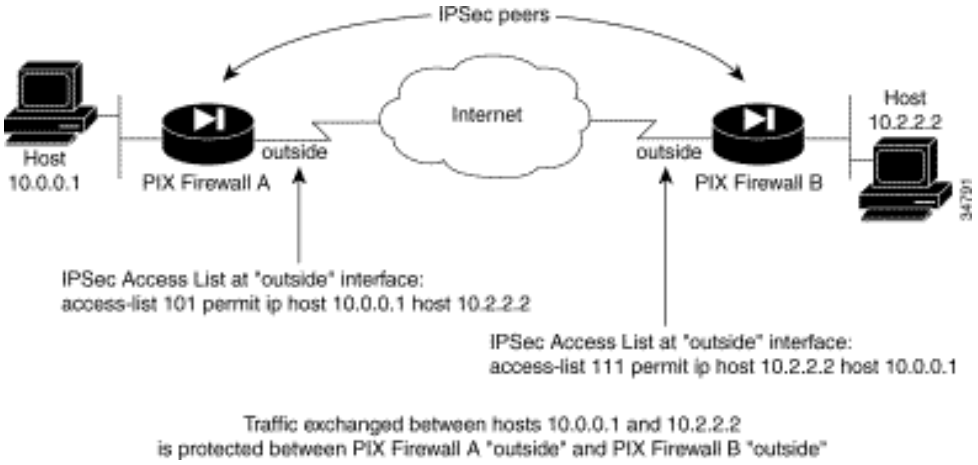
The **Certificate Configuration** panel lets you use digital certificates for Internet Key Exchange (IKE) negotiation with a remote IPSec peer. Your configuration edits are captured by PDM but are not sent to the firewall unit until you click **Apply**.

The following sections are included in this Help topic:

- Introduction to Digital Certificates
- Important Notes
- Field Descriptions
  - CA Parameters
  - Configuration Parameters
    - Key Generation Parameters
    - Certification Authority
  - Advanced
  - Xauth and Mode Config
- Configuring CAs on Firewalls with PDM

Introduction to Digital Certificates

Digital certificates (also known as public key certificates) are an efficient way to manage the security keys used for establishing an IPSec tunnel. A digital certificate contains information that identifies a user or device, such as a name, serial number, company, department or IP address. A digital certificate also contains a copy of the owner's public key.



With digital certificates, each peer is enrolled with a CA and when two peers wish to communicate, they exchange certificates and digitally sign data to authenticate each other. When a new peer is added to the network, it simply enrolls with a CA, and none of the other peers need any additional configuration. Using manual configuration of pre-shared keys, each IPSec peer has to be configured for every peer with which it communicates.

You obtain a certificate from a certification authority (CA), which is responsible for managing certificate requests and issuing digital certificates. A CA can be a trusted third-party, such as VeriSign, or a private (in-house) CA that you establish within your organization.

To use certificates, you must select the **rsa-sig** option when defining your IKE policy. An IKE policy identifies the security parameters required to establish the Phase 1 security associations (SAs). Digital certificates (also known as public key certificates) are an efficient way to manage the security keys used for establishing the IKE SA.

CAs are responsible for managing certificate requests and issuing digital certificates. A digital certificate contains information that identifies a user or device, such as a name, serial number, company, department or IP address. A digital certificate also contains a copy of the owner's public key. A CA can be a trusted third-party, such as VeriSign, or a private (in-house) CA that you establish within your organization.

Additional information on digital certificates and your firewall, see:

More ▸ VPN

VPN>IPSec

▲

Important Notes

- The lifetime of a certificate and the CRL is maintained in GMT, so the firewall clock must be set to GMT to ensure that CRLs work correctly.

  Certificate revocation lists (CRLs) are used to maintain a list of certificates that have been revoked before expiring. Certificates automatically expire after the period of time specified by the CA when it issues the

certificate. However, sometimes it is necessary to revoke a certificate before it expires, such as when an employee leaves an organization or when a server is removed from the network. If your network is configured to use CRLs, a certificate will no longer work once it is added to the CRL.

- It is recommended that you enable **CRL Optional** when using the VeriSign CA. This prevents errors that might otherwise occur when the firewall is not able to poll the CRL from VeriSign. Connection requests to the firewall may fail if the use of CRLs is enforced when using the VeriSign CA.

Field Descriptions

CA Parameters

- **Nickname**—Type the nickname of the CA.
- **CA IP/Hostname**—Type the IP address or DNS host name of the CA server, which is provided to you for this purpose by your CA. The Firewall will issue a certificate request to this CA.
- **LDAP IP/Hostname**—Type the IP address of DNS host name of the Lightweight Directory Access Protocol (LDAP) server where certificates are stored. With an LDAP directory, you can associate a certificate with each user that requires access through the firewall. When a user tries to connect through the firewall, the firewall obtains the user's certificate from the LDAP directory to determine if the connection is permitted.
- **CA Script Location**—Type the URL of the location at the CA to which the firewall should direct its certificate request. The default location and script is /cgi-bin/pkiclient.exe.

Configuration Parameters

- **Retry Interval**—Enter the number of minutes that the firewall should wait before resending a certificate request to the CA if it does not receive a response from the CA to its previous request. The range of values is from 1 to 60 minutes; the default is 1 minute.
- **Retry Count**—Enter the number of times the firewall will resend a certificate request to the CA if it does not receive a response from the CA to its previous request. The range of values is from 1 to 100 minutes. The default is 0, which specifies that there is no limit to the number of retries.
- **CRL Optional**—Select the **CRL Optional** check box if you do not want to enforce the use of CRLs in your network. When this check box is selected, your firewall will accept certificates even if the appropriate CRL is not accessible.

Key Generation Parameters

Key Modulus Size—The modulus determines the length of the prime number used to generate the public key for your firewall. The value you enter will be determined by your CA. A larger value provides a public key that is more resistant to attack, but may require an additional charge from a public CA or may conflict with export restrictions for customers outside the USA In addition, a longer key requires more processing and may slightly reduce system performance in some circumstances. The recommended size for most applications is 768.

Certification Authority

- **CA**—Enable this option if the CA parameters refer to a certification authority (CA).
- **RA**—Enable this option if the CA parameters refer to a registration authority (RA). Some CAs use an RA that acts as a proxy for the CA so that CA functions can continue when the CA is offline.

Advanced

See **VPN>IKE>Certificate>Configuration>Advanced**

Xauth and Mode Config

See **VPN>IKE>Certificate>Peer FQDN/IP**

Configure CA on PIX

Click **Configure CA on PIX** to generate RSA keys and a certificate request to be sent to the specified certification authority. Click **Continue** on each screen that appears to complete the process.

If you are renewing or changing an existing certificate, first delete the existing RSA keys by clicking **Advanced** and selecting **Remove previously saved certificates and keys from the PIX flash**.

Copyright © 2001-2004, Cisco Systems, Inc.

IPSec Rules

Configuration>VPN>IPSec>IPSec Rules

To view the **IPSec Rules** panel, click the **VPN** tab and then select **IPSec>IPSec Rules** from the Categories tree. The **IPSec Rules** panel describes how to define rules for how and when to apply IPSec encryption. Your configuration edits are captured by PDM but are not sent to the firewall unit until you click **Apply**.

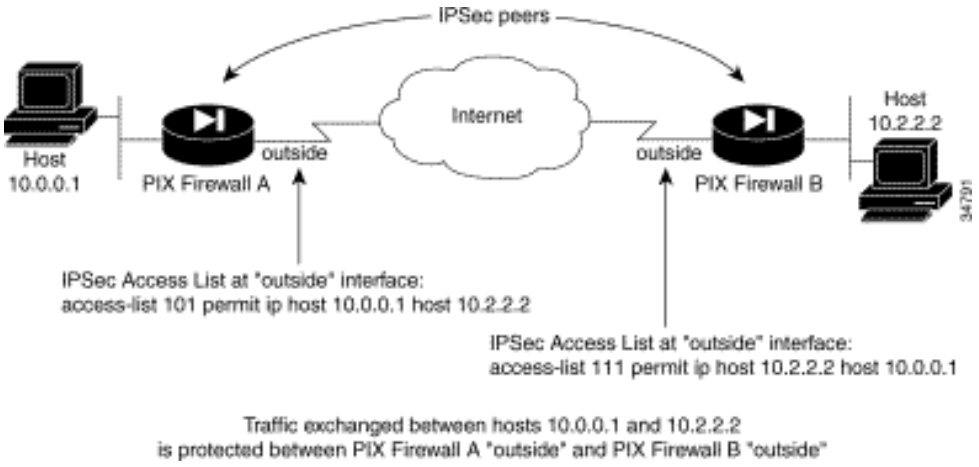
The following sections are included in this Help topic:

- IPSec Overview
- IPSec Rules Table
- Adding a Rule
- Changing a Rule
- Deleting a Rule

IPSec Overview

IPSec provides secure communication over an insecure network, such as the public Internet, by encrypting traffic between two IPSec peers, such as your local PIX Firewall and a remote Firewall or VPN concentrator. IPSec operates in two phases:

- Phase 1 negotiates the security associations (SAs) used to establish a single, reusable secure tunnel between two IPSec peers.
- Phase 2 uses the Phase 1 tunnel to negotiate SAs and establish secure tunnels for transmitting user data.



Traffic exchanged between hosts 10.0.0.1 and 10.2.2.2
is protected between PIX Firewall A "outside" and PIX Firewall B "outside"

To establish a secure tunnel, either in Phase 1 or Phase 2, both peers must agree on the encryption algorithm and other security parameters to use. Once negotiation is completed, each peer establishes an SA that defines the security parameters to use with the other peer.

IPSec rules control the creation of Phase 2 SAs. Phase 1 SAs are controlled by IKE policies. IPSec rules define when to encrypt traffic based on the following criteria:

- IP address or host name of the local host
- Network address of the local subnetwork
- IP address or host name of the remote host
- Network address of the remote subnetwork
- Protocol and service

See **VPN**, **More** ▸ **VPN**.

IPSec Rules Table

The IPSec Rules panel provides a table that lists each rule that you have defined and provides a column for each attribute of the rule. The meaning of each column heading is summarized as follows:

- #—The number of the IPSec rule, which determines the order in which the rule is applied to traffic.
- **Action**—Identifies whether traffic will be selected for encryption or will not be selected for encryption.
- **PIX Side Name/Address**—Traffic from this host name, IP address, or network address will be selected or not selected for encryption, depending on the specified **Action**.
- **Remote Side Name/Address**—Traffic to this host name, IP address, or network address will be selected or not selected for encryption, depending on the specified **Action**.
- **Service**—Traffic related to this TCP or UDP service (well-known port number) or IP protocol will be selected or not selected for encryption, depending on the specified **Action**.

Note: Review **Important Notes about Object Groups** regarding the naming of Network and Service Groups**.**

- **Tunnel Policy**—Lists one or more tunnel policies, used to negotiate the SAs for transmitting traffic that matches the IPSec rule. IPSec tunnel policies are similar to IKE Policies, but are used to negotiate the security association (SA) used in Phase 2 of IPSec. An IKE tunnel policy applies to the SAs used in Phase 1.

  You can define multiple Phase 2 tunnel policies and assign a priority to each. When your firewall is negotiating a Phase 2 SA with a remote peer, it will try to use the parameters in the highest priority tunnel policy. If the remote peer does not support these parameters, your firewall will offer to use the parameters in each lower priority tunnel policy until security parameters are found that are acceptable to both peers.

- **Description**—A text description explaining the effect and behavior of the IPSec rule.

Adding a Rule

Follow these steps to define a new IPSec rule:

1. Click the **Add a New Rule** button on the toolbar or click **Rules>Add** on the menu.
2. In the **Add Rule** dialog box that appears, select the security parameters you wish to use for this policy.
3. Click **OK**.
4. Click **Apply**.

Changing a Rule

Follow these steps to edit an existing IPSec rule:

1. Select an existing IPSec rule from the table.
2. Click the **Edit Rule** button on the toolbar or click **Rules>Edit** on the menu.
3. In the Edit Rule dialog box that appears, select the security parameters you wish to use for this policy.
4. Click **OK**.
5. Click **Apply**.

Deleting a Rule

Follow these steps to delete an existing IPSec rule:

1. Select an existing IPSec rule from the table.
2. Click the **Delete Rule** button on the toolbar or click **Rules>Delete** on the menu.
3. Confirm the operation.
4. Click **Apply**.

Copyright © 2001-2004, Cisco Systems, Inc.

Peer Certificate

Configuration>VPN>IKE>Certificate>Configuration>Advanced>Peer Certificate

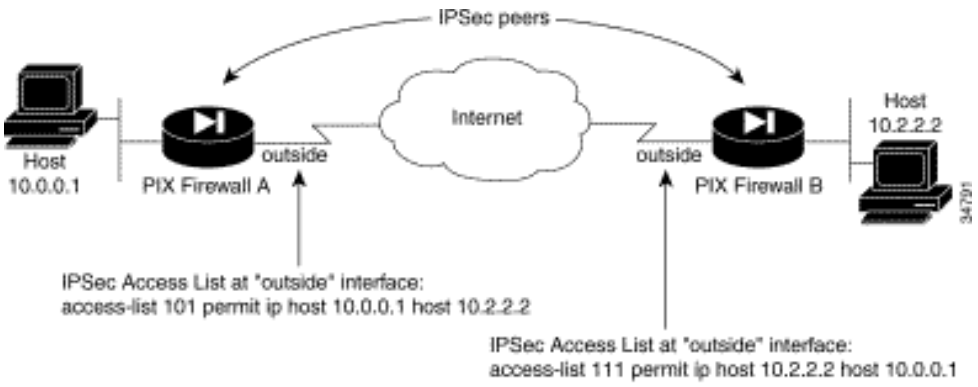
The **Peer Certificate** tab lets you configure peer certificate rules that the firewall uses during authentication to examine the peer identity. As a result, the firewall refuses or filters any unwanted IPSec connections. If there are no matching rules configured, the certificate will be accepted.

The following sections are included in this Help topic:

- Introduction
- Field Descriptions
  - Verify Peer Certificate Table
  - Attribute
  - Operator
  - Value
- Adding/Editing a Verify DN Filter
- Deleting a Verify DN Filter

Introduction

To communicate, IPSec peers must authenticate each other. In **VPN>IKE>Certificate>Configuration** you can configure digital certificates for Internet Key Exchange (IKE) negotiation with a remote IPSec peer as the authentication method.



Traffic exchanged between hosts 10.0.0.1 and 10.2.2.2
is protected between PIX Firewall A "outside" and PIX Firewall B "outside"

For a firewall using certificates as a method of authentication, the firewall can examine the peer certificate identity to

establish an authenticated VPN tunnel or refuse (filter out) any unwanted connections.

VPN>IKE>Certificate>Peer Certificate lets you configure these filters.

See **VPN>Certificate>Configuration and >Advanced, More VPN**

Field Descriptions

Verify Peer Certificate Table

Attribute

The defined attributes are matched in the following order:

- Common Name (cn)
- Department (ou)
- Company Name (o)
- State/Province (st)
- Country (c)
- E-mail Address (ea)
- Unstructured Name
- Unstructured IP

Operator

Operators are defined as follows:

- equals
- does not equal
- contains
- does not contain

Value

The value that the rule is checked against. If there are no matching rules, the certificate will be accepted.

Adding/Editing a Verify DN Filter

Follow these steps to add or edit a Verify DN Filter:

1. Click **Add** in the **Peer Certificate** tab.
2. In the **Add Verify DN Filter** dialog box that appears, select an entry for the following fields:

- **Attribute**—Click the attribute from the drop-down list that you would like to filter.
- **Operator**—Click the operator from the drop-down list for the attribute that you would like to filter.
- **Value**—Enter a value that the rule is checked against to complete your filter.

3. Click **OK**.

Deleting a Verify DN Filter

Follow these steps to delete a Verify DN Filter:

1. Select an attribute filter from the **Verify Peer Certificate Table**.
2. Click **Delete**.
3. Click **OK** to confirm.

Copyright © 2001-2004, Cisco Systems, Inc.

Peer FQDN/IP

Configuration>VPN>IKE>Certificate>Configuration>Advanced>Peer FQDN/IP

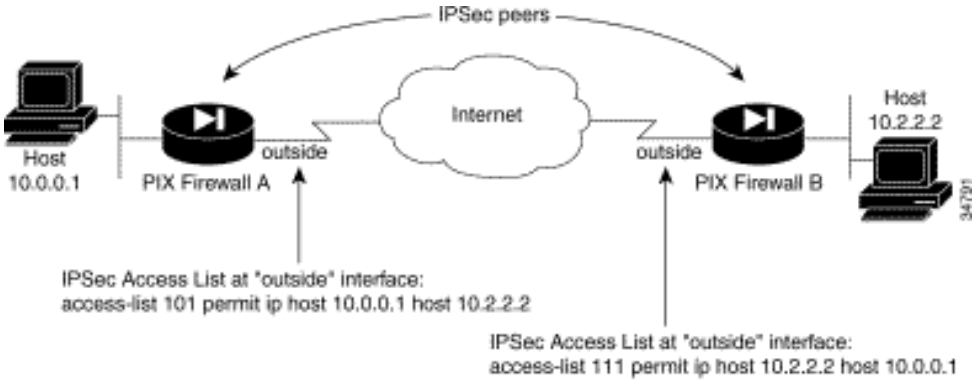
The **Peer FQDN/IP** panel lets you configure multiple IPSec peers and enable or disable Xauth and Mode Config for each.

The following sections are included in this Help topic:

- Introduction
- Field Descriptions
- Adding a Peer FQDN/IP
- Editing a Peer FQDN/IP
- Deleting a Peer FQDN/IP

Introduction

To communicate, IPSec peers must authenticate each other. In the **Configuration>VPN>Configuration** panel, you can configure digital certificates for Internet Key Exchange (IKE) negotiation with a remote IPSec peer as the authentication method.



When you use the certificate method of authentication, your local firewall and its IPSec peer, such as a remote access server, are identified by their fully qualified domain name (FQDN), such as **cisco.example.com** or **example.com** The IP address is resolved by DNS (Domain Name System) for the fully qualified domain name.

You should configure the Xauth feature for the peer depending on the authentication method used within your IKE

policies. If the peer is not a gateway, accept the default setting of the Xauth feature, where the peer is challenged for a username and password. If the peer is a gateway, configure the firewall to make an exception to the authentication method, so that the site-to-site peer is *not* challenged for a username and password.

Field Descriptions

The **Peer FQDN/IP** panel displays the following fields in the Peer FQDN/IP table:

- **Peer FQDN/IP—**Specifies the fully qualified domain name or the IP address (FQDN/IP) of the IPSec VPN peer with which the firewall does not exchange Xauth or Mode Config information.
- **Xauth—**Xauth is configured in the **Configuration>VPN>IKE>Xauth/Mode Config>Edit** panel. If you have both a site-to-site VPN peer and VPN client peers terminating on the same interface, and have the Xauth feature configured, configure the firewall to make an exception to this feature for the site-to-site VPN peer. With this exception, the firewall will not challenge the site-to-site peer for a username and password. The command that you employ to make an exception to the Xauth feature depends on the authentication method you are using within your IKE policies. See **Edit** for more information.
- **Mode Config—**Mode Config is configured in the **Configuration>VPN>IKE>Xauth/Mode Config>Edit** panel. If you have both a site-to-site VPN peer and VPN clients terminating on the same interface, and have the IKE Mode Config (Config Mode) feature configured, you should also configure the firewall to make an exception. With this exception, the firewall does not attempt to download an IP address to the peer for dynamic IP address assignment. See **Edit** for more information.

Adding a Peer FQDN/IP

Follow these steps to add a peer FQDN/IP:

1. Click **Add** and the **Add Peer FQDN/IP** dialog box displays.
2. Enter the domain name or IP address of the VPN peer in the Fully Qualified Domain Name (FQDN) box.
3. Click the **no-xauth** check box to disable the exchange of Xauth (username and password) information with the FQDN/IP peer. By default Xauth is enabled.
4. Click the **no-config-mode** check box to disable the exchange of Mode Config (dynamically assigned IP address) information with the FQDN/IP peer. By default Mode Config is enabled.

Editing a Peer FQDN/IP

Follow these steps to edit a peer FQDN/IP:

1. Click **Edit** and the **Edit Peer FQDN/IP** dialog box displays.
2. Highlight the peer FQDN/IP to edit in the **Peer FQDN/IP** table.
3. Click the **no-xauth** check box to disable the exchange of Xauth (username and password) information with

the FQDN/IP peer. Or deselect the check box to enable it.

4. Click the **no-config-mode** check box to disable the exchange of Mode Config (dynamically assigned IP address) information with the FQDN/IP peer. Or deselect the check box to enable it.
5. Click **OK** to accept the changes or click **Cancel** to cancel them.

Deleting a Peer FQDN/IP

Follow these steps to delete a peer FQDN/IP:

1. Highlight the peer FQDN/IP to delete in the **Peer FQDN/IP** table.
2. Click **Delete** and a caution message displays.
3. Click **OK** to delete the peer or click **Cancel** to cancel the procedure.

Copyright © 2001-2004, Cisco Systems, Inc.

Edit Setup

VPN>IKE>XAuth/Mode Config>Edit Setup

The **Edit Setup** dialog box appears when you select an entry on the **XAuth/Mode Config** panel and click **Edit**. To view the **XAuth/Mode Config** panel, select **XAuth/Mode Config** in the Categories tree of the VPN tab. After making any necessary changes, click **OK** to apply the changes to the currently selected entry.

The following sections are included in this Help topic:

- Server Group
- Server is token based
- Mode Config

Server Group

- Use this list to select the type of Xauth server to use.
- Select **TACACS+** to use a Terminal Access Controller Access Control System Plus (TACACS+) server.
- Select **RADIUS** to use a Remote Authentication Dial-In User Service (RADIUS) server.
- Select **LOCAL** to use the local database.

Server is Token Based

Enable this option if the AAA server uses a compatible token-card system, such as the one from Security Dynamics. This option is disabled when the **Server Group** box is set to **LOCAL**.

Mode Config

Choose an option from this list to determine whether the firewall or the remote access client initiates the configuration mode session.

- **Initiate**—This indicates that the firewall initiates the config mode with the client and then waits for the client to respond before it sends information to the client.
- **Respond**—This indicates that the client initiates the configuration mode with the firewall. The firewall then responds to the remote access client with the IP address it allocates for that client.

Copyright © 2001-2004, Cisco Systems, Inc.

Enrollment

Configuration>VPN>IKE>Certificate>Enrollment

To view the **Certificate Enrollment** panel, click the **VPN** tab and then click **IKE>Certificate>Enrollment** in the Categories tree. The Certificate Enrollment panel generates a request for a digital certificate from a certification authority (CA).

Note: Before you can use the **Certificate Enrollment** panel, you must first complete the **Certificate Configuration** panel. Also, make sure that your firewall has a registered host name and domain name before you begin this process.

Your configuration edits are captured by PDM but are not sent to the firewall unit until you click **Apply**.

To use certificates, you must select the **rsa-sig** option when defining your IKE policy. An IKE policy identifies the security parameters required to establish the Phase 1 security associations (SAs). Digital certificates (also known as public key certificates) are an efficient way to manage the security keys used for establishing the IKE SA.

CAs are responsible for managing certificate requests and issuing digital certificates. A digital certificate contains information that identifies a user or device, such as a name, serial number, company, department or IP address. A digital certificate also contains a copy of the owner's public key. A CA can be a trusted third-party, such as VeriSign, or a private (in-house) CA that you establish within your organization.

With digital certificates, each peer is enrolled with a CA and when two peers wish to communicate, they exchange certificates and digitally sign data to authenticate each other. When a new peer is added to the network, it simply enrolls with a CA, and none of the other peers need any additional configuration. Using manual configuration of pre-shared keys, each IPSec peer has to be configured for every peer with which it communicates.

The following sections are included in this Help topic:

- Configure X500 Directory
- Challenge Password
- Return PIX Serial Number in Certificate
- Return PIX IP Address in Certificate
- Certificate Information
- Enroll PIX with the CA

Configure X500 Directory

For certification authority enrollment using X.500, click **Configure X500 Directory** to configure X.500 directory content. X.500 content fields include the following:

- Common Name (cn)
- Department (ou)
- Company Name (o)
- State/Province (st)
- Country (c)
- E-mail Address (e)

Note: Configuring X.500 is optional, but will not become effective until you click **Enroll PIX with the CA**.

Challenge Password

This is a required password that allows the CA administrator to authenticate a request for revoking a certificate. This password is not stored anywhere, so you must remember it.

Return PIX Serial Number in Certificate

Select this check box if you want the firewall serial number to be included in the digital certificate issued by the CA to the firewall.

Return PIX IP Address in Certificate

Select this check box if you want the firewall IP address to be included in the digital certificate issued by the CA to the firewall.

Certificate Information

The **Certificate information** area displays any certificate that is currently configured for the firewall.

Enroll PIX with the CA

Click **Enroll PIX with the CA** to enroll the firewall with the certification authority that is specified on the **Certificate Configuration** panel.

Copyright © 2001-2004, Cisco Systems, Inc.

X500

Configuration>VPN>IKE>Certificate>Enrollment>X500

For certification authority (CA) enrollment using X.500, use the **Configure X500 Directory Content** panel to configure the X.500 directory content fields.

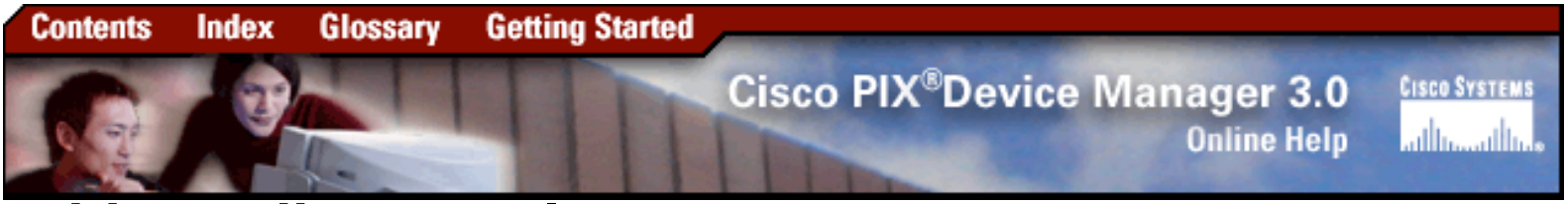
Configuring X.500 is optional, but before you can access the **Configure X500 Directory Content** panel, you must first complete the **Certificate Configuration** and **Certificate Authentication** panels. The settings will not become effective until the user enrolls the PIX Firewall with the CA. PDM will warn the user if there is no entry for the OU (Organizational Unit) when configuring new X.500 values. This is because the PIX Firewall will search for a match between the OU in the certificate and a Cisco VPN Client Group setting on the Cisco Easy VPN Server before it successfully establishes an IPSec VPN Tunnel.

Field Descriptions

- **Common Name (cn)**
- **Department (ou)**
- **Company Name (o)**
- **State/Province (st)**
- **Country (c)**
- **E-mail Address (e)**

OK—Accepts changes and returns to the previous panel.

Copyright © 2001-2004, Cisco Systems, Inc.



Add or Edit IKE Rule

Configuration>VPN>IKE>Policies>Add or Edit IKE Rule

The **Add IKE Rule** and **Edit IKE Rule** dialog boxes appear when you click **Add** or **Edit** on the **Configure IKE Policies** panel. These dialog boxes let you define or change Internet Key Exchange (IKE) policies used for establishing Phase 1 security associations (SAs). After completing either of these windows, click **OK** to add the new IKE policy to the **Configure IKE Policies** panel.

The following sections are included in this Help topic:

- Priority
- Encryption
- Hash
- Authentication
- D-H Group
- Lifetime

Priority

Use this box to enter a numeric priority, so if the remote IPSec peer does not support the parameters selected in your first priority policy, the firewall will try to use the parameters defined in the policy with the next highest priority.

Encryption

Use this list to select the symmetric encryption algorithm used to establish the Phase 1 SA for protecting Phase 2 negotiations. The encryption algorithms supported by the firewall include Data Encryption Standard (DES), which uses a 56-bit key, 3DES (Triple DES), which performs encryption three times using a 56-bit key, and Advanced Encryption Standard (AES). The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits. 3DES is more secure than DES but requires more processing for encryption and decryption. DES is generally considered secure enough for most business purposes.

Hash

Use this list to select the hash algorithm used for authentication and ensuring data integrity. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has been a demonstrated successful (but extremely difficult) attack against MD5. However, the Keyed-Hash Message Authentication Code (HMAC) version used by PIX Firewall prevents this attack.

Authentication

Use this list to select the method of authentication used to establish the identify of each IPSec peer.

When you select the **rsa-sig** (RSA signatures) option you use digital certificates for managing the public keys required for completing IKE Phase 1 negotiation. Digital certificates scale well for large or growing networks with many IPSec peers. Digital certificates also establish non-repudiation for IKE negotiation, which means that you can prove to a third party that IKE negotiation was completed with a specific peer.

When you select the option **pre-share** you use manually configured pre-shared keys for completing IKE (Phase 1) negotiation. A pre-shared key is like a password, which is configured on each pair of IPSec peers that need to establish a secure tunnel. Pre-shared keys do not scale well with a growing network but are easier to set up in a smaller network with a limited and stable number of IPSec peers.

D-H Group

Specifies the Diffie-Hellman group identifier, which is used by the two IPSec peers to derive a shared secret without transmitting it to each other. The default, Group 1 (768-bit Diffie-Hellman) requires less CPU time to execute but is less secure than Group 2 (1024-bit Diffie-Hellman). Diffe-Hellman Group 5 uses a 1536 bit prime number, is the most secure, and is recommended for use with AES.

Lifetime

Specifies the SA lifetime. The default is 86,400 seconds or 24 hours. As a general rule, a shorter lifetime (up to a point) provides more secure IKE negotiations. However, with longer lifetimes, future IPSec security associations can be set up more quickly.

Copyright © 2001-2004, Cisco Systems, Inc.

Add or Edit Pre-Shared Key

Configuration>VPN>IKE>Pre-Shared Keys>Add or Edit Pre-Shared Key

The **Add/Edit Pre-shared Key** dialog box appears when you click **Add** or **Edit** on the **Configure Pre-shared Keys** panel of the **VPN** tab. The **Add Pre-shared Key** dialog box lets you configure a pre-shared authentication key, called a public key or an Internet Security Association and Key Management Protocol (ISAKMP) key. This dialog box also lets you associate the key with an IPSec peer (another PIX Firewall, VPN headend, or host). Your configuration edits are captured by PDM but are not sent to the firewall unit until you click **OK** and then click **Apply**.

When you cannot use IKE to establish security associations (SAs) between your firewall and a remote IPSec peer, you can manually configure a pre-shared key used for establishing the Phase 1 (IKE) SA. This is only practical with a limited number of IPSec peers having known IP addresses (or DNS host names). This method of configuration is most practical for site-to-site VPNs. When using pre-shared keys, whenever a new IPSec peer is added to the network, you must configure pre-shared keys for that peer and any PIX Firewall or other VPN headend using pre-shared keys. Also, the enhanced security provided by SA lifetimes and perfect forward secrecy (PFS) is not available when using pre-shared keys.

The following sections are included in this Help topic:

- Peer Name/IP
- Netmask
- Key
- no-xauth
- no-config-mode

Peer Name/IP

Enter the IP address or DNS host name of the remote peer for which you want to configure a pre-shared key.

Netmask

Enter the subnet mask of the remote peer for which you want to configure a pre-shared key.

Key

Paste in the pre-shared authentication key, called a public key or an Internet Security Association and Key Management Protocol (ISAKMP) key. You may obtain this key from the public certificate of the remote peer or in an

e-mail message from the remote peer.

no-xauth

Select this check box if you do not wish to use extended authentication (XAuth) for the specified remote peer. Xauth lets you deploy IPSec VPNs using TACACS+ or RADIUS as your user authentication method. This feature, which is designed for VPN clients, provides user authentication by prompting the user for username and password and verifies these with information stored in your TACACS+ or RADIUS database. Xauth is negotiated between IPSec Phase 1 (IKE device authentication phase) and IPSec Phase 2 (IPSec SA negotiation phase). If the Xauth fails, the IPSec security association will not be established and the IKE security association will be deleted.

no-config-mode

Select this check box if you do not wish to use the Mode Configuration (Mode Config) feature. This allows a security gateway (in this case a PIX Firewall) to download an IP address (and other network level configuration) to a VPN client peer as part of SA negotiation. Using this exchange, the firewall gives an IP address to the VPN client to be used as an “inner” IP address encapsulated under IPSec. This provides a known IP address for a VPN client, which can be matched against the IPSec policy To implement this feature, it must also be supported by any routers handling the IPSec traffic.

Copyright © 2001-2004, Cisco Systems, Inc.

XAuth/Mode Config

Configuration>VPN>IKE>XAuth/Mode Configuration

To view the **XAuth/Mode Config** panel, select **IKE>XAuth/Mode Config** in the Categories tree of the VPN tab.

Extended Authentication (Xauth) lets you deploy IPSec VPNs using TACACS+, RADIUS, or LOCAL as your user authentication method. This feature, which is designed for VPN clients, provides user authentication by prompting the user for username and password and verifies these with information stored in your TACACS+, RADIUS, or LOCAL database. Xauth is negotiated between IPSec Phase 1 (IKE device authentication phase) and IPSec Phase 2 (IPSec SA negotiation phase). If the Xauth fails, the IPSec security association will not be established and the IKE security association will be deleted.

The Mode Configuration (Mode Config) feature allows a security gateway (in this case a PIX Firewall) to download an IP address (and other network level configuration) to a VPN client peer as part of SA negotiation. Using this exchange, the firewall gives an IP address to the VPN client to be used as an “inner” IP address encapsulated under IPSec. This provides a known IP address for a VPN client, which can be matched against the IPSec policy. To implement this feature, it must also be supported by any routers handling the IPSec traffic

The following sections are included in this Help topic:

- Interface
- Mode Config
- Xauth Server
- Server Token Based?

Interface

The **Interface** column identifies the firewall interface to which the Xauth and Mode Config setup parameters apply.

Mode Config

Identifies if the Mode Config feature is configured to initiate, respond, or initiate and respond.

- **Initiate**—This indicates that the firewall initiates the config mode with the client and then waits for the client to respond before it sends information to the client.
- **Respond**—This indicates that the client initiates the configuration mode with the firewall. The Firewall then responds to the remote access client with the IP address it allocates for that client.
- **Initiate & Respond**—This indicates that the firewall can initiate and respond.

XAuth Server

Identifies if the Xauth server is a Terminal Access Controller Access Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS) server, or the LOCAL database.

Server Token Based?

Enable this option if the AAA server supports a user authentication system based on a hardware token, such as an ID card, that is physically verified by a hardware device on the client side. This option is disabled when using the local database.

An example token is a magnetic striped card. Similar to an ATM (Automated Teller Machine) transaction, the user inserts the card into a reader connected to a PC and enters a PIN number. Cryptographic information in the card is then read and presented over the network to the server to authenticate the user.

Tokens can also be packaged as key fobs, rings, or other small portable devices. Not all card or other hardware token systems are compatible with PIX Firewall. See the *Cisco PIX Firewall and VPN Configuration Guide* for more information.

Copyright © 2001-2004, Cisco Systems, Inc.

Add Rule

Configuration>VPN>IPSec>IPSec Rules>Add Rule

The **Add Rule** dialog box appears when you click **Add** on the **IPSec Rules** panel of the **VPN** tab.

The following sections are included in this Help topic:

- Action
- PIX Side Name/Address (Host/Network)
- Remote Side Name/Address (Host/Network)
- Service/Protocol
- Tunnel Policy Number
- Exempt PIX side host/network from address translation

The **Add Rule** dialog box lets you define an IPSec rule. IPSec rules define when to encrypt traffic based on the following criteria:

- IP address or host name of the local host
- Network address of the local subnetwork
- IP address or host name of the remote host
- Network address of the remote subnetwork
- Protocol or service

See **VPN**, More ▸ **VPN**

Action

Use this list (**select** for encryption or **do not select**) to identify whether traffic will be selected for encryption or will not be selected for encryption.

PIX Side Name/Address (Host/Network)

Use this area to identify the local hosts or subnetworks to which the specified **Action** (**select** for encryption or **do not select**) is applied.

IP Address—Select this option to use an IP address and subnet mask for identifying a host or subnetwork

reachable from the inside (higher security) interface of the firewall. When you select this option, the following controls appear:

- **Interface**—Use this list to choose the firewall interface to which the rule applies.
- **IP address**—Use this box to enter the IP address of the host or the network address of the subnetwork to which the rule applies.
- **Mask**—Use this box to enter the subnet mask of the host or subnetwork to which the rule applies.
- **Browse**—Shows tree list of defined of defined IP addresses.
- **Name**—Select this option to use a host name to identify any host reachable from the inside (higher security) interface of the firewall. Enter the host name in the **Name** box that appears.

Group—Select this option to identify a group of hosts or subnetworks reachable from the inside (higher security) interface of the firewall. When you select this option, the following controls appear:

- **Interface**—Use this list to choose the firewall interface to which the rule applies.
- **Group Name**—Use this list to choose the name of the group of hosts or subnetworks to which the rule applies.

Remote Side Name/Address (Host/Network)

Use this area to identify the remote hosts or subnetworks to which the specified **Action** (**select** for encryption or **do not select**) is applied.

IP Address—Select this option to use an IP address and subnet mask for identifying a host or subnetwork reachable from the outside (lower security) interface of the firewall. When you select this option, the following controls appear:

- **Interface**—Use this list to choose the firewall interface to which the rule applies.
- **IP address**—Use this box to enter the IP address of the host or the network address of the subnetwork to which the rule applies.
- **Mask**—Use this box to enter the subnet mask of the host or subnetwork to which the rule applies.
- **Browse**—Shows tree list of defined of defined IP addresses.

Name—Select this option to use a host name to identify any host reachable from the outside (lower security) interface of the firewall. Enter the host name in the **Name** box that appears.

Group—Select this option to identify a group of hosts or subnetworks reachable from the outside (lower security) interface of the firewall. When you select this option, the following controls appear:

- **Interface**—Use this list to choose the firewall interface to which the rule applies.
- **Group Name**—Use this list to choose the name of the group of hosts or subnetworks to which the rule applies.

Protocol and Service

Use this region to select the TCP or UDP service (well-known port number) or IP protocol to be selected or not selected for encryption.

- **TCP**—When you select this option, two **Source Port** lists are displayed. The left list lets you select an operator (=, not=, >, <, range) to apply to the right list, containing well-known Transport Control Protocol (TCP) port names.
- **UDP**—When you select this option, two **Source Port** lists are displayed. The left list lets you select an operator (=, not=, >, <, range) to apply to the right list, containing well-known User Data Protocol (UDP) port names.
- **ICMP**—When you select this option, the **ICMP Type** list is displayed, which lets you select the Internet Control Message Protocol (ICMP) message type to which you wish to apply the current IPSec rule..
- **IP**—When you select this option, the **IP protocol** list is displayed, which lets you select the Internet Protocol (IP) protocol to which you wish to apply the current IPSec rule.
- **Manage Service Groups**—When you click this button, the **Manage Service Groups** window appears, which lets you define a group of services, ICMP message types, or IP protocols to which you wish to apply the current IPSec rule.

Tunnel Policy

Use this region to identify the tunnel policy to include in the IPSec rule. Tunnel policies, expressed as numbers, are used to negotiate the security associations (SAs) for an IPSec (Phase 2) tunnel, which is used for handling traffic that matches the IPSec rule. You can select an existing policy from the **Policy** list, or you can define a new policy by clicking **New**. When you click **New**, the **Tunnel Policy** dialog box appears.

Exempt PIX side host/network from address translation

When this check box is selected, traffic to which the current IPSec rule applies will be exempted from Network Address Translation (NAT) and Port Address Translation (PAT). To apply NAT or PAT to the traffic matching the current rule, clear this check box.

Copyright © 2001-2004, Cisco Systems, Inc.

Add Service

Configuration>VPN>IPSec>IPSec Rules>Add Rule>Manage Service Groups>
Add Service

The **Add Service** dialog box appears when you click **Add** in the **Manage Service Groups** dialog box.

The following sections are included in this Help topic:

- Service Group Name
- Service
- Range/Port#
- Adding a Service
- Removing a Service

The **Add Service** dialog box lets you select TCP or UDP services or identify port numbers when creating or changing a service group. After making any changes required to this dialog box, click **OK** to apply the changes.

See **VPN**, **More** ▸ **VPN**.

Service Group Name

Use the **Service Group Name** box to enter or change the descriptive name of the service group.

Service

Click the **Service** option if you want to identify services by service name. Then use the **Service** list to select the protocols you wish to include in the service group. To select a protocol, click the protocol name in this list and click **Add**.

Range/Port#

Click the **Range/Port#** option if you want to identify services by port number, or if you wish to include a range of services in the group. Then enter the single port number or range of port numbers in the boxes provided.

Adding a Service

Follow these steps to add a service to a service group:

1. Select the protocol you wish to include in a service group in the **Service** list.
2. Click **Add** to move the selected service to the right column.
3. Click **OK**.

Removing a Service Group

Follow these steps to remove a service from a service group:

1. Select the protocol you wish to include in a service group in the right list.
2. Click **Remove** to move the selected service to the left column.
3. Click **OK**.

Copyright © 2001-2004, Cisco Systems, Inc.

Add or Edit Transform Set

Configuration>VPN>IPSec>Transform Sets>Add/Edit

The **Add Transform Set** and **Edit Transform Set** dialog boxes appear when you click **Add** or **Edit** in the **Transform Sets** dialog box. This panel lets you define or modify a transform set that can be applied to tunnel policies. A transform set specifies the IPSec protocol, encryption algorithm, and hash algorithm to use on traffic matching the IPSec policy. After completing this panel, click **OK** to add the new transform set to the **Transform Sets** panel.

The following sections are included in this Help topic:

- Set Name
- Mode
- ESP Encryption
- ESP Authentication
- AH Authentication

Set Name

Enter a name for a new transform set.

Mode

The **Tunnel** and **Transport** options let you choose the mode in which IPSec functions.

Tunnel Mode—This is the normal way in which IPSec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the public Internet.

Tunnel mode encapsulates the entire IP header and datagram, prefixes an IPSec header, and then creates an outer IP header to tunnel the packet. Tunnel mode is used when the firewall is protecting traffic to and from hosts positioned behind the firewall.

Transport Mode—This method of implementing IPSec is typically done with L2TP to allow authentication of remote Windows 2000 VPN clients.

Transport mode places the IPSec header after the original outer IP header and before the upper layer protocol. Transport mode can be performed only by the sender of the original datagram and therefore requires special software to be installed on the source and destination hosts.

ESP Encryption

Encapsulating Security Protocol (ESP) is the IPSec protocol used in the default transform sets provided with PIX Firewall. ESP is an IP protocol (type 50) that ensures message privacy through encryption, as well as data integrity, authentication, replay detection.

The encryption algorithms supported by the firewall include Data Encryption Standard (DES), which uses a 56-bit key, 3DES (Triple DES), which performs encryption three times using a 56-bit key, and Advanced Encryption Standard (AES). The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits. 3DES is more secure than DES but requires more processing for encryption and decryption. DES is generally considered secure enough for most business purposes.

ESP Authentication

A hash algorithm is used to create a message digest, which is used for ensuring message integrity. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has been a successful (but extremely difficult) attack demonstrated against MD5.

AH Authentication

Authentication Header is an IP protocol (type 51) that can ensure data integrity, authentication, and replay detection. AH does not provide encryption and has been largely superseded by ESP. AH may be required when the remote peer does not support ESP.

A hash algorithm is used to create a message digest, which is used for ensuring message integrity. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has been a successful (but extremely difficult) attack demonstrated against MD5.

Copyright © 2001-2004, Cisco Systems, Inc.

Add or Edit Tunnel Policy

Configuration>VPN>IPSec>Tunnel Policy>Add or Edit Tunnel Policy

The **Add** or **Edit Tunnel Policy** dialog box appears when you click **Add** or **Edit** in the **Tunnel Policy** panel of the **VPN** tab. The **Tunnel Policy** dialog box lets you define a tunnel policy that is used to negotiate an IPSec (Phase 2) security association (SA). Your configuration edits are captured by PDM but are not sent to the firewall unit until you click **OK** and then click **Apply**.

The following sections are included in this Help topic:

- Interface
- Type
- Priority
- Transform Set
- Static Tunnel Policy

Interface

Select the interface on the firewall to which the tunnel policy applies from the **Interface** list.

Type

Select the type of tunnel policy (static or dynamic) from the **Type** list. A tunnel policy is *static* when it applies to one or more remote peers that can be accurately identified by IP address or DNS host name. A tunnel policy is *dynamic* when it applies to an unknown remote peer that seeks to initiate an IPSec connection with the firewall. A static policy is more secure than a dynamic policy. However, a dynamic policy is necessary when a remote IPSec peer has a dynamically assigned IP address or when the firewall is configured to allow connections from unknown remote hosts.

Priority

Enter a number in the Priority box to indicate the relative priority of the current tunnel policy. You can define multiple tunnel policies and assign a priority to each. When your firewall negotiates an IPSec SA with the remote peer, it will propose to use the parameters in the highest priority tunnel policy first. If the remote peer cannot match the parameters proposed in the first tunnel policy, your firewall will use each lower priority tunnel policy until it finds one that matches a policy acceptable to the remote peer.

Transform Set

Identifies the transform set that is included in this policy A transform set specifies the IP Sec protocol, encryption algorithm, and hash algorithm to use on traffic matching the IPSec policy. These options are described as follows:

- The IPSec protocol used in almost all transform sets is the Encapsulating Security Protocol (ESP), which provides both encryption and authentication.
- The encryption algorithms supported by the firewall include Data Encryption Standard (DES), which uses a 56-bit key, 3DES (Triple DES), which performs encryption three times using a 56-bit key, and Advanced Encryption Standard (AES). The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits. 3DES is more secure than DES but requires more processing for encryption and decryption. DES is generally considered secure enough for most business purposes.
- A hash algorithm is used to create a message digest, which is used for ensuring message integrity. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has been a successful (but extremely difficult) attack demonstrated against MD5.

Advanced—Click this button to apply multiple transform sets to a single tunnel policy. When you click **Advanced**, the **Select Transform Set** dialog box appears. Select the transform sets in the **Available** column, click **Add**, and then click **OK**.

Static Tunnel Policy

Peer IP Address—Identifies the host name or IP address of the remote IPSec peer for static tunnel policies.

Security Association Lifetime—Identifies the lifetime of the IPSec security association in terms of the length of time it can be used or the amount of traffic that can flow through the tunnel created with the SA before it expires.

Enable Perfect Forward Secrecy—Identifies if perfect forward secrecy (PFS) is used as part of a specific tunnel policy. This option is only useful if you periodically and systematically change your firewall public security key or certificate. Without PFS, the same security key is used to establish a Phase 1 (IKE) SA and a Phase 2 (IPSec) SA. With PFS, a different security key is used for the SAs used in the different phases.

The vulnerability of a security key to attack is a factor of time and the amount of traffic transmitted. For this reason, PFS lets you assign a shorter lifetime to the security key used for establishing the Phase 2 SA. A Phase 1 SA is only used to negotiate the security parameters for the Phase 2 SA, while the Phase 2 SA is used for the actual transmission of user data. Because the Phase 2 SA is used to transmit far more data than the Phase 1 SA, the security key used to establish the Phase 2 SA should theoretically be assigned a shorter lifetime than the key used for establishing Phase 1 SAs.

Diffie-Hellman Group 1 and Group 2—Diffie-Hellman refers to a type of Public key cryptography using asymmetric encryption based on large prime numbers to establish both Phase 1 and Phase 2 SAs. Group 1 provides a smaller prime number than Group 2 but may be the only version supported by some IPSec peers.

Copyright © 2001-2004, Cisco Systems, Inc.

Advanced

Configuration>VPN>IPSec>Tunnel Policy>Add>Advanced

The **Specify Peers** dialog box appears when you click **Advanced** in the **Tunnel Policy** panel. The **Specify Peers** dialog box lets you specify multiple IPSec peers for an IPSec tunnel policy. Your configuration edits are captured by PDM but are not sent to the firewall unit until you click **OK** and then click **Apply**.

The **Current List** box in the **Specify Peers** dialog box provides a list of the currently configured peers for the policy you are adding or modifying. To change the items on this list, use **Add** or **Remove**.

The following sections are included in this Help topic:

- Adding a Peer
- Removing a Peer

Adding a Peer

To add a peer to the **Current List**, identify the peer in the Specify Additional Peer list and click **Add**. Then click **OK** to close the **Specify Peers** dialog box and to return to the **Tunnel Policy** panel.

Removing a Peer

To remove a peer from the **Current List**, select the peer and click **Remove**. Then click **OK** to close the **Specify Peers** dialog box and to return to the **Tunnel Policy** panel.

Copyright © 2001-2004, Cisco Systems, Inc.

Select Transform Set

Configuration>VPN>IPSec>Tunnel Policy>Advanced>
Select Transform Set

The **Select Transform Set** dialog box appears when you click **Advanced** in the **Tunnel Policy** panel. The **Tunnel Policy** panel appears when you click **Add** in the Tunnel Policy panel of the **VPN** tab or when you select an entry and click **Edit**. The **Select Transform Set** dialog box lets you select a transform set to include in the tunnel policy for a Phase 2 (IPSec) SA.

A transform set specifies the IPSec protocol, encryption algorithm, and hash algorithm to use on traffic matching the IPSec policy. These options are described as follows:

- The IPSec protocol used in almost all transform sets is the Encapsulating Security Protocol (ESP), which provides both encryption and authentication.
- The encryption algorithms supported by the firewall include Data Encryption Standard (DES), which uses a 56-bit key, 3DES (Triple DES), which performs encryption three times using a 56-bit key, and Advanced Encryption Standard (AES). The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits. 3DES is more secure than DES but requires more processing for encryption and decryption. DES is generally considered secure enough for most business purposes.
- A hash algorithm is used to create a message digest, which is used for ensuring message integrity. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has been a successful (but extremely difficult) attack demonstrated against MD5.

You can associate multiple transform sets with a single tunnel policy. After adding or removing a transform set, click **OK** to apply your changes to the current tunnel policy.

The following sections are included in this Help topic:

- Adding a Transform Set
- Removing a Transform Set

Adding a Transform Set

Select the transform set in the **Available** column and click **Add** to move it to the **Selected** column. You can associate multiple transform sets with a single tunnel policy.

To define new transform sets, use the **Transform Sets** panel on the VPN tab.

Removing a Transform Set

Select the transform set in the **Selected** column and click **Remove** to move it to the **Available** column.

Copyright © 2001-2004, Cisco Systems, Inc.

IP Pools

Configuration>VPN>Remote Access>IP Pools

IP Pools lets you create a named pool of local IP addresses. A pool can be used for assigning dynamic addresses to remote VPN client (Mode Config).

The following sections are included in this Help topic:

- Field Descriptions
- Adding an IP Pool
- Editing an IP Pool
- Deleting an IP Pool

Field Descriptions

IP Pools shows existing address pools in a table, which lists the following properties for each pool:

- **Pool Name**—A descriptive identifier for the address pool.
- **Start Address**—The starting IP address in the address pool.
- **End Address**—The ending IP address in the address pool.

- **Add**—Opens the **Add IP Pool** dialog box.
- **Edit**—Opens the **Edit IP Pool** dialog box.
- **Delete**—Deletes the selected item.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Adding an IP Pool

Follow these steps to add a new IP pool:

1. Click **Add**.

2. When the **Add IP Pool** dialog box appears, enter the name and address range for the address pool.
3. Click **OK**.
4. Click **Apply**.

Editing an IP Pool

Follow these steps to edit an existing IP pool:

1. Select an existing address pool from the **Configure Address Pools** table.
2. Click **Edit**.
3. When **Edit IP Pool** dialog box appears, enter the name and address range for the IP pool.
4. Click **OK**.
5. Click **Apply**.

Deleting an IP Pool

Follow these steps to delete an existing IP pool:

1. Select an existing address pool from the **IP Pools** table.
2. Click **Delete**.
3. Click **OK** to confirm the operation.
4. Click **Apply**.

Copyright © 2001-2004, Cisco Systems, Inc.

Cisco VPN Client

Configuration>VPN>Remote Access>Cisco VPN Client

The **Cisco VPN Client** panel lets you create a new Cisco VPN Client v3.x client group, or modify an existing client group.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Adding a VPN Client Group
- Editing a VPN Client Group
- Deleting a VPN Client Group
- Resetting to Last Applied Settings

Important Notes

- PDM supports Cisco VPN Client version 3.x, Cisco VPN 3000 Client version 2.5/2.6, Cisco VPN 3002 Hardware Client, and the firewall as the VPN client. For all clients except the Cisco VPN 3000 Client, the configuration is the same although some parameters may not be used.

Field Descriptions

The **Cisco VPN Client** panel lets you to add, edit, or delete a Cisco VPN Client version 3.x.

- **Group Name**—A descriptive group name to be used for this Cisco VPN Client 3.x client group.
- **Pool**—The IKE pool created in **VPN>Remote Access>IP Pools**. This pool determines the range of local addresses that will be assigned to the VPN clients.
- **Primary DNS**—The IP address of the primary DNS server on your local network that will be passed to the Cisco VPN 3.x client.
- **Primary WINS**—The IP address of the primary WINS server on your local network that will be passed to the Cisco Client VPN 3.x client.
- **Domain**—The local domain name that will be passed to the Cisco VPN Client 3.x client.
- **Add**—Displays the **Add Client Settings** dialog box.
- **Edit**—Displays the **Edit Client Settings** dialog box.
- **Delete**—Deletes the selected client group.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover

standby firewall unit. See Configuration Changes.

- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Adding a VPN Client Group

1. In the **Cisco VPN Client** panel, click **Add**. The **Add Cisco VPN Client Settings** dialog box appears.
2. When finished making your selections, click **OK**.

Editing a VPN Client Group

1. Select a VPN client group from the **VPN Client** table.
2. Click **Edit**. The **Edit Cisco VPN Client Settings** dialog box is appears.
3. When finished making your selections, click **OK**.

Deleting a VPN Client Group

1. Select a VPN client group from the **VPN Client** table.
2. Click **Delete**.

Apply—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Add or Edit Client Group

Configuration>VPN>Remote Access>Cisco VPN Client>Add or Edit Client Group

The **Add or Edit Client Group** panel lets you create a new Cisco VPN Client v3.x client group, or modify an existing client group.

The following sections are included in this Help topic:

- Field Descriptions
- Adding a Cisco VPN Client group
- Editing a Cisco VPN Client group
- Deleting a Cisco VPN Client group

Field Descriptions

The **Add Cisco VPN Client Settings** and **Edit Cisco VPN Client Settings** dialog boxes display the following fields:

- **Group Information**—Determines the names and passwords for the Cisco VPN Client v3.x client group.
  - **Group Name**—Type a descriptive group name to be used for this Cisco VPN Client v3.x client group.
  - **Password**—The group pre-shared key to be used for IKE authentication by the Cisco VPN Client 3.x client group. This must be at least eight characters, and alphanumeric with no special (non-alphanumeric) characters.
  - **Confirm Password**—Reenter the group password.
  - **Select if using Cisco VPN 3000 Client Version 2.5/2.6**—Because it uses Diffie-Hellman Group 2 key exchange, you need to select this check box if you are using the Cisco VPN 3000 Client version 2.5/2.6.
  - **Advanced**—Opens the **Advanced Options** dialog box, where you can configure Secure Unit Authentication (SUA), Individual Unit Authentication (IUA) and backup servers.
- **Pool Information**—Lets you select or deselect the IKE pool created in **VPN>Remote Access>IP Pools**. This pool determines the range of local addresses that will be assigned to the Cisco VPN Clients.
  - **Pool Name**—The name of the address pool specified by the Start and End Address Range and set by **Select Pool**.
  - **Start Address Range**—Starting address associated with the pool name.
  - **End Address Range**—Ending address associated with the pool name.
  - **Select Pool**—Lets you select an address pool from **Add Client Pool** which has been added in **VPN>Remote Access>IP Pools**.
  - **Deselect Pool**—Deselects an address pool selected by Select Pool.

- **General Information**—Determines the settings for the Cisco VPN Client.
  - **Idle Timeout (secs)**—Sets the inactivity timeout for a client in seconds. When the inactivity timeout for all IPSec SAs have expired for a Cisco VPN Client, the tunnel is terminated. The default inactivity timeout is 1800 seconds (30 minutes).
  - **Max. Conn. Time (secs)**—Sets the maximum connection time for a client in seconds. When the maximum connection time is reached for a Cisco VPN Client, the tunnel is terminated. This means the connection between the client and the firewall will have to be reestablished. The default maximum connection time is set to an unlimited amount of time.
  - **Primary DNS** —The IP address of the primary DNS server on your local network that will be passed to the Cisco VPN Client v3.x.
  - **Primary WINS**—The IP address of the primary WINS server on your local network that will be passed to the Cisco VPN Client v3.x.
  - **Secondary DNS**—The IP address of the secondary DNS server on your local network that will be passed to the Cisco VPN Client v3.x.
  - **Secondary WINS**—The IP address of the secondary WINS server on your local network that will be passed to the Cisco VPN Client v3.x.
  - **Domain**—The local domain name that will be passed to the Cisco VPN client v3.x.
  - **Enable PFS**—Enables perfect forward secrecy.

  - **Manage Split DNS**—Lets you create a list of up to 8 domain names. Requests to these domain names will be tunneled if split tunneling is enabled.
    - **Domain**—Enter the name of a new domain name to be added.
    - **List of DNS**—The list of all the domain names added.
    - **Add**—Clicking **Add** adds the domain name entered in the **Domain** box.
    - **Remove**—Removes a domain name from **List of DNS**.
    - **OK**—Accepts changes and returns to the previous panel.
    - **Cancel**—Discards changes and returns to the previous panel.

  - **Manage Split Tunneling**—Lets you specify what traffic will be subject to split tunneling. Split tunneling allows a remote Cisco VPN Client simultaneous encrypted access to the corporate network and clear access to the Internet.
    - **Derive from tunnel template**—If a tunnel template is available you can select it here. For all firewall interfaces on which IKE has been enabled, PDM finds all dynamic cryptos map entries that match an access control list. This access control list can then also be used as a vpngroup split-tunnel, and is automatically entered into this list. **Note:** You must enable IKE on an interface before tunnel templates appear here. See IKE Policies for more information.
    - **Specify network(s) manually**—Lets you enter a network and mask rather than selecting an existing one.
      - **Network**—The IP address of a network.
      - **Mask**—The network mask for the specified network**.**
    - **Network/Mask**—The list of networks/masks to which the remote traffic will be encrypted/ tunneled.
    - **Add**—Adds a network/mask to the network/mask list for split tunneling.
    - **Remove**—Removes (deletes) a network/mask to the Network/Mask list for split tunneling.
    - **Cancel**—Discards changes and returns to the previous panel.
    - **OK**—Accepts changes and returns to the previous panel.

- **Cancel**—Discards changes and returns to the previous panel.
- **OK**—Accepts changes and returns to the previous panel.
- **Help**—Provides more information.

Adding a Cisco VPN Client Group

1. In the **Cisco VPN Client** panel, click **Add**. The **Add Cisco VPN Client Settings** dialog box appears.
2. Specify a group name.
3. Specify a group password. Remember this must be at least eight characters, and alphanumeric with no special (non-alphanumeric) characters.
4. Click **Select Pool** to select an address pool from the list. If one does not exist, return to **VPN>Remote Access>IP Pools** to create one.
5. Specify the primary and, optionally, secondary DNS and WINS IP addresses, and the domain name.
6. Optionally, you can modify the defaults for the Idle Timeout and Maximum Connection time.
7. If you would like to allow this group of connecting clients to access the Internet as well as your internal network, click **Manage Split Tunneling**.
8. When finished making your selections, click **OK**.

Editing a Cisco VPN Client Group

1. Select a Cisco VPN Client group from the **Cisco VPN Client** table.
2. In the **Cisco VPN Client** panel, click **Edit**. The **Edit Cisco VPN Client Settings** dialog box appears.
3. Make your selections as desired.
4. Click **OK**.

Deleting a Cisco VPN Client Group

1. Select a Cisco VPN Client group from the **Cisco VPN Client** table.
2. Click **Delete**.

Copyright © 2001-2004, Cisco Systems, Inc.

Advanced Options

Configuration>VPN>Remote Access>Add Cisco VPN Client Settings> Advanced Options

The **VPN>Remote Access>Add Cisco VPN Client Settings>Advanced Options** dialog box lets you configure authentication options for your firewall acting as a Cisco Easy VPN Remote device, and for individuals using the Cisco VPN client within your network. From here you can configure Secure Unit Authentication (SUA), Individual Unit Authentication (IUA) and backup servers.

The mechanisms supported for authentication are static usernames and passwords using a local database, a TACACS+ or Radius server, or one-time passwords (OTP). Dynamic credentials are obtained from the Cisco Easy VPN Server during the Phase I authentication of IKE.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions

Important Notes

With SUA enabled, the IKE tunnel needs to be manually triggered by selecting the **Enable Secure Unit Authentication (SUA) for the group** check box. The tunnel will not be automatically brought up with traffic, so you must do so manually.

Field Descriptions

- **Unit/User Authentication & Backup Server(s)**
  - **Enable Secure Unit Authentication (SUA) for the group**—Enables SUA for the group.
  - **Individual User Authentication (IUA)**—Individual User Authentication lets you individually authenticate users based on IP address on your inside network. IUA is independent of SUA and all combinations of their configurations are supported.
    - **Enable Individual User Authentication for the group**—Enables IUA for the group.
    - **User Idle Timeout (seconds)**—Select the number of seconds of inactivity before the tunnel is torn down. The default is 180 seconds, or three minutes.
    - **Authentication Server Group**—Select the method VPN clients will use to authenticate from the list.

        - **Enable device pass through for the group**—Select this check box to enable device pass through for the group. If certain devices on the inside interface of the Easy VPN Remote Device are incapable of authentication, such as IP phones, this option lets them bypass authentication when IUA is enabled. This feature must be enabled on the Easy VPN Server.
    - **Backup Server(s)**—If the primary Easy VPN Server is not available, you can specify a list of backup Easy VPN Servers to connect to.
        - **Enable Backup Server Configuration**—Select this check box to enable configuration of a list of backup Easy VPN Servers.
        - **Server IP Address**—Enter the IP address of the backup Easy VPN Server you wish to add.
        - **Add**—Click to add the IP address of the Easy VPN Server to the **Backup Server List**.
        - **Remove**—Select the IP address you wish to remove from the **Backup Server List** and click to remove the selected Easy VPN Server from your **Backup Server List**. If you wish to remove all of the listed Easy VPN Servers from the Backup Server List, select the **Clear backup server(s) list from the client configuration** check box and click **OK**.
        - **Backup Server List**—Lists the locally stored Easy VPN Servers.
        - **Clear backup server(s) list from the client configuration**—Select this check box to clear the local list of backup Easy VPN Servers from the configuration. If this is selected, the PIX Firewall will attempt to download a list of backup servers from the Easy VPN Server.

- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Copyright © 2001-2004, Cisco Systems, Inc.

L2TP/PPTP Client

Configuration>VPN>Remote Access>L2TP/PPTP Client

The **L2TP/PPTP Client** panel lets you configure the parameters for inbound Layer Two Tunneling Protocol (L2TP) or Point-to-Point Tunneling Protocol (PPTP) connections.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Adding an L2TP or PPTP Client Configuration
- Editing an L2TP or PPTP Client Configuration
- Deleting an L2TP or PPTP Client Configuration
- Resetting to Last Applied Settings

Important Notes

- It is necessary to enable virtual private dial-up network (VPDN) on the interface on which the L2TP or PPTP client will terminate for the clients to establish a connection. This is done under **Enable/Disable VPDN**.
- You can specify more than one interface to accept incoming L2TP or PPTP traffic.
- If VPDN is not enabled on any interfaces, neither L2TP or PPTP will work.

Field Descriptions

The **L2TP/PPTP Client** panel lets you configure inbound Layer Two Tunneling Protocol (L2TP) or Point-to-Point Tunneling Protocol (PPTP) connections. It displays a list of current L2TP and PPTP client groups and the properties of that group, such as group name, dial-in protocol, pool name, and authentication type.

- **Add**—Displays the **Add L2TP/PPTP Client Settings** dialog box, where you can configure the L2TP or PPTP parameters.
- **Edit**—Displays the **Edit L2TP/PPTP Client Settings** box. This is active only if an existing group is selected.
- **Delete**—Deletes the selected group.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

The **Enable/Disable VPDN** group box displays a list of each interface and whether virtual private dial-up network (VPDN) is enabled on that interface.

- **Enable**—You can enable VPDN with this button with an interface selected. The **VPDN Enabled** column will list **yes** if VPDN is enabled on the selected interface.
- **Disable**—You can disable VPDN with this button with an interface selected. The **VPDN Enabled** column will list **no** if VPDN is disabled on the selected interface.

Adding an L2TP or PPTP Client Configuration

1. Click **Add**. The **Add L2TP/PPTP Client Settings** dialog box appears.
2. Add or modify the fields as needed.
3. When finished, click **OK**.
4. Select the interface to which incoming L2TP or PPTP clients will establish their connection in the **Enable/Disable VPDN** group box. Usually this will be the **outside** interface.

Editing an L2TP or PPTP Client Configuration

1. Select an existing L2TP or PPTP client group from the **L2TP/PPTP Client** table.
2. Click **Edit**. The **Edit L2TP/PPTP Client Settings** dialog box appears.
3. Add or modify the fields as needed.
4. When finished, click **OK**.
5. Select the interface to which incoming L2TP or PPTP clients will establish their connection in the **Enable/Disable VPDN** group box. Usually this will be the **outside** interface.

Deleting an L2TP or PPTP Client Configuration

1. Select an existing L2TP or PPTP client group from the **L2TP/PPTP Client** table.
2. Click **Delete**.

Resetting to Last Applied Settings

Apply—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

Add/Edit L2TP/PPTP Client Settings

Configuration>VPN>Remote Access>Add/Edit L2TP/PPTP Client Settings

Add L2TP/PPTP Client Settings and **Edit L2TP/PPTP Client Settings** let you configure the parameters for inbound Layer Two Tunneling Protocol (L2TP) or Point-to-Point Tunneling Protocol (PPTP) connections.

The following sections are included in this Help topic:

- Field Descriptions
- Configuring Access for L2TP and PPTP Clients

Field Descriptions

Add Windows Client Settings and **Edit Windows Client Settings** display the following fields:

- **L2TP** and **PPTP**—Click either option to select L2TP or PPTP.
  - **Group Name**—Type a descriptive group name to be used for this Cisco VPN Client 3.x group.
  - **Authentication**—Select either Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) or Microsoft Challenge Handshake Authentication Protocol (MS/CHAP) for client authentication.
  - **Keepalive Timeout**—For L2TP clients, specify the L2TP tunnel keepalive hello timeout value in seconds. The default is 60 seconds if not specified. The value can be between 10 to 300 seconds. For PPTP clients, specify the PPTP keepalive echo timeout value in seconds. PIX Firewall terminates a tunnel if an echo reply is not received within the timeout period you specify.
  - **Enable MPPE Encryption**—If the client is using PPTP, then specify the number of session key bits (40 or 128 or auto) used for Microsoft Point-to-Point Encryption (MPPE) negotiation. To force the client to use MPPE, select the **Required** check box to indicate that MPPE must be negotiated or the connection will be terminated. To use 128-bit encryption your firewall must have a 3DES license.
- **DNS/WINS Info**—Determines the Domain Name System (DNS) and Microsoft Windows Internet Name Service (WINS) information.
  - **Primary DNS**—The IP address of the primary DNS server on your local network that will be passed to the Windows client.
  - **Secondary DNS**—The IP address of the secondary DNS server on your local network that will be passed to the Windows 2000 client.
  - **Primary WINS**—The IP address of the primary WINS server on your local network that will be passed to the Windows client.
  - **Secondary WINS**—The IP address of the secondary WINS server on your local network that will be passed to the Windows 2000 client.
- **Pool Info**—Displays the address pool information to be sent to the Windows clients.

    - **Name**—Displays the name of the selected pool.
    - **Start Address Range**—Displays the start address range of the selected pool.
    - **End Address Range**—Displays the end address range of the selected pool.
    - **Select Pool**—Click to open the Set Client Pool box. When displayed, it lets you select or deselect the IP pool created in **VPN>Remote Access>IP Pools**. This pool determines the range of local addresses that will be assigned to the VPN clients.
- **User Authentication**—Lets you configure local authentication and set up users, or point users to an authentication, authorization, and accounting (AAA) server.
    - **Local**—Lets you add and remove local usernames and passwords used for authentication. Local users can be added or removed from the **VPN>Remote Access>L2TP/PPTP** panel by clicking **Manage Users**.
    - **AAA**—Lets you configure the location and type of AAA server to be used for user authentication.
        - **AAA Server Group**—Select either **TACACS+** or **Radius**.
        - **Account Server**—Enter the IP address of the AAA server.
- **Cancel**—Discards changes and returns to the previous panel.
- **OK**—Accepts changes and returns to the previous panel.
- **Help**—Provides more information.

Configuring Access for L2TP and PPTP Clients

1. Select **L2TP** or **PPTP**.
2. Under **Authentication**, click **PAP**, **CHAP**, and/or **MSCHAP**.
3. For L2TP, you can either leave the default keepalive timeout or enter a new timeout, in seconds. For PPTP, you must enter a keepalive timeout.
4. Optionally, for PPTP, you can specify the strength of encryption for the MPPE and if it is required for a client to access the network.
5. Enter the primary and secondary DNS and WINS server ip addresses. The secondary DNS and WINS information is optional.
6. Click **Select Pools** and choose a pool from the list. If one does not exist, return to **VPN>Remote Access>IP Pools** and create one to use here.
7. Choose **local** or **AAA** authentication.
    - Local users can be added or removed from the **VPN>Remote Access>L2TP/PPTP** panel by clicking **Manage Users**.
    - If you choose **AAA**, select what protocol to use, and enter the IP address of the accounting server.
8. When finished, click **OK**, or to discard your changes, click **Cancel**.

Copyright © 2001-2004, Cisco Systems, Inc.

Easy VPN Remote

Configuration>VPN>Easy VPN Remote

The **Easy VPN Remote** panel lets you connect your firewall to a VPN concentrator or headend as a VPN client.

You can use PDM to configure PIX Firewall as a VPN client when connecting to a VPN headend, such as a Cisco VPN 3000 Concentrator, a Cisco IOS-based router, or PIX Firewall acting as an Easy VPN Remote Server. This functionality, sometimes called a "hardware client," let the firewall act as a VPN client and to establish a VPN tunnel to the VPN headend. Hosts running on the LAN behind the firewall can connect through the VPN headend without individually running any VPN client software.

You must select locally one of the following modes of operation when you enable your firewall VPN client:

- **Client mode**—This option applies Network Address Translation (NAT) to all IP addresses of clients connected to the inside (higher security) interface of the firewall. To use this mode, you must also enable the DHCP server on the inside interface.
- **Network Extension Mode**—This option does not apply NAT to any IP addresses of clients on the inside (higher security) interface of the firewall.

In network extension mode, the IP addresses of clients on the inside interface are received without change at the VPN headend. If these addresses are registered with the Network Information Center (NIC), they may be forwarded to the public Internet without further processing. Otherwise, they may be translated by the VPN headend or forwarded to a private network without translation.

The following sections are included in this Help topic:

- Important Notes
- Field Descriptions
- Configuring an Easy VPN Remote device
- Resetting to Last Applied Settings

Important Notes

- You can configure the DHCP server in **System Properties>DHCP Server**.
- If you disable the Easy VPN client feature, PDM will prompt to either disable the feature without removing all of the Easy VPN Remote related configuration or disable the feature and remove all the configuration.
- The following are not currently supported in this release of Cisco Easy VPN Remote device:
  - DNEM—Dynamic Network Extension Mode is not supported.

- Per-user authentication
- Clustering or load balancing with the Cisco VPN 3000 Servers.
- Backup list push from headend
- WINS relaying
- VPN NAT transparency
- Failover support

- Multiple peers are supported

```
crypto map newmap 1 ipsec-isakmp
crypto map newmap 1 match address 102
crypto map newmap 1 set peer (public IP of PIX1) (public IP of PIX2)
crypto map newmap 1 set transform-set myset
```

Field Descriptions

The Easy VPN Remote panel lets you configure the firewall as a Cisco Easy VPN Remote device.

- **Enable Easy VPN Remote**—Select the **Enable Easy VPN Remote** check box to enable the firewall as a Cisco Easy VPN Remote device. The configurable options are unavailable until this check box is selected.
- **Mode**—You must select one of the following modes of operation when you enable your firewall as an Easy VPN Remote device:
  - **Client Mode**—This option applies Network Address Translation (NAT) to all IP addresses of clients connected to the inside (higher security) interface of the firewall. To use this mode, you must also enable the DHCP server on the inside interface.
  - **Network Extension Mode**—This option does not apply NAT to any IP addresses of clients on the inside (higher security) interface of the firewall.
- **Group Settings**—For authentication, you must either specify a group name and password or use X.509 Certificate. The following boxes apply to **Group Password** only:
  - **Group Name**—Specify the alphanumeric group name of the VPN client as determined by the VPN concentrator or headend.
  - **Group Password**—Specify the group password. This is sometimes referred to as the pre-shared key. Cisco recommends it be at least eight alphanumeric characters with no special (non-alphanumeric) characters, such as @, ! or *.
  - **Confirm Password**—Retype the group password.
- **User Name**—Specify the alphanumeric username of the VPN client as determined by the VPN concentrator or headend. This is optional, and is used when the VPN concentrator or headend is using Xauth.
- **User Password**—Specify the user password. Review the password policy of your organization.
- **Confirm Password**—Retype the user password.
- **Easy VPN Server To Be Added**—Lets you specify the IP address of the remote VPN concentrator or headend.
  - **IP Address**—The IP address of the remote VPN concentrator or headend.
  - **Add**—Click to add the IP address to the **IP Addresses** box.
  - **Delete**—Deletes the selected server IP address from the **IP Addresses** box.
- **Easy VPN Server Addresses**—Displays the configured IP addresses of the remote VPN concentrator or headend. The up and down arrows next to the **IP Addresses Box** let you reorder the servers.
- **Advanced**—Lets you configure MAC Exemption and Tunneled Management features in the **Advanced**

Options dialog box.

- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Configuring Easy VPN Remote

1. Select the **Enable Easy VPN Remote** check box.
2. Select **Client Mode** or **Network Extension Mode**.
3. Select **Group Password** or **X.509 Certificate**.
4. If you select **Group Password**, you must also specify a **Group Name** and **Group Password**. These boxes are enabled for **Group Password** only:
    - Specify a **Group Name**. This must match what the VPN concentrator or headend expects as a group name.
    - Specify a **Group Password**. Remember this must be at least eight characters, and alphanumeric with no special (non-alphanumeric) characters. You must also confirm this password in the **Confirm Password** box. Review the password policy of your organization.
5. Optionally, you can specify a username and password if required by the remote VPN concentrator in the **User Name**, **User Password** and **Confirm Password** boxes.
6. Specify the IP address of the remote VPN concentrator or headend in the **Easy VPN Remote Server To Be Added** box.
7. Add the server by clicking **Add**. You can specify up to ten Easy VPN servers.
8. When finished, click **Apply**.

Apply—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.

Reset—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.

VPN System Options

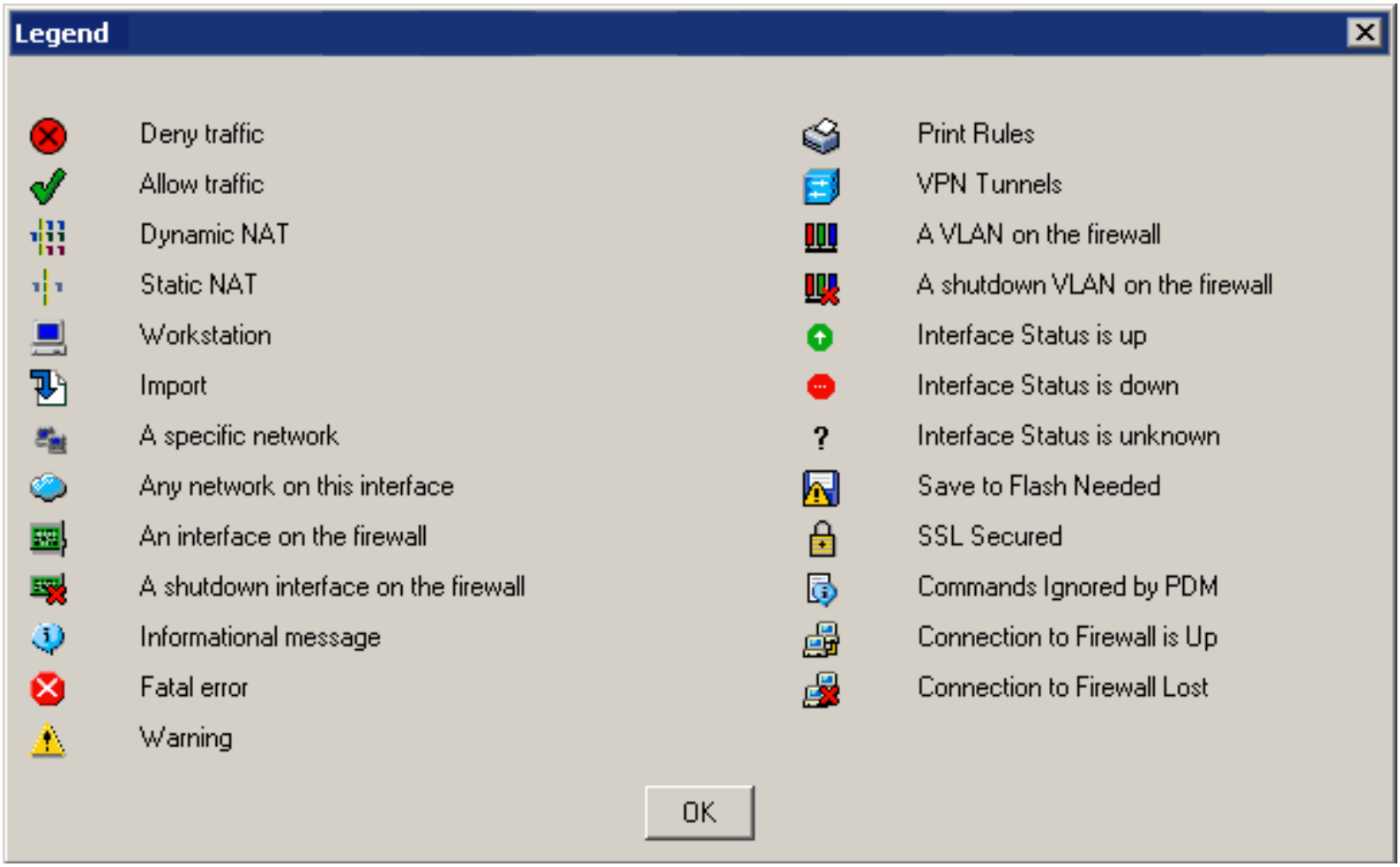
Configuration>VPN>VPN System Options

VPN System Options lets you configure PDM so that the firewall will allow IPSec, Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2TP) traffic through it without the need for access rules. This means it will not be necessary to configure specific access rules to permit this type of traffic. These system options are not enabled by default and must be explicitly enabled.

Field Descriptions

- **Bypass access check for IPSec and L2TP traffic**—This command enables IPSec authenticated/cipher inbound sessions to always be permitted. This permits IPSec traffic to pass through the firewall without a check of the **conduit** or **access-list** command statements. The **sysopt connection permit-ipsec** command is written to the firewall. Because L2TP traffic can only come from IPSec, the **sysopt connection permit-ipsec** command allows L2TP traffic to pass as well.
- **Bypass access check for L2TP traffic only**—Specifying this command in the firewall configuration permits L2TP traffic to pass through the firewall without a check of the **conduit** or **access-list** command statements. The **sysopt connection permit-l2tp** command is written to the firewall.
- **Bypass access check for PPTP traffic**—Specifying this command in the firewall configuration permits PPTP traffic to pass through the firewall without a check of the **conduit** or **access-list** command statements. The **sysopt connection permit-pptp** command is written to the firewall.
- **Apply**—Sends changes made in PDM to the firewall unit and applies them to the running configuration. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts the panel to the information displayed when it was opened or the last time **Refresh** was clicked while open.

Copyright © 2001-2004, Cisco Systems, Inc.


Legend
Deny traffic
Allow traffic
Dynamic NAT
Static NAT
Workstation
Import
A specific network
Any network on this interface
An interface on the firewall
A shutdown interface on the firewall
Informational message
Fatal error
Warning
Print Rules
VPN Tunnels
A VLAN on the firewall
A shutdown VLAN on the firewall
Interface Status is up
Interface Status is down
Interface Status is unknown
Save to Flash Needed
SSL Secured
Commands Ignored by PDM
Connection to Firewall is Up
Connection to Firewall Lost
OK

DNS

Configuration>Properties>Advanced>Fixup>DNS

Domain Name System (DNS) is a service that translates IP domain names to IP addresses.

Fixup DNS enables you to use UDP EDNS packets greater than 512 bytes as specified in IETF RFC 2671.

Field Descriptions

- **Enable Fixup DNS—**Enables DNS (EDNS0) service.
- **Maximum Length—**Specifies packet lengths up to 65535. The default is 512 bytes.
- **Apply**—Sends changes made in PDM to the firewall and applies them to the running configuration. Click Save to write a copy of the running configuration to Flash memory. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby firewall unit. See Configuration Changes.
- **Reset**—Discards changes and reverts to the information displayed before changes were made or the last time you clicked Refresh or Apply. After Reset, use Refresh to make sure that information from the current running configuration is displayed.

Copyright © 2001-2004, Cisco Systems, Inc.