



Cisco PIX Security Appliance Release Notes Version 7.0(2)

July 2005

Contents

This document includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 3](#)
- [New and Changed Information, page 5](#)
- [Important Notes, page 19](#)
- [Caveats, page 21](#)
- [Obtaining Documentation and Submitting a Service Request, page 24](#)

Introduction



Note

The PIX 501, PIX 506E, and PIX 520 security appliances are not supported in software Version 7.0.

The Cisco PIX 500 series security appliance delivers unprecedented levels of defense against threats to the network with deeper web inspection and flow-specific analysis, improved secure connectivity through end-point security posture validation and voice and video over VPN support. It also provides enhanced support for intelligent information networks through improved network integration, resiliency, and scalability.

Version 7.0 introduces significant enhancements to all major functional areas, including: firewalling and inspection services, VPN services, network integration, high availability services, and management/monitoring:

- Advanced Firewall Services



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

- Transparent Firewall (Layer 2 Firewall)
- Security Contexts (Virtual Firewall)
- Outbound ACLs and Time-based ACLs
- Enabling/Disabling of ACL Entries
- Modular Policy Framework
- EtherType Access Control
- Application-Aware Inspection Services
 - Advanced HTTP Inspection Engine
 - Enhanced FTP Inspection Engine
 - ESMTP Inspection Engine
 - Enhanced SunRPC / NIS+ Inspection Engine
 - ICMP Inspection Engine
 - GTP Inspection Engine for Mobile Wireless Environments
 - Enhanced H.323 Inspection Engine
 - Enhanced SIP Inspection Engine
 - Enhanced MGCP Inspection Engine
 - Enhanced RTSP Inspection Engine
 - Enhanced SNMP Inspection Engine
 - Enhanced TCP Security Engine
 - Improved URL Filtering Performance
- Virtual Private Networking (VPN) Services
 - OSPF Dynamic Routing over VPN
 - Enhanced Spoke-to-Spoke VPN Support
 - Enhanced X.509 Certificate Support
 - VPN Client Security Posture Enforcement
 - VPN Client Update
 - VPN Client Blocking by Operating System and Type
 - Movian VPN Client Support
 - Enhanced VPN NAT Transparency
- Network Integration
 - Common Security-Level for Multiple Interfaces
 - IPv6 Inspection, Access Control, and Management
 - Enhanced Multicast Support
 - Optional Address Translation Services
 - Outbound Low Latency Queuing (LLQ) and Policing
- High Availability
 - Active/Active Failover with Asymmetric Routing Support
 - VPN Stateful Failover

- Zero-Downtime Software Upgrades
- General High Availability Enhancements
- Management and Monitoring
 - SSHv2 and SCP, FTP Support
 - Improved SNMP Support
 - Storage of Multiple Configurations in Flash Memory
 - Secure Asset Recovery
 - Scheduled System Reload (Reboot)
 - Enhanced AAA Integration
 - Enhanced ICMP Ping Services
 - Enhanced Command-Line Interface (CLI) Usability
 - Dedicated Out-of-Band Management Interface
 - SMTP E-mail Alerts
 - Enhanced System Health Monitoring and Diagnostic Services
 - Enhanced Debug Services
 - Enhanced Capture Support

Additionally, the Security Appliance software supports ASDM. ASDM is a browser-based, Java applet used to configure and monitor the software on the security appliances. ASDM is loaded from the security appliance, then used to configure, monitor, and manage the device.

System Requirements

The sections that follow list the system requirements for operating a Security Appliance.



Note

The PIX 501, PIX 506E, and PIX 520 security appliances are not supported in software Version 7.0.

Memory Requirements

If you are using a PIX 515/515E running PIX Version 6.2/6.3, you will need to upgrade your memory before performing an upgrade to PIX Version 7.0. PIX Version 7.0 requires at least 64MB of RAM for Restricted (R) licenses and 128MB of RAM for Unrestricted (UR) and Failover (FO) licenses. The following Security Appliance platforms require at least 64 MB of RAM. [Table 1](#) lists Flash memory requirements for Version 7.0.

Table 1 *Flash Memory Requirements*

Security Appliance Model	Flash Memory Required in Version 7.0
PIX 515/515E	16 MB
PIX 525	16 MB
PIX 535	16 MB

For more information on minimum memory requirements, see the “Minimum Memory Requirements” section in the *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*.

Software Requirements

Version 7.0(1) requires the following:

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

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

<http://www.cisco.com/public/sw-center/index.shtml>

2. For information on specific licenses supported on each model of the Security Appliance, go to the following websites: <https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet>
3. If you are upgrading from a previous PIX version, save your configuration and write down your activation key and serial number. See the “[Upgrading to a New Software Release](#)” for new installation requirements.

Maximum Recommended Configuration File Size

For the PIX 525 and PIX 535, the maximum supported configuration file size is 2 MB for Version 7.0(1). For the PIX 515/515E, the maximum supported configuration file size is 1 MB for Version 7.0(1). If you are using ASDM, we recommend no more than a 500 KB configuration file because larger configuration files can interfere with the performance of ASDM on your workstation.

While configuration files up to 2 MB are supported on the PIX 525 and PIX 535, be aware that such large configuration files can reduce system performance. For example, a large configuration file is likely to noticeably slow execution times in the following situations:

- While executing commands such as the **write terminal** and **show running-config** commands
- Failover (the configuration synchronization time)
- During a system reload

Cisco VPN Software Interoperability

Cisco VPN Series	Interoperability Comments
Cisco IOS routers	Version 7.0(1) requires Cisco IOS Release 12.3(T)T or higher running on the router when using IKE Mode Configuration on the Security Appliance.
Cisco VPN 3000 concentrators	Version 7.0(1) requires Cisco VPN 3000 concentrator Version 3.6 or higher for correct VPN interoperability.

Cisco VPN Client Interoperability

Cisco VPN Client	Interoperability Comments
Cisco VPN client v3.x/4x (Unified VPN client framework)	Version 7.0(1) supports the Cisco VPN client Version 3.6 or higher that runs on all Microsoft Windows platforms. It also supports the Cisco VPN client Version 3.6 or higher that runs on Linux, Solaris, and Macintosh platforms.

Cisco Easy VPN Remote Interoperability

Cisco Easy VPN Remote	Interoperability Comments
Cisco PIX Security Appliance Easy VPN Remote v6.3	Version 7.0(1) Cisco Easy VPN server requires the Cisco PIX security appliance Version 6.3 Easy VPN remote that runs on the PIX 501 and PIX 506 platforms.
VPN 3000 Easy VPN remote v3.x/4x	Version 7.0(1) Cisco Easy VPN server requires the Version 3.6 or higher of the Easy VPN remote that runs on the VPN 3002 platform.
Cisco IOS Easy VPN remote Release 12.2(16.4)T	Version 7.0(1) Cisco Easy VPN server interoperates with Cisco IOS 806 Easy VPN remote Release (16.4)T.

Determining the Software Version

Use the **show version** command to verify the software version installed on your Security Appliance.

Upgrading to a New Software Release

If you have a Cisco.com (CDC) login, you can obtain software from the following website:

<http://www.cisco.com/public/sw-center/index.shtml>

New and Changed Information

This section describes new and changed information in this release. This section includes the following topics:

- [New Features, page 5](#)
- [Changes to Existing PIX 6.x Features, page 19](#)

New Features

This section describes the new features in this release. This section includes the following topics:

- [Advanced Firewall Services, page 6](#)

- [Application-Aware Inspection Services, page 8](#)
- [Virtual Private Networking \(VPN\) Services, page 11](#)
- [Network Integration, page 13](#)
- [High Availability, page 15](#)
- [Management and Monitoring, page 16](#)

Advanced Firewall Services

Transparent Firewall (Layer 2 Firewall)

Version 7.0(1) debuts the ability to deploy the security appliance in a secure bridging mode, similar to a Layer 2 device, to provide rich Layer 2 – 7 firewall security services for the protected network. This enables businesses to deploy this security appliance into existing network environments without requiring readdressing of the network. While the security appliance can be completely “invisible” to devices on both sides of a protected network, administrators can manage it via a dedicated IP address (which can be hosted on a separate interface). Administrators have the ability to specify non-IP (EtherType) ACLs, in addition to standard ACLs, for access control over Layer 2 devices and protocols.

To configure transparent firewall on the security appliance, see the “Firewall Mode Overview” and “Transparent Mode Overview” sections in the *Cisco Security Appliance Command Line Configuration Guide*. The following commands are added for the transparent firewall: **arp-inspection**, **firewall**, **mac-address-table**, and **mac-learn**. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Security Contexts (Virtual Firewall)

Version 7.0(1) introduces the ability to create multiple security contexts (virtual firewalls) within a single appliance, with each context having its own set of security policies, logical interfaces, and administrative domain. This provides businesses a convenient way of consolidating multiple firewalls into a single physical appliance, yet retaining the ability to manage each of these virtual instances separately. These capabilities are only available on Version 7.0(1) with either unrestricted (UR) or failover (FO) licenses. This is a licensed feature, with multiple tiers of supported security contexts (2, 5, 10, 20, and 50).

To configure Security Contexts on the security appliance, see the “Enabling Multiple Context Mode” and “Adding and Managing Security Contexts” section in the *Cisco Security Appliance Command Line Configuration Guide*. Some of the commands added for the Security Contexts are: **admin-context**, **context**, **changeto**, and **mode**.



Note

The **context** command enters the context configuration mode which has additional commands.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Outbound ACLs and Time-based ACLs

Version 7.0(1) gives administrators improved flexibility for defining access control policies by adding support for outbound ACLs and time-based ACLs (building on top of our existing inbound ACL support). Using these new capabilities, administrators can now apply access controls as traffic enters an interface or exits an interface. Time-based access control lists provide administrators greater control over resource usage by defining when certain ACL entries are active. New commands allow administrators to define time ranges, and then apply these time ranges to specific ACLs.

The existing versatile **access-list** global configuration command was extended with the **time-range** command to specify a time-based policy defined using the **time-range** global configuration command. Additionally, the **access-group** global configuration command supports the **out** keyword to configure an outbound ACL. For more information, see the “Inbound and Outbound Access List Overview” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enabling/Disabling of ACL Entries

Version 7.0(1) provides a convenient troubleshooting tool that allows administrators to test and fine-tune ACLs, without the need to remove and replace ACL entries.

The **access-list** global configuration command was extended with the **inactive** keyword which lets the user temporarily disable an access entry without removing it from the configuration file.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

EtherType Access Control

The security appliance now includes very powerful support for performing packet filtering and logging based on the EtherType of the packets. When operating as a transparent firewall, this provides tremendous flexibility for permitting or denying non-IP protocols.

The **access-list** global configuration command includes a new **ethertype** keyword to support defining access control rules based on EtherTypes. For more information, see the “Permitting or Denying Network Access” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Modular Policy Framework

Version 7.0(1) introduces a highly flexible and extensible next-generation modular policy framework. It enables the construction of flow-based policies that identify specific flows based on administrator-defined conditions, and then apply a set of services to that flow (such as firewall/inspection policies, VPN policies, QoS policies, and more). This provides significantly improved granular control over traffic flows, and the services performed on them. This new framework also enables inspection engines to have flow-specific settings (which were global in previous releases).

The **class-map**, **policy-map**, and **service-policy** commands were added to support this feature. For more information, see the “Using Modular Policy Framework” chapter in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Application-Aware Inspection Services

Advanced HTTP Inspection Engine

Version 7.0(1) introduces deep analysis of web traffic, enabling granular control over HTTP sessions for improved protection from a wide range of web-based attacks. In addition, this new HTTP inspection engine allows administrative control over instant messaging applications, peer-to-peer file sharing applications, and applications that attempt to tunnel over port 80 or any port used for HTTP transactions. Capabilities provided include RFC compliance enforcement, HTTP command authorization and enforcement, response validation, Multipurpose Internet Mail Extension (MIME) type validation and content control, Uniform Resource Identifier (URI) length enforcement, and more.

A user can define the advanced HTTP Inspection policy using the **http-map** global configuration command and then apply it to the **inspect http** configuration mode command that was extended to support the specification of a map name. For more information, see the “Managing HTTP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enhanced FTP Inspection Engine

Version 7.0(1) includes an enhanced FTP inspection engine, providing new command filtering support. Building upon the FTP security services previously supported, such as protocol anomaly detection, protocol state tracking, NAT/PAT support, and dynamic port opening, Version 7.0 gives administrators granular control over the usage of 9 different FTP commands, enforcing operations that users/groups can perform in FTP sessions. Version 7.0 also introduces FTP server cloaking capabilities, hiding the type and version of the FTP server from those who access it through Version 7.0(1).

Similar to the enhanced inspection engines, the **inspect ftp** command was enhanced to support enforcing a policy defined with the **ftp-map** global configuration command. For more information, see the “Managing FTP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

ESMTP Inspection Engine

Version 7.0(1) builds on top of the existing SMTP (RFC 821) feature with the addition of support for the Enhanced SMTP (ESMTP) protocol, featuring a variety of commands defined in RFC 1869. Supported commands include **AUTH**, **DATA**, **EHLO**, **ETRN**, **HELO**, **HELP**, **MAIL**, **NOOP**, **QUIT**, **RCPT**, **RSET**, **SAML**, **SEND**, **SOML**, and **VRFY** (all other commands are automatically blocked to provide an additional level of security).

The **inspect esmtp** global configuration command provides inspection services for SMTP and ESMTP traffic. For more information, see the “Managing SMTP and Extended SMTP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enhanced SunRPC / NIS+ Inspection Engine

The SunRPC inspection engine is enhanced in Version 7.0 by providing better support for NIS+ and SunRPC services. Specific enhancements include support for all three versions of the lookup service - Portmapper v2 and RPCBind v3 and v4.

Use the **inspect sunrpc** and the **sunrpc-server** global configuration commands to configure the SunRPC / NIS+ inspection Engine.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

ICMP Inspection Engine

Version 7.0(1) introduces an ICMP inspection engine. This engine enables secure usage of ICMP, by providing stateful tracking for ICMP connections, matching echo requests with replies. Additional controls are available for ICMP error messages, which are only permitted for established connections.

Use the **inspect icmp** and the **inspect icmp error** commands to configure the ICMP inspection engine.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

GTP Inspection Engine for Mobile Wireless Environments

Version 7.0(1) introduces a new inspection engine for securing 3G Mobile Wireless environments that provide packet switched data services using the GPRS Tunneling Protocol (GTP). These new advanced GTP inspection services permit mobile service providers secure interaction with roaming partners and provide mobile administrators robust filtering capabilities based on GTP specific parameters such as IMSI prefixes, APN values and more. This is a licensed feature.

The **inspect gtp** command in the policy-map configuration mode and the **gtp-map** global configuration commands are new features introduced in Version 7.0. For more information on GTP and detailed instructions for configuring your GTP inspection policy, see the “Managing GTP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. You may need to install a GTP activation key using the **activation-key exec** command.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enhanced H.323 Inspection Engine

The H.323 inspection engine has been enhanced in Version 7.0 to support the T.38 protocol, an ITU standard that enables the secure transmission of Fax over IP (FoIP). Both real-time and store-and-forward FAX methods are supported. The H.323 inspection engine has been enhanced to support Gatekeeper Routed Call Signaling (GKRCS) in addition to the Direct Call Signaling (DCS) method currently supported. GKRCS support, based on the ITU standard, now allows the security appliance to handle call signaling messages exchanged directly between H.323 Gatekeepers.

The existing **inspect h323** command is enhanced to deliver new functionality. For more information, see the “Managing H.323 Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enhanced SIP Inspection Engine

Version 7.0(1) adds support for Session Initiation Protocol (SIP)-based instant messaging clients, such as Microsoft Windows Messenger. Enhancements include support for features described by RFC 3428 and RFC 3265.

The existing **inspect sip** global configuration command is enhanced to deliver new functionality. For more information, see the “Managing SIP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enhanced MGCP Inspection Engine

Version 7.0(1) includes an enhanced MGCP inspection engine that supports NAT and PAT for the MGCP protocol. This ensures seamless security integration in distributed call processing environments that include MGCP Version 0.1 or 1.0 as the VoIP protocol.

The **inspect mgcp** command in the policy-map configuration mode and the **mgcp-map configuration** command enables the user to configure MGCP inspection policy. For more information, see the “Managing MGCP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enhanced RTSP Inspection Engine

Version 7.0(1) introduces NAT support for the Real Time Streaming Protocol (RTSP), which allows streaming applications such as Cisco IP/TV, Apple Quicktime, and RealNetworks RealPlayer to operate transparently across NAT boundaries.

The existing **inspect rtsp** global configuration command in the policy-map configuration mode is enhanced to deliver the NAT functionality. For more information, see the “Managing RTSP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enhanced SNMP Inspection Engine

Similar to other new inspection engines, the **inspect snmp** command in policy-map configuration mode and the **snmp-map** global configuration command enables the user to configure an SNMP inspection policy. For more information, see the “Managing SNMP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enhanced TCP Security Engine

Version 7.0(1) introduces several new foundational capabilities to assist in detecting protocol and application layer attacks. TCP stream reassembly helps detect attacks that are spread across a series of packets by reassembling packets into a full packet stream and performing analysis of the stream. TCP traffic normalization provides additional techniques to detect attacks including advanced flag and option checking, detection of data tampering in retransmitted packets, TCP packet checksum verification, and more.

You can configure the extensive TCP security policy using the **set connection advanced-options** in **policy-map** global configuration command and **tcp-map** global configuration command.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Improved URL Filtering Performance

Version 7.0(1) significantly increases the number of concurrent URLs that can be processed by improving the communications channel between Version 7.0(1) and Websense servers.

The existing **url-server** global configuration command now supports the **connections** keyword to specify the number of TCP connections in the pool that is used. For more information, see the “Applying Filtering Services” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Virtual Private Networking (VPN) Services

OSPF Dynamic Routing over VPN

Support for OSPF has been extended to support neighbors across an IPsec VPN tunnel. This allows the Security Appliance to support dynamic routing updates across a VPN tunnel to other OSPF peers. OSPF hellos are unicast and encrypted for transport down the tunnel to an identified neighbor in an RFC-compliant manner.

The **ospf network point-to-point non-broadcast** command in interface configuration mode extends comprehensive OSPF dynamic routing services to support neighbors across IPsec VPN tunnels, providing improved network reliability for VPN connected networks. For more information, see the “Configuring OSPF” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enhanced Spoke-to-Spoke VPN Support

Version 7.0(1) improves support for spoke-to-spoke (and client-to-client) VPN communications, by providing the ability for encrypted traffic to enter and leave the same interface. Furthermore, split-tunnel remote access connections can now be terminated on the outside interface for the security appliance, allowing Internet-destined traffic from remote access user VPN tunnels to leave on the same interface as it arrived (after firewall rules have been applied).

The **same-security-traffic** command permits traffic to enter and exit the same interface when used with the **intra-interface** keyword enabling spoke-to-spoke VPN support. For more information, see the “Permitting Intra-Interface Traffic” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enhanced X.509 Certificate Support

Support for X.509 certificates has been significantly improved in the Version 7.0(1), adding support for n-tier certificate chaining (for environments with a multi-level certification authority hierarchy), manual enrollment (for environments with offline certificate authorities), and support for 4096-bit RSA keys. Version 7.0 also includes support for the new certificate authority introduced in Cisco IOS software, a lightweight X.509 certificate authority designed to simplify roll-out of PKI-enabled site-to-site VPN environments.

See the extensive set of **crypto ca** global configuration commands to leverage the new certificate functionality.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

VPN Client Security Posture Enforcement

Version 7.0(1) introduces the ability to perform VPN client security posture checks when a VPN connection is initiated. Capabilities include enforcing usage of authorized host-based security products (such as the Cisco Security Agent) and verifying its version number, policies, and status (enabled/disabled).

To set personal firewall policies that the security appliance pushes to the VPN client during IKE tunnel negotiation, use the **client-firewall** command in group-policy configuration mode.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

VPN Client Update

To configure and change client update parameters, use the **client-update** command in tunnel-group ipsec-attributes configuration mode. For more information, see the “Configuring Group Policies” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

VPN Client Blocking by Operating System and Type

Version 7.0(1) adds the ability to restrict the different types of VPN clients (software client, router, VPN 3002, and PIX) that are allowed to connect based on type of client, operating system version installed, and VPN client software version. When non-compliant users attempt to connect, they can be directed to a group that specifically allows connections from non-compliant users.

To configure rules that limit the remote access client types and versions that can connect via IPSec through the security appliance, use the **client-access-rule** command in group-policy configuration mode. For more information, see the “Configuring Group Policies” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Movian VPN Client Support

Version 7.0(1) introduces support for handheld (PocketPC and Palm) based Movian VPN clients, securely extending access to your network to mobile employees and business partners.

New support for Diffie-Hellman Group 7 (ECC) to negotiate perfect forward secrecy was added to Version 7.0. This option is intended for use with the MovianVPN client, but can be used with other clients that support D-H Group 7 (ECC).

Enhanced VPN NAT Transparency

Version 7.0(1) further extends support for site-to-site and remote-access IPSec-based VPNs to network environments that implement NAT or PAT, such as airports, hotels, wireless hot spots, and broadband environments. Version 7.0 also adds support for Cisco TCP and User Datagram Protocol (UDP) NAT traversal methods as complementary methods to existing support for the IETF UDP wrapper mechanism for safe traversal through NAT/PAT boundaries.

See the **isakmp** global configuration command for additional options when configuring a NAT traversal policy. For more information, see the “Enabling IPSec over NAT-T” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Network Integration

Common Security-Level for Multiple Interfaces

Version 7.0(1) extends the security-level policy structure by enabling multiple interfaces to share a common security level. This allows for simplified policy deployments by allowing interfaces with a common security policy (for example two ports connected into the same DMZ, or multiple zones/departments within a network) to share a common security level. Communication between interfaces with the same security level is governed by the ACL on each interface.

See the **same-security-traffic** command and the **inter-interface** keyword to enable traffic between interfaces configured with the same security level. For more information, see the “Allowing Communication Between Interfaces on the Same Security Level” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

IPv6 Inspection, Access Control, and Management

Version 7.0(1) introduces support for IP version 6 (IPv6) inspection, access control, and management. Full stateful inspection is provided for through-the-box IPv6 traffic in both a dedicated IPv6 mode and in a dual-stack IPv4 / IPv6 mode. In addition, a security appliance can be deployed in a pure IPv6 environment, supporting IPv6 to-the-box management traffic for protocols including SSHv2, Telnet, HTTP, and ICMP. Inspection engines that support IPv6 traffic in Version 7.0 include HTTP, FTP, SMTP, UDP, TCP and ICMP.

Besides the following configuration and exec commands adds support for IPv6: **capture, configure, copy, debug, fragment, http, ip verify, mtu, name, object-group, ping**, various **show** exec commands, **ssh, telnet, tftp-server, who**, and **write**. For more information, see the “Configuring IPv6” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enhanced Multicast Support

PIM Sparse mode was added to allow direct participation in the creation of a multicast tree using PIM-SM. This capability extends existing multicast support for IGMP forwarding and for Class D access control policies and ACLs. PIM-SM provides an alternative to transparent mode operation in multicast environments.

The **pim** commands and the **multicast-routing** command added support to the new functionality in addition to the **show mrib** EXEC command in this feature. For more information, see the “Configuring Multicast Routing” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Optional Address Translation Services

Version 7.0(1) simplifies deployment of the security appliance by eliminating previous requirement for address translation policies to be in place before allowing network traffic to flow. Now, only hosts and networks that require address translation will need to have address translation policies configured. This feature introduces a new configuration option, “nat-control”, which allows NAT to be enabled incrementally.

Version 7.0 introduces the **nat-control** command and preserves the current behavior for customers upgrading from previous versions of the software. For new security appliances or devices which have their configurations cleared, the default will be to not require a NAT policy for traffic to traverse the security appliance. For more information, see the “NAT Control” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Outbound Low Latency Queuing (LLQ) and Policing

Version 7.0(1) supports applications with demanding quality of service (QoS) requirements through support of Low Latency Queuing (LLQ) and Traffic Policing – supporting the ability to have an end-to-end network QoS policy. When enabled, each interface maintains two queues for outbound traffic – one for latency-sensitive traffic (such as voice or market-data), and one for latency-tolerant traffic (such as file transfers). Queue performance can be optimized through a series of configuration parameters.

The QoS functionality is managed using the following commands: **police**, **priority**, **priority-queue**, **queue-limit**, and **tx-ring-limit**. For more information, see the “Applying QoS Policies” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

High Availability

Active/Active Failover with Asymmetric Routing Support

Version 7.0(1) builds upon the award-winning Security Appliance high availability architecture, introducing support for Active/Active failover. This enables two UR licensed or one UR and one FO-AA licensed security appliance to act as a failover pair, both actively passing traffic at the same time, and with Asymmetric Routing Support. The Active/Active failover feature leverages the Security Context feature of this software release – where each security appliance in a failover pair is active for one context and standby for the other, as an inverse symmetric pair. Another key customer challenge that we are addressing in Version 7.0 is Asymmetric Routing Support. This will enable customers with advanced routing topologies, where packets may enter from one ISP and exit via another ISP, to deploy the security appliance to protect those environments (leveraging the Asymmetric Routing Support introduced in Version 7.0).

To support the Active/Active feature, the **failover active** command is extended with the **group** keyword and this software release introduces the failover group configuration mode. In addition, the **asr-group** command in interface configuration mode extends the Active/Active solution to environments with Asymmetric Routing. For more information, see the “Configuring Active/Active Failover” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

VPN Stateful Failover

Version 7.0(1) introduces Stateful Failover for VPN connections, complementing the award-winning firewall failover services. All security association (SA) state information and key material is automatically synchronized between the failover pair members, providing a highly resilient VPN solution.

The VPN Stateful Failover is enabled implicitly when the device operates in single routed mode. In addition to the **show failover EXEC** command, which includes a detailed view of VPN Stateful Failover operations and statistics, the **show isakmp sa**, **show ipsec sa** and **show vpnd-sessiondb** commands have information about the tunnels on both the active and standby unit.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Zero-Downtime Software Upgrades

Version 7.0(1) introduces the ability for customers to perform software upgrades of failover pairs without impacting network uptime or connections flowing through the units. Version 7.0 introduces the ability to do inter-version state sharing between security appliance failover pairs, allowing customers to perform software upgrades to maintenance releases (for example Version 7.0(1) upgrading to 7.0(2)) without impacting traffic flowing through the pair (in active/standby failover environments or Active/Active environments where the pair is not oversubscribed – more that 50% load on each pair member).

General High Availability Enhancements

Version 7.0(1) includes many significant enhancements to the Failover operation and configuration to deliver faster Failover transitions, increased scalability and even further robustness in failover operation.

The release introduces the following new commands: **failover interface-policy**, **failover polltime**, and **failover reload-standby**.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Management and Monitoring

SSHv2 and SCP, FTP Support

Version 7.0(1) adds support for using SSHv2 to remotely manage the security appliance. This new SSHv2 support also improves compatibility with third-party SSH tools. Support for SCP and FTP was added, extending support beyond TFTP, HTTP, and HTTPS for transferring files to/from a security appliance.

The **ssh** global configuration command was extended to support the **version** keyword to provide control on the SSH version which is used to manage the security appliance as well as the **ssh scopy enable** command to enable the use of Secure Copy when transferring files. For more information, see the “Configuring SSH Access” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Improved SNMP Support

Version 7.0(1) adds support for SNMPv2c, providing new services including 64-bit counters (useful for packet counters on Gigabit Ethernet interfaces) and support for bulk MIB data transfers. Additionally, Version 7.0 includes SNMPv2 MIB (RFC 1907), and the IF-MIB (RFCs 1573 and 2233) and the Cisco IPsec Flow Monitoring MIB, giving complete visibility into VPN flow statistics including tunnel uptime, bytes/packets transferred, and more.

The **snmp-server** global configuration command is enhanced to provide additional functionality. For more information, see the “Using SNMP” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Storage of Multiple Configurations in Flash Memory

This release debuts a new flash file system on Version 7.0(1) enabling administrators to store multiple configurations on the security appliance. This provides the ability to do configuration roll-back in the event of a mis-configuration. Commands are introduced to manage files on this new file system.



Note

The new Flash file system is capable of storing not only configuration files but also multiple system images and multiple PIX images when there is adequate flash space available.

The **boot config** global configuration command provides the ability to specify which configuration file should be used at start-up.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Secure Asset Recovery

Version 7.0(1) introduces the ability to prevent the recovery of configuration data, certificates and key material if the **no service password recovery** command is in a security appliance's configuration (while still allowing customers to recover the asset). This feature is useful in environments where physical security may not be ideal, and to prevent nefarious individuals gaining access to sensitive configuration data.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Scheduled System Reload (Reboot)

Administrators now have the ability to schedule a reload on a Version 7.0(1) either at a specific time, or at an offset from the current time, thus making it simpler to schedule network downtimes and notify remote access VPN users of an impending reboot.

The existing **reload EXEC** command has been enhanced to deliver this functionality.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enhanced AAA Integration

Version 7.0(1) native integration with authentication services including Kerberos, NT Domain, and RSA SecurID (without requiring a separate RADIUS/TACACS+ server) for simplified VPN user authentication. This release also introduces the ability to generate TACACS+AAA accounting records for tracking administrative access to security appliances, as well as tracking all configuration changes that are made during an administrative session.

For more information see the “Configuring AAA Servers and the Local Database” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enhanced ICMP Ping Services

Version 7.0(1) introduces several additions to ping (ICMP echo) services, including support for IPv6 addresses. The enhanced **ping** command also supports extended options including data pattern, df-bit, repeat count, datagram size, timeout interval, verbose output, and sweep range of sizes.

The existing **ping EXEC** command has been extended with various keywords and parameters to aid in troubleshooting network connectivity issues. It also provides support for an interactive mode of operation.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enhanced Command-Line Interface (CLI) Usability

Version 7.0(1) enhances the CLI “user experience” by incorporating many popular Cisco IOS software command-line services such as command completion, inline help, and aliasing for improved ease-of-use and common user experience.

See the “Using the Command-Line Interface” section in the *Cisco Security Appliance Command Line Configuration Guide* and the **command-alias** global configuration command for additional information.

Dedicated Out-of-Band Management Interface

The management-only configuration command has been introduced in the interface configuration mode to enable dedicated out-of-band management access to the device.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

SMTP E-mail Alerts

Version 7.0(1) includes the ability for administrators to be notified of system events via SMTP-based e-mail alerts. See the enhancements in the **logging** global configuration command and the **smtp-server** global configuration command to configure sending critical syslogs using SMTP.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enhanced System Health Monitoring and Diagnostic Services

Many enhancements have been made to provide improved monitoring of the system operation and to help isolate potential network and security appliance issues. To monitor and to troubleshoot memory usage levels or potential leaks the **show memory** command was enhanced together with the addition of a **show process memory EXEC** command.

The **show resource** and **show counters** commands provide detailed information about resource utilization for the appliance and security contexts as well as detailed statistics. To monitor the CPU utilization you may use the new **show cpu EXEC** command as well as the enhanced **show process cpu-hog EXEC** commands. To isolate potential software flaws the software introduces the **checkheaps** command and related **show EXEC** command. Finally, to get a better understanding of the block (packet) utilization, the **show blocks EXEC** command has been enhanced to provide extensive analytical tools on block queuing and utilization in the system.

Enhanced Debug Services

The enhanced **debug** commands have been improved and many new features include to respective debug support. Furthermore, the debug output is now supported to all virtual terminals without restrictions. That is, when you enable debug output for a particular feature, you will be able to view the output without any limitations. Clearly, the output will be restricted to the session where it was enabled. Finally, the user can send debug output over syslogs if your security policy allows it and you wish to do so by leveraging the enhanced **logging** command.

Enhanced Capture Support

The Version 7.0(1) introduces additional support to improve the ability of the user to diagnose device operation by supporting the ability to capture ISAKMP traffic and only capture packets dropped by the new Accelerated Security Path (ASP).

The existing **capture** command has been extended with a new **type** keyword and parameters to capture ISAKMP, packet drops, and packet drops matching a specified reason string.

Changes to Existing PIX 6.x Features

As a result of extensive enhancements and improvements made in the Security Appliance, a number of existing Security Appliance commands have been changed or deprecated.

For detailed information on the changed or deprecated commands, go to:

http://www.cisco.com/en/US/docs/security/asa/asa70/pix_upgrade/upgrade/guide/pixupgrd.html

Important Notes

Important Notes in Release 7.0

This section lists important notes related to Version 7.0(1).

Maximum Security Contexts and VLANs Supported

The maximum security contexts supported in release 7.0(1) for the PIX 535 are 50 tiers. The maximum number of VLANs supported are 150. For more information on the feature support for each platform license, see the “Platform Feature Licenses” section in the *Cisco Security Appliance Command Line Configuration Guide*

IKE Delete-with-Reason

IKE syslogs for Delete-with-Reason will not contain the reason text unless the clients support this feature. Currently the VPN 3002 Version 4.7 and PIX 501 Version 6.3(4) hardware clients do not support this feature.



Note

The PIX 501security appliance is not supported in software Version 7.0.

User Upgrade Guide

Before upgrading to Version 7.0(1), read the *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*. This guide also includes information about deprecated features and other changes in the Cisco PIX Software Version 7.0. For a list of deprecated features, and user upgrade information, go to the following URL:

http://www.cisco.com/en/US/docs/security/asa/asa70/pix_upgrade/upgrade/guide/pixupgrd.html



Caution

If you share the stateful failover update link with a link for regular traffic such as your inside interface, you must change your configuration before upgrading. Do not upgrade until you have corrected your configuration, as this is not a supported configuration and Version 7.0(1) treats the LAN failover and stateful failover update interfaces as special interfaces. If you upgrade to Version 7.0(1) with a configuration that shares an interface for both regular traffic and the stateful failover updates, configuration related to the regular traffic interface will be lost after the upgrade. The lost configuration may prevent you from connecting to the security appliance over the network.

Readme Document for the Conduits and Outbound List Conversion Tool 1.2

The Security Appliance Outbound/Conduit Conversion tool assists in converting configurations with **outbound** or **conduit** commands to similar configurations using access control lists (ACLs). ACL-based configurations provide uniformity and leverage the powerful ACL feature set. ACL based configurations provide the following benefits:

- Access control element (ACE) insertion capability - System configuration and management is greatly simplified by the ACE insertion capability that allows users to add, delete or modify individual ACEs.
- Outbound ACLs and Time-based ACLs - Gives administrators improved flexibility for defining access control policies by adding support for outbound ACLs and time-based ACLs.
- Enabling/Disabling of ACL Entries - Provides a convenient troubleshooting tool that allows administrators to test and fine-tune ACLs, without the need to remove and replace ACL entries.

Features not Supported in Version 7.0

The following features are not supported in Version 7.0 (1) release:

- PPPoE
- L2TP over IPSec
- PPTP

MIB Supported

For information on MIB Support, go to:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

Downgrade to Previous Version

To downgrade to a previous version of the operating system software (software image), use the **downgrade** command in privileged EXEC mode.

For more information and a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

**Caution**

Do not load a previous version of software if your PIX security appliance is currently running PIX Version 7.0 or later. Loading a software image from monitor mode, on a PIX security appliance that has a PIX Version 7.0 file system, results in unpredictable behavior and is not supported. We strongly recommend that you use the **downgrade** command from a running PIX Version 7.0 image that facilitates the downgrade process.

Caveats

The following sections describe the caveats for the 7.0(1) release.

For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

**Note**

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

<http://tools.cisco.com/Support/BugToolKit>

To become a registered cisco.com user, go to the following website:

<http://tools.cisco.com/RPF/register/register.do>

Open Caveats - Release 7.0(2)

Table 2 *Open Caveats*

ID Number	Software Release 7.0(2)	
	Corrected	Caveat Title
CSCeh60845	No	Logging queue incorrectly registers 8192 256-byte blocks
CSCeh81062	No	wrong ip addr on outgoing packets when PAT and static port are used
CSCeh90617	No	Recompiling ACLs can cause packet drops on low-end platforms
CSCeh98117	No	Tunnel-group passwords in cleartext when viewed with more
CSCei00497	No	PIX/ASA 7.0 doesnt encrypt packets if next hop is PIX interface.
CSCei20466	No	Increase in CPU utilization when OSPF is enabled
CSCei20809	No	sh access-l counters not updated when acl used in nat/nat-exempt

Table 2 Open Caveats (continued)

ID Number	Software Release 7.0(2)	
	Corrected	Caveat Title
CSCei21362	No	PIX traceback after issuing show isakmp sa detail command.
CSCei23290	No	DHCP Relay fails when static specified
CSCei24062	No	Some hosts in the network connects to inside intf cannot be reached
CSCei38640	No	AAA: radius /w expiry does not work when using funk radius server
CSCei38651	No	NT auth for VPN clients do not work with domainuser or user@domain
CSCei38667	No	Can't differentiate between root CA certs that have been re-keyed
CSCei41326	No	AAA: fallback to LOCAL authentication does not work for SSH
CSCei50190	No	PIX/ASA not accepting 2 ISAKMP policies with different AES types
CSCei51867	No	Usability - crypto config should be grouped together in CLI output
CSCei52413	No	PIX/ASA fails to import cert if CA issuer has 4096 bits cert
CSCsb31740	No	VPN IP local pool - detection of invalid IP OK - but fails to assign IP
CSCsb33629	No	address-pool subcommand doesn't error when list is full
CSCsb36188	No	PIX/ASA 7.0.1 - sending multiple authentication requests to ACS Server
CSCsb37531	No	Traceback after failover if TCP Intercept is triggered.
CSCsb40331	No	PIX 7.0(1)2 Assertion Violation w/Multiple Context & VOIP Configuration

Resolved Caveats - Release 7.0(2)

Table 3 Resolved Caveats

ID Number	Software Release 7.0(2)	
	Corrected	Caveat Title
CSCeg85121	Yes	Not able to specify url-server timeout to 5 seconds
CSCeh27584	Yes	rem-access-mon.mib fails GetNext&Bulk ops
CSCeh39197	Yes	Inspect proxy should not queue dropped packet
CSCeh50620	Yes	Traceback on standby when failing over dynamic L2L tunnel
CSCeh57035	Yes	Named networks not working in ospf network statements
CSCeh57562	Yes	Memory leak in ssh code
CSCeh59635	Yes	GTP: When the PDP CTX reached to 30000 Contexts the System Traceback
CSCeh60361	Yes	isakmp key no-config-mode - will not be converted on upgrade to 7.0
CSCeh60367	Yes	Default tunnel-groups do not appear in the output of show run all
CSCeh60673	Yes	PIX crashes on pinhole preparation and connection limit exceeded
CSCeh60887	Yes	PIX crashes due to memory corruption 7.0.1
CSCeh64177	Yes	Not able to configure infinite isakmp lifetime in pix/asa 7.0
CSCeh69389	Yes	Split-tunnel ACLs not converted to Standard ACLs on upgrade to 7.0

Table 3 Resolved Caveats (continued)

ID Number	Software Release 7.0(2)	
	Corrected	Caveat Title
CSCeh71023	Yes	Broadcasts leak from High Level Sec. Intf to Low Level Sec. Intf.
CSCeh71492	Yes	xauth enabled by default on Remote Access VPN tunnels on upgrade
CSCeh72706	Yes	traceback: IKE_daemon: Unexpected cleanup of tunnel table entry
CSCeh75725	Yes	7.0 does not support Extended ACLs (object groups) for split tunnel
CSCeh79645	Yes	ASDM handler stream for blocks data is missing for 2048 size
CSCeh81233	Yes	DCHP client: ip address dhcp setroute missing: no default route
CSCeh81774	Yes	un-NATed ACK packets sent on outside interface
CSCeh89562	Yes	PIX crashes when shuns are cleared while sh shun is running
CSCeh90902	Yes	Support for multiple crypto maps to the same peer missing
CSCeh94725	Yes	Embedded RTP IP not NATed in H.245 OLC Ack
CSCeh96708	Yes	Syslog reports erroneous transfer size in TCP Teardown 302014 syslog
CSCeh96865	Yes	H323: Media stream disconnect in the middle of H323 call
CSCeh97110	Yes	PIX should not response to reset packet outside window
CSCeh97407	Yes	RA Tunnels fail to connect after re-xauth during re-key
CSCei00227	Yes	isakmp key hostname converted to invalid tunnel-group
CSCei02443	Yes	PKI:F1 crash during srl retrieval at Crypto CA ,eip_free_pslct_108
CSCei03165	Yes	PIX reboots continuously with overlapping/redundant statics
CSCei04829	Yes	PIX 7.0 crash in IPsec message handler
CSCei08652	Yes	np70.bin reboots PIX without asking to erase the password
CSCei09266	Yes	Traceback when shuns are cleared
CSCei09829	Yes	AppsFW:HTTP-Strict when no reson string in response
CSCei12178	Yes	PIX crashes with memory corruption
CSCei12460	Yes	PIX-ASA crashes with TCP packet where dst IP is a multicast addr
CSCei12915	Yes	PIX ASA sends Syslogs with source port other than 514
CSCei15053	Yes	IKE test suite causes multiple reboots in 7.0(1)
CSCei15215	Yes	Firewall drops IP Options packets needed for igmp and rsvp traffic
CSCei16294	Yes	ISAKMP: Port selector are in host-order on the wire
CSCei16403	Yes	TCP keepalives on H.225 (1720) blocked with inspect h323 h225
CSCei16904	Yes	Syslog adds extra space
CSCei18370	Yes	sqlnet version 1 inspection crashes the box
CSCei19528	Yes	FTP Failed if client supports EPRT but server does not
CSCei20197	Yes	Can't get acl for pim rp-address cmd
CSCei21386	Yes	SIP: CSeq No parsed incorrectly if CSeq no length is 10
CSCei21387	Yes	SIP: SIP URI Parse error happens when receiving SIP Response
CSCei24376	Yes	Interface mtu minimum value changed from 64 to 300 bytes

Table 3 Resolved Caveats (continued)

ID Number	Software Release 7.0(2)	
	Corrected	Caveat Title
CSCei25213	Yes	PIX crashes with thread name SSH
CSCei27053	Yes	One byte TCP keepalives not processed correctly by normalizer
CSCei27070	Yes	Pass-through pptp with PAT stops working after a while
CSCei28815	Yes	FIN-ACK Dropped Despite Fact that Sequence Number within TCP Window
CSCei29901	Yes	Inconsistant baehvior on scanning
CSCei30474	Yes	Issue <clear con> command would hit page fault traceback
CSCei33574	Yes	GTP: box reloads on 2ndary PDP create when 1st fails
CSCei34524	Yes	Deny rule in nat exempt fails xlate replication to standby
CSCei50549	Yes	License mismatch when a pix has 4-tuple key and another has 5-tuple

Related Documentation

Use this document in conjunction with the PIX Firewall and Cisco VPN client Version 3.x documentation at the following websites:

http://www.cisco.com/en/US/products/sw/secursw/ps2120/tsd_products_support_series_home.html

http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd_products_support_series_home.html

Software Configuration Tips on the Cisco TAC Home Page

The Cisco Technical Assistance Center has many helpful pages. If you have a CDC account you can visit the following websites for assistance:

TAC Troubleshooting, Sample Configurations, Hardware Info, Software Installations and more:

http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

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

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

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

This document is to be used in conjunction with the documents listed in “[Related Documentation](#)” section.

CCSP, the Cisco Square Bridge logo, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2005 Cisco Systems, Inc.
All rights reserved.