Data Sheet

Cisco PIX Security Appliance Software Version 6.3

The world-leading Cisco PIX® Security Appliance Series provides robust, enterprise-class, integrated network security services, including stateful inspection firewalling, protocol and application inspection, virtual private networking (VPN), in-line intrusion protection, and rich multimedia and voice security—in cost-effective, easy-to-deploy solutions. Ranging from compact, "plug-and-play" desktop firewalls for small and home offices to carrier-class gigabit firewalls for the most demanding enterprise and service-provider environments, Cisco PIX Security Appliances provide robust security, performance, and reliability for network environments of all sizes.

Advanced Firewall Technologies Provide Enterprise-Class Network Security

Cisco PIX Security Appliances deliver a broad range of advanced firewall services that protect enterprise networks from threats lurking on the Internet and in today's network environments. The state-of-the-art Cisco Adaptive Security Algorithm (ASA) provides rich stateful inspection firewall services, tracking the state of all authorized network communications and preventing unauthorized network access. Cisco PIX Security Appliances deliver an additional layer of security through intelligent, "application-aware" security services that examine packet streams at Layers 4–7, using inspection engines specialized for many of today's popular applications. Administrators can also easily create custom security policies for firewall traffic by using the flexible access control methods and the more than 100 predefined applications, services, and protocols that Cisco PIX Security Appliances provide.

Access to network resources can also be strongly authenticated through the Cisco PIX Security Appliance's local user database or through integration with enterprise databases, either directly using TACACS+/RADIUS or indirectly with Cisco Secure Access Control Server (ACS). Cisco PIX Security Appliances provide extensive logging, URL filtering, content filtering, and more, when combined with Cisco AVVID (Architecture for Voice, Video and Integrated Data) partner solutions.

Market-Leading Voice-over-IP Security Services Protect Next-Generation Converged Networks

Cisco PIX Security Appliances provide market-leading protection for a wide range of voice-over-IP (VoIP) standards and other multimedia standards, including H.323 Version 4, Session Initiation Protocol (SIP), Cisco Skinny Client Control Protocol

(SCCP), Real-Time Streaming Protocol (RTSP), and Media Gateway Control Protocol (MGCP). Additionally, Cisco PIX Security Appliances provide security services for Telephony Application Programming Interface (TAPI) and Java Telephony Application Programming Interface (JTAPI)-based applications, when these applications use Computer Telephony Interface Quick Buffer Encoding (CTIQBE) as the network transport mechanism—such as Cisco SoftPhone and Cisco Customer Response Solution (CRS). This allows businesses to securely take advantage of the many benefits that converged data, voice, and video networks provide, including improved productivity and new competitive advantages. By combining VPN with the rich stateful inspection firewall services that Cisco PIX Security Appliances provide for these converged networking standards, businesses can securely extend voice and multimedia services to home office and remote office environments for additional cost savings and the other benefits converged networks bring.

Site-to-Site VPNs Extend Networks Economically to Remote Sites and Business Partners

Using the standards-based site-to-site VPN capabilities provided by Cisco PIX Security Appliances, businesses can securely extend their networks across low-cost Internet connections to business partners and remote and satellite offices worldwide. Built upon the Internet Key Exchange (IKE) and IP security (IPsec) VPN standards, Cisco PIX Security Appliances encrypt data using 56-bit Data Encryption Standard (DES), 168-bit Triple DES (3DES), or up to 256-bit Advanced Encryption Standard (AES) encryption. Cisco PIX Security Appliances can also participate in X.509-based Public Key Infrastructures (PKIs), and provide easy, automated certificate enrollment using the Simple Certificate Enrollment Protocol (SCEP)—another Internet standard Cisco Systems helped pioneer. Certain Cisco PIX Security Appliance models also support hardware VPN acceleration, delivering up to 440 megabits per second (Mbps) of 256-bit AES encrypted throughput, as well as support for up to 2000 IKE security associations.

Cisco Easy VPN Enables Highly Scalable, Easy-to-Manage VPN Deployments

The innovative Easy VPN capabilities found in Cisco PIX Security Appliances and other Cisco solutions—such as Cisco IOS® routers and Cisco VPN 3000 Series Concentrators—deliver a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture. Built upon the foundation of dynamic policy distribution and effortless provisioning, Easy VPN eliminates the operational costs associated with maintaining remote-device configurations typically required by traditional VPN solutions. Easy VPN enables Cisco customers to enjoy the numerous benefits that VPNs provide—increased employee productivity by taking advantage of high-speed broadband connectivity, and significantly reduced operational costs by eliminating expenses associated with legacy dialup architectures—without the problems commonly found with other remote-access VPN solutions.

Using the Cisco PIX Security Appliance robust, remote-access VPN concentrator services, enterprises can securely extend their networks to traveling employees, teleworkers, and remote offices for anytime, anywhere access to vital corporate resources. Acting as Cisco Easy VPN Servers, Cisco PIX Security Appliances support the wide range of software- and hardware-based Cisco Easy VPN Remote products. Cisco PIX Security Appliances enforce the latest VPN security policies by dynamically pushing these policies to Easy VPN Remote users as they connect.

Certain models of Cisco PIX Security Appliances can also act as “hardware VPN clients” using innovative, embedded Easy VPN Remote features, transparently providing secure access to a corporate network for all devices in a remote network protected by a Cisco PIX Security Appliance. This dramatically simplifies the initial deployment and ongoing management of VPNs deployed to remote offices and teleworker environments by eliminating the need to

install and maintain VPN client software on the individual devices protected by a remote Cisco PIX Security Appliance. Advanced client-side resiliency features help ensure maximum VPN uptime by providing automatic failover to backup Easy VPN Servers in the event of a network or service failure.

Integrated Intrusion Protection Guards Against Popular Internet Threats

The integrated in-line intrusion-protection capabilities in Cisco PIX Security Appliances protect today's networks from many popular forms of attacks, including Denial-of-Service (DoS) attacks and malformed packet attacks. Using a wealth of advanced intrusion-protection features, including DNSGuard, FloodGuard, FragGuard, MailGuard, IPVerify and TCP intercept, in addition to looking for more than 55 different attack "signatures," Cisco PIX Security Appliances keep a vigilant watch for attacks, can optionally block them, and can notify administrators about them in real time. Additionally, Cisco PIX Security Appliances support virtual packet reassembly, searching for attacks that are hidden over a series of fragmented packets. Strong integration with Cisco Intrusion Detection Systems (IDS) sensors enables Cisco PIX Security Appliances to automatically shun (block) network nodes identified as being hostile by Cisco IDS sensors.

Enterprise-Class Resiliency Provides Maximum Business Uptime

Cisco PIX Security Appliance select models provide award-winning stateful failover capabilities that ensure resilient network protection for enterprise network environments. Employing a cost-effective, active-standby, high-availability architecture, Cisco PIX Security Appliances that are configured as a failover pair continuously synchronize their connection state and device configuration data. Synchronization can take place over a high-speed LAN connection, providing another layer of protection through the ability to geographically separate the failover pair. In the event of a system or network failure, network sessions are automatically transitioned between firewalls, with complete transparency to users.

Robust Remote-Management Solutions Lower Total Cost of Ownership

Cisco PIX Security Appliances deliver a wealth of remote-management methods for configuration, monitoring, and troubleshooting. Management solutions range from centralized, policy-based management tools to integrated, Web-based management to support for remote-monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog. Cisco PIX Security Appliances additionally provide up to 16 levels of customizable administrative roles so that enterprises can grant administrators and operations personnel the appropriate level of access to each firewall (for example, monitoring only, read-only access to the configuration, VPN configuration only, firewall configuration only, and so on). Cisco PIX Security Appliances also include robust Auto Update capabilities, a set of revolutionary secure remote-management services that ensure firewall configurations and software images are kept up to date.

Administrators can easily manage large numbers of remote Cisco PIX Security Appliances using CiscoWorks VPN/Security Management Solution (VMS). This suite consists of numerous modules including Management Center for Firewalls, Auto Update Server Software, and Security Monitor. This powerful combination provides a highly scalable, next-generation, three-tier management solution that includes the following features:

- Comprehensive configuration and software image management
- Device hierarchy with "Smart Rules"-based configuration inheritance

- Customizable administrative roles and access privileges
- Comprehensive enterprise change management and auditing
- "Touchless" software image management for remote Cisco PIX Security Appliances
- Support for dynamically addressed appliances

Additional integrated event management and inventory solutions are also available as part of the CiscoWorks VMS network management suite.

The integrated Cisco PIX Device Manager provides an intuitive, Web-based management interface for remotely configuring, monitoring, and troubleshooting a single Cisco PIX Security Appliance—without requiring any software (other than a standard Web browser) to be installed on an administrator's computer. Alternatively, through methods including Telnet and Secure Shell (SSH), or out of band through a console port, administrators can remotely configure, monitor, and troubleshoot Cisco PIX Security Appliances using a command-line interface (CLI).

New Features Found in Cisco PIX Security Appliance Software Version 6.3

Cisco PIX Security Appliance Software Version 6.3 provides a wealth of new features, including those detailed below. A complete list of features is available in the Cisco PIX Security Appliance Software Version 6.3 Release Notes.

Table 1 New Features and Benefits

Key Features	Benefit
Enterprise-Class Security	
Virtual LAN (VLAN)-based virtual interfaces	• Provides increased flexibility when defining security policies and eases overall integration into switched network environments by supporting the creation of logical interfaces based on IEEE 802.1q VLAN tags, and the creation of security policies based on these virtual interfaces • Supports multiple virtual interfaces on a single physical interface through VLAN trunking • Supports multiple VLAN trunks per Cisco PIX Security Appliance • Supports up to 8 VLANs on Cisco PIX 515 and 515E Security Appliances, 10 VLANs on Cisco PIX 520 and 525 Security Appliances, and 24 VLANs on Cisco PIX 535 Security Appliances
Open Shortest Path First (OSPF) dynamic routing	• Provides comprehensive OSPF dynamic routing services on Cisco PIX Security Appliances using technology based on world-renowned Cisco IOS Software • Offers improved network reliability through fast route convergence and secure, efficient route distribution • Delivers a secure routing solution in environments using Network Address Translation (NAT) through tight integration with Cisco PIX Security Appliance NAT services • Supports MD5-based OSPF authentication, in addition to plaintext OSPF authentication, to prevent route spoofing and various routing-based DoS attacks • Provides route redistribution between OSPF processes, including OSPF, static, and connected routes • Supports load balancing across equal-cost multipath routes
Secure Hypertext Transfer Protocol (HTTPS) authentication proxy	• Offers a secure, Web-based method for user authentication to the firewall prior to allowing any of the user's network traffic to traverse the firewall

Table 1 New Features and Benefits

Key Features	Benefit
Local user authentication database	• Enables administrators to define usernames and associated passwords locally on a Cisco PIX Security Appliance, which can then be used to authenticate users prior to allowing them network and VPN access • Provides a cost-effective alternative for storage of user authentication information
HTTPS and FTP web request filtering via enhanced Websense integration	• Extends integration with Websense-based employee web usage management solutions by adding support for filtering of users' HTTPS and FTP web requests
Advanced Encryption Standard (AES)	• Adds support for securing site-to-site and remote access VPN connections with new international encryption standard, Advanced Encryption Standard (AES) • Provides software-based AES support on all supported Cisco PIX Security Appliance models and hardware-accelerated AES via the new VAC+ card on select Cisco PIX Security Appliance models • Supports all standard AES key sizes: 128, 192, and 256
VPN Acceleration Card+ (VAC+)	• Delivers up to 440 Mbps of hardware-accelerated 168-bit 3DES and 256-bit AES encryption (on select Cisco PIX Security Appliance models) for highly scalable site-to-site and remote access VPN services • Provides hardware acceleration of 56-bit DES, 168-bit 3DES, and all standard AES key sizes (128, 192, and 256) • Supports up to 2000 concurrent IKE associations
VPN NAT transparency	• Extends support for site-to-site and remote access IPsec-based VPNs to network environments that implement NAT or Port Address Translation (PAT), such as airports, hotels, wireless hot spots, and broadband environments • Supports automatic discovery of NAT/PAT environments during VPN tunnel negotiation and can dynamically encapsulate VPN traffic using an Internet Engineering Task Force (IETF)-based UDP wrapper mechanism for safe traversal through NAT/PAT boundaries
Custom IKE port numbers	• Enables IKE sessions to be accepted on administrator-specified UDP ports, providing additional flexibility for enterprise network environments
Integrated Dynamic Host Configuration Protocol (DHCP) server support on multiple interfaces	• Extends integrated DHCP server to provide DHCP services on one or more administrator-specified interfaces concurrently, each with a separate DHCP address pool
Management	
Syslog by access control list (ACL) entry	• Introduces powerful new reporting and troubleshooting capabilities that enable detailed statistics to be gathered on which ACL entries are triggered by network traffic attempting to traverse a Cisco PIX Security Appliance • Gives precise control over which ACL entry-related syslog events are generated
Assignable syslog levels by message	• Provides administrators tremendous flexibility and control over which syslog messages Cisco PIX Security Appliances generate
ACL editing	• Provides capabilities for inserting and deleting individual ACL entries without deleting and re-creating the entire ACL
DHCP relay	• Forwards DHCP requests from internal devices to an administrator-specified DHCP server, enabling centralized distribution, tracking and maintenance of IP addresses

Table 1 New Features and Benefits

Key Features	Benefit
Interface name as address in ACLs and conduits	• Enables the creation of security policies based on interface name instead of IP address, which is especially useful in broadband environments where the outside interface is typically assigned a dynamic IP address
Custom administrative access banner messages	• Provides facility to define custom messages that will appear when anyone attempts to access the CLI interface, after successful login and when entering “exec mode” of Cisco PIX Security Appliances via console port, telnet, or SSH
Console connection inactivity timeout	• Protects console from unauthorized administrative access by automatically logging out sessions after a configurable period of inactivity
Show command output filter	• Provides tools to customize the output of CLI-based **show** commands, such as filtering using Cisco IOS Software style regular expressions
Custom logging identifier	• Allows a custom firewall identifier to be selected, such as an interface IP address, that will be included in all syslog messages to improve the centralized reporting of firewall events
Remote management enhancements	• Supports secure remote management of Cisco PIX Security Appliances through a VPN tunnel to their inside interface IP address; especially useful in broadband network environments where firewalls outside interface addresses are typically assigned dynamically
Small Office and Home Office	
Easy VPN Remote (hardware VPN client) enhancements	• Introduces ability to authenticate individual users behind a Cisco PIX Security Appliance through an easy-to-use, Web-based interface with support for standard and one-time passwords (including authentication tokens) • Allows certain network devices, such as printers and IP phones, to pass through a VPN tunnel using authentication based on the devices’ Media Access Control (MAC) addresses and/or their IP addresses • Provides robust client-side VPN resiliency with support for dynamic downloading of backup Easy VPN Server information and automatic failover, in the event of a VPN link failure • Supports VPN 3000 Series Concentrator load balancing with automatic redirection to the least utilized concentrator • Provides new, easy-to-use Web interface for manual VPN tunnel control, user authentication, and tunnel status information • Introduces method to specify the networks and individual IP addresses that can manage a Cisco PIX Security Appliance securely via its outside interface, regardless if the VPN tunnel is up or down
DHCP relay	• Forwards DHCP requests from devices on specific interfaces to an administrator-specified DHCP server • Provides method for enterprises to centrally distribute, track, and maintain IP addresses
PAT for Point-to-Point Tunneling Protocol (PPTP)	• Enhances the rich PAT functionality in Cisco PIX Security Appliances to enable multiple PPTP sessions to traverse firewall
PAT for IPsec	• Supports IPsec passthrough services, enabling a single device behind the Cisco PIX Security Appliance to establish a VPN tunnel through the firewall to a VPN peer

Table 1 New Features and Benefits

Key Features	Benefit
Increased firewall performance on PIX 501 and 506E Security Appliances	• Unleashes new performance levels on new and existing Cisco PIX 501 and 506E Security Appliances, delivering up to 6 times more performance than previous software releases
Increased number of IPsec VPN peers supported on Cisco PIX 501 Security Appliances	• Increases number of site-to-site and remote access VPN peers supported on Cisco PIX 501 Security Appliances from 5 to 10, enabling greater VPN scalability in home office and small office environments
Voice over IP (VoIP) and Multimedia	
H.323 Version 3 and 4	• Extends Cisco PIX Security Appliance market-leading VoIP security by adding support for the latest versions of the H.323 standard, which is used by numerous applications and millions of users worldwide • Adds support for many new H.323 features, including the ability to handle multiple calls that use the same call signaling channel
TAPI and JTAPI over CTIQBE	• Supports inspection of various Cisco TAPI and JTAPI based applications that use CTIQBE, including Cisco IP SoftPhone and Cisco Customer Response Solution (CRS)
MGCP	• Inspects MGCP messages passing between call agents, media gateways, and other components in production VoIP environments
PAT for SCCP	• Extends market-leading VoIP support and enables SCCP (the call-signaling protocol used by Cisco IP phones) to work in PAT environments; typically found in home offices and remote offices

Technical Specifications

VPN Client Compatibility

Cisco PIX Security Appliances support a wide variety of software- and hardware-based VPN clients, which include the following:

Software IPsec VPN clients	Cisco Secure VPN Client, Version 1.1 Cisco VPN 3000 Concentrator Client, Version 2.5 and later Cisco VPN Client for Windows, Version 3.0 and later Cisco VPN Client for Linux, Version 3.5 and later Cisco VPN Client for Solaris, Version 3.5 and later Cisco VPN Client for Mac OS X, Version 3.5 and later
Hardware IPsec VPN clients	Cisco VPN 3002 Hardware Client, Version 3.0 and higher Cisco IOS Software Easy VPN Remote, Release 12.2(8)YJ Cisco PIX Security Appliance, Version 6.2 and higher
Layer 2 Tunneling Protocol (L2TP)/IPsec VPN clients	Microsoft Windows 2000
Point-to-Point Tunneling Protocol (PPTP) VPN clients	Microsoft Windows 95 Microsoft Windows 98 Microsoft Windows NT 4.0 Microsoft Windows 2000

Easy VPN Server Compatibility

Cisco PIX Security Appliances can now act as hardware-based VPN clients, taking advantage of the new Cisco Easy VPN Remote capabilities in Cisco PIX Security Appliance Software. The following Cisco Easy VPN Server platforms are supported for this deployment scenario:

Cisco IOS Routers	Release 12.2(8)T and later
Cisco PIX Security Appliances	Version 6.0(1) and later
Cisco VPN 3000 Series Concentrators	Version 3.1 and later

Cisco Site-to-Site VPN Compatibility

In addition to providing interoperability for many third-party VPN products, Cisco PIX Security Appliances interoperate with the following Cisco VPN products for site-to-site VPN connectivity:

Cisco IOS Routers	Release 12.1(6)T and later
Cisco PIX Security Appliances	Version 5.1(1) and later
Cisco VPN 3000 Concentrators	Version 2.5.2 and later

Cryptographic Standards Supported

Cisco PIX Security Appliances support numerous cryptographic standards and related third-party products and services, including the following:

Asymmetric (public key) encryption algorithms	RSA (Rivest, Shamir, Adelman) public/private key pairs, 512 bits to 2048 bits
Symmetric encryption algorithms	AES: 128, 192, and 256 bits DES: 56 bits 3DES: 168 bits RC4: 40, 56, 64, and 128 bits
Perfect Forward Secrecy (Diffie-Hellman key negotiation)	Group 1: 768 bits Group 2: 1024 bits Group 5: 1536 bits
Hash algorithms	MD5: 128 bits SHA-1: 160 bits
X.509 certificate authorities	Baltimore UniCERT Entrust Authority Microsoft Windows 2000 Certificate Services VeriSign OnSite
X.509 certificate enrollment protocols	SCEP

System Requirements

Platforms supported	Cisco PIX 501 Security Appliance Cisco PIX 506 Security Appliance Cisco PIX 506E Security Appliance Cisco PIX 515 Security Appliance Cisco PIX 515E Security Appliance Cisco PIX 520 Security Appliance Cisco PIX 525 Security Appliance Cisco PIX 535 Security Appliance
Minimum RAM	32 megabytes (MB), except the Cisco PIX 501 Security Appliance, which requires 16 MB
Minimum Flash memory	16 MB, except the Cisco PIX 501, 506, and 506E Security Appliance models, which require 8 MB
Expansion cards supported	Single-port 10/100 Fast Ethernet card 4-port 10/100 Fast Ethernet card Single-port Gigabit Ethernet, multimode (SX) SC, card VPN Acceleration Card (Cisco VAC) VPN Acceleration Card+ (Cisco VAC+)

Product Ordering Information

PIX-SW-UPGRADE=	Cisco PIX Security Appliance Software one-time upgrade for customers without a current Cisco SMARTnet™ support contract

Support Services

Support services are available from Cisco and Cisco partners. Cisco SMARTnet service augments customer support resources, and provides anywhere, anytime access to technical resources (both online and by telephone), the ability to download updated system software, and hardware advance replacement.

Additional Information

For more information, please visit the following links:

Cisco PIX Security Appliance Series:

http://www.cisco.com/go/pix

Cisco PIX Device Manager:

http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pixdm_ds.pdf

Cisco Secure ACS:

http://www.cisco.com/go/acs

CiscoWorks VMS, Management Center for Firewalls, Auto Update Server Software, and Security Monitor:

http://www.cisco.com/go/vms

SAFE Blueprint from Cisco:

http://www.cisco.com/go/safe

To download the latest Cisco PIX Security Appliance Software and Cisco PIX Device Manager (with a valid Cisco.com login), visit:

http://www.cisco.com/cgi-bin/tablebuild.pl/pix

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

RD/LW3946 0303