Data Sheet

Cisco PIX Firewall Version 6.2

The world-leading Cisco PIX® Firewall Series of purpose-built security appliances provides robust, enterprise-class security services, including stateful inspection firewalling, virtual private networking (VPN), intrusion protection, and much more—in cost-effective, easy-to-deploy solutions. Ranging from compact, plug-and-play desktop firewalls for small/home offices to carrier-class gigabit firewalls for the most demanding enterprise and service-provider environments, Cisco PIX Firewalls provide robust security, performance, and reliability for network environments of all sizes.

Advanced Firewall Technologies Provide Enterprise-Class Network Security

Cisco PIX Firewalls deliver a broad range of advanced firewall services that protect enterprise networks from the 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 Firewalls deliver an additional layer of security through intelligent, "application-aware" security services that examine packet streams at Layers 4 through 7, using inspection engines specialized for many of today's popular applications. Administrators can easily create custom security policies that will be enforced on network traffic traversing the firewall by leveraging more than 100 pre-defined applications, services, and protocols within Cisco PIX Firewalls, and the flexible access control capabilities that Cisco PIX Firewalls provide. Access to network resources can also be strongly authenticated via the Cisco PIX Firewall's seamless integration with enterprise databases, either directly using TACACS+/RADIUS or indirectly via Cisco Secure Access Control Server (ACS). In addition to these services, Cisco PIX Firewalls provide extensive logging, URL filtering, content filtering, and more in concert 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 Firewalls continue to provide market-leading protection for numerous voice-over-IP (VoIP) standards and other multimedia standards, including H.323, Session Initiation Protocol (SIP), Skinny, Real-Time Transport Protocol (RTP), Real-Time Streaming Protocol (RTSP), and Real-Time Transport Control Protocol (RTCP). This allows businesses to securely take advantage of the many benefits that converged data and voice networks provide, such as significant total cost of ownership (TCO) savings and the competitive advantages and improved productivity gained through the power of fully integrated voice, video, and data networks. By combining VPN with the rich

stateful inspection firewall services that Cisco PIX Firewalls provide for these converged networking standards, businesses can easily extend voice and multimedia services to remote/satellite offices for additional bandwidth and cost savings.

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

Using the standards-based site-to-site VPN capabilities within Cisco PIX Firewalls, businesses can securely extend their network across low-cost Internet connections to business partners and remote/satellite offices worldwide. Built upon the Internet Key Exchange (IKE) and IP Security (IPSec) VPN standards, Cisco PIX Firewalls encrypt data using 56-bit Data Encryption Standard (DES) or advanced 168-bit Triple DES (3DES) encryption, ensuring that malicious individuals cannot see sensitive business data as it safely travels across the Internet. Cisco PIX Firewalls can also participate in X.509-based Public Key Infrastructures (PKI) and provide easy, automated certificate enrollment by taking advantage of the Simplified Certificate Enrollment Protocol (SCEP)—another Internet standard Cisco helped to pioneer. Certain Cisco PIX Firewall models also provide integrated hardware VPN acceleration, providing up to 100 Mbps of 3DES throughput and support for up to 2000 IKE security associations.

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

The innovative Easy VPN capabilities found in Cisco PIX Firewalls and other Cisco solutions—such as Cisco IOS® Software-based 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.

Cisco PIX Firewalls provide robust, remote-access VPN concentrator services that enable enterprises to securely extend their network to traveling employees, teleworkers, and remote offices for “anytime, anywhere access” to vital corporate network resources. Acting as an Easy VPN Server, Cisco PIX Firewalls support the wide range of Cisco software- and hardware-based Easy VPN Remote products. By dynamically pushing VPN security policies to Easy VPN-enabled users as they connect, Cisco PIX Firewalls ensure that the latest VPN security policy is consistently enforced for all remote-access users.

Certain models of Cisco PIX Firewalls can also act as “hardware VPN clients” using the new Easy VPN Remote features in Cisco PIX Firewall OS, transparently providing secure access to a corporate network for all devices protected by a Cisco PIX Firewall in a remote network. 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 Firewall. Advanced client-side resiliency features 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 from Popular Internet Threats

The integrated intrusion-protection capabilities in Cisco PIX Firewalls 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, and TCP intercept, in addition to looking for more than 55 different attack "signatures," Cisco PIX Firewalls keep a vigilant watch for attacks, can optionally block them, and can notify administrators about them in real time. Additionally, Cisco PIX Firewalls 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 Firewalls to automatically shun (block) network nodes identified as being hostile by Cisco IDS sensors.

Enterprise-Class Resiliency Provides Maximum Business Uptime

Cisco PIX Firewalls provide award-winning stateful failover capabilities (on select models) that ensure resilient network protection for enterprise network environments. Employing a cost-effective, active-standby high-availability architecture, Cisco PIX Firewalls configured as a failover pair continuously synchronize connection state information and device configuration data between one another. Performing this synchronization over a high-speed LAN connection provides the added benefit of being able to geographically separate failover pair members, thus providing a further layer of protection. In the rare event of a system or network failure, network sessions are automatically transitioned between firewalls seamlessly, and with complete transparency to network users.

Robust Remote-Management Solutions Lower Total Cost of Ownership

Cisco PIX Firewalls deliver a wealth of remote-management methods for configuration, monitoring, and troubleshooting. Management solutions range from an integrated, Web-based management application to highly scalable multi-firewall management tools to support for remote-monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog. Cisco PIX Firewalls additionally provide up to 16 levels of customizable administrative roles, so that enterprises can grant administrators and operations personnel the appropriate level of permissions they need for each firewall they manage (for example, monitoring only, read-only access to the configuration, VPN configuration only, firewall configuration only, etc.). Cisco PIX Firewalls now also support Auto Update, a revolutionary secure remote-management capability that ensures firewalls configurations and software images are kept up-to-date.

Cisco PIX Device Manager (PDM), integrated with Cisco PIX Firewalls, provides administrators an intuitive, Web-based management interface for remotely configuring and monitoring a single Cisco PIX Firewall, without requiring any software (other than a standard Web browser) to be installed on an administrator's computer. Administrators can also remotely configure, monitor, and troubleshoot Cisco PIX Firewalls using a command-line interface (CLI) through various methods, including Telnet and Secure Shell (SSH) Protocol, or out-of-band via a console port.

Administrators can easily manage a large number of remote Cisco PIX Firewalls using either the new combination of the CiscoWorks Management Center for Cisco PIX Firewalls and Auto Update Server, or Cisco Secure Policy Manager (CSPM)—all available within the Cisco VPN Security Management Solution (VMS) network management suite. The CiscoWorks Management Center for Cisco PIX Firewalls is a highly scalable, next-generation, three-tier management solution for Cisco PIX Firewalls that includes features such as hierarchical grouping of managed firewalls, "Smart Rules" configuration inheritance, customizable administrative roles and access privileges,

workflow-based enterprise change management, comprehensive support for Cisco PIX Firewall's new Auto Update capabilities, and support for dynamically addressed firewalls. Cisco Secure Policy Manager Release 3.0 is a policy-based centralized management solution for Cisco PIX Firewalls that includes a task-based interface, an interactive network topology map, policy wizards, and policy import capabilities. Additional integrated event management and inventory solutions are also available as part of the Cisco VMS network management suite.

New Features Found in Cisco PIX Firewall Release 6.2

Cisco PIX Firewall Release 6.2 provides a wealth of new innovative features, which are detailed below:

Table 1 New Features and Benefits

New Features	Benefits
Enterprise-Class Security	
LAN-based failover	• Extends failover functionality and enables geographic separation of Cisco PIX Firewalls in a failover pair by allowing failover information to be shared over a dedicated LAN connection (instead of a serial cable) between failover pairs
Bidirectional Network Address Translation (NAT)	• Enhances rich NAT functionality in Cisco PIX Firewalls to support environments with overlapping private address ranges
Turbo access control lists (ACLs)	• Provides significantly enhanced performance and deterministic search times for ACL processing; especially useful in environments where extensive ACLs are deployed
N2H2 URL filtering	• Integrates with N2H2 Sentian™ products—leading Internet filtering solutions—to provide robust employee Web access control and monitoring
Enhanced small-packet performance	• Delivers up to 48 percent more firewall performance for 64- to 512-byte packets than previous Cisco PIX Firewall OS releases, due to further optimization of small-packet processing
Management	
Auto Update	• Provides highly scalable, secure remote management of PIX Firewalls with a unique push/pull management model • Next-generation secure XML/HTTPS interface can be leveraged by Cisco and third-party management applications for remote firewall configuration management, inventory, software image management/deployment and monitoring • Supports dynamically addressed firewalls in addition to firewalls with static IP addresses • Integrates seamlessly with CiscoWorks Management Center for Cisco PIX Firewalls and Auto Update Server for robust, scalable remote management of up to 1000 PIX Firewalls
Object grouping	• Enables administrators to group network objects (such as devices, networks, and services) into logical groups to greatly simplify access control rule definition and maintenance

Table 1 New Features and Benefits

New Features	Benefits
Command-level authorization	• Enables businesses to create up to 16 customizable administrative roles and profiles for accessing Cisco PIX Firewalls (for example, monitoring only, read-only access to configuration, VPN administrator, firewall administrator, etc.) • Uses either the internal Cisco PIX Firewall administrator database or outside sources via TACACS+, such as Cisco Secure ACS
Dynamic ACLs via Cisco Secure ACS	• Supports dynamic downloading and enforcement of ACLs on a per-user basis, upon user authentication with the firewall
Network Time Protocol (NTP) v3 client	• Provides convenient method for synchronizing the clock on Cisco PIX Firewalls with other devices on a network
CPU monitoring via SNMP v2	• Extends SNMP-based remote firewall health monitoring to include the ability to monitor CPU utilization
Software and configuration updates via HTTP and HTTPS	• Adds support for downloading Cisco PIX Firewall OS and Cisco PIX Device Manager software, as well as configuration updates via HTTP or HTTPS • Provides ability to deliver configuration and software updates over authenticated, encrypted network connection
HTTPS-based CLI access	• Delivers flexible, secure interface for interactive and easily scriptable access to Cisco PIX Firewall CLI via standard HTTPS requests
Packet capture	• Gives administrators new, powerful troubleshooting capabilities by providing robust packet-capturing facilities on each interface of the firewall • Supports several methods of accessing captured packets, including via the console, secure Web access or a file exported to a Trivial File Transfer Protocol (TFTP) server
Small Office/Home Office	
Easy VPN Remote (hardware VPN client)	• Enables dramatically simplified VPN rollouts to small office, teleworker, and remote/branch-office environments, allowing Cisco PIX 501, 506, and 506E Firewalls to act as hardware VPN clients, and eliminating the provisioning complexities of traditional site-to-site VPN deployments • Downloads VPN policy dynamically from an Easy VPN Server upon connection, ensuring the latest corporate security policies are enforced • Provides robust client-side VPN resiliency with support for up to ten Easy VPN servers with automatic failover, in addition to Dead Peer Detection (DPD) support • Enables the network behind a Cisco PIX Firewall to appear as a single user to the VPN headend when using Easy VPN Remote Client Mode • Provides site-to-site VPN-like functionality without requiring any additional provisioning when using Easy VPN Remote Network Extension Mode • Supports both split and non-split tunneling environments • Provides intelligent, transparent Domain Name System (DNS) proxy capabilities for access to both corporate and public DNS servers
PPP over Ethernet (PPPoE) support	• Ensures compatibility with networks that require PPPoE support, such as xDSL and cable modem broadband environments

Table 1 New Features and Benefits

New Features	Benefits
Voice-over-IP (VoIP)/Multimedia	
Multicast support	• Supports wide range of multicast applications by introducing support for Internet Group Management Protocol (IGMP) v2 and stub multicast routing, including NAT and Port Address Translation (PAT) and the ability to build access control lists for multicast traffic
PAT for H.323 and SIP	• Extends market-leading VoIP support and enables SIP and H.323 to work in PAT environments, typically found in home offices and remote offices
DHCP server support for Cisco IP phones	• Simplifies remote Cisco IP Phone deployments by providing Cisco CallManager contact information via DHCP options 66 and 150 to Cisco IP phones for automated bootstrapping
Internet Locator Service (ILS) Fixup	• Adds support for ILS, a popular directory service used by applications such as Microsoft NetMeeting, SiteServer and Active Directory, for registration and location of network entities/endpoints

Technical Specifications

VPN Client Compatibility

Cisco PIX Firewalls support a wide variety of software- and hardware-based VPN clients, including:

Software IPSec VPN clients	Cisco Secure VPN Client Release 1.1 Cisco VPN 3000 Concentrator Client, Release 2.5 and higher Cisco VPN Client for Microsoft Windows, Release 3.0 and higher Cisco VPN Client for Linux, Release 3.5 and higher Cisco VPN Client for Solaris, Release 3.5 and higher Cisco VPN Client for Mac OS X, Release 3.5 and higher
Hardware IPSec VPN clients	Cisco VPN 3002 Hardware Client, Release 3.0 and higher Cisco IOS Software Easy VPN Remote, Release 12.2(8)YJ Cisco PIX Firewall Easy VPN Remote, Release 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 Firewalls can now act as hardware-based VPN clients, taking advantage of the new Easy VPN Remote capabilities in Cisco PIX Firewall OS. The following Easy VPN Server platforms are supported for this deployment scenario:

Cisco IOS Routers	Release 12.2(8)T and higher
Cisco PIX Firewalls	Release 6.0(1) and higher
Cisco VPN 3000 Concentrators	Release 3.1 and higher

Cisco Site-to-Site VPN Compatibility

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

Cisco IOS Routers	Release 12.1(6)T and higher
Cisco PIX Firewalls	Release 5.1(1) and higher
Cisco VPN 3000 Concentrators	Release 2.5.2 and higher

Cryptographic Standards Supported

Cisco PIX Firewalls 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	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
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 Firewall Cisco PIX 506 Firewall Cisco PIX 506E Firewall Cisco PIX 515 Firewall Cisco PIX 515E Firewall Cisco PIX 520 Firewall Cisco PIX 525 Firewall Cisco PIX 535 Firewall
RAM, minimum	32 MB, except Cisco PIX 501 which requires 16 MB
Flash memory, minimum	16 MB, except Cisco PIX 501/506/506E which require 8 MB
Expansion cards supported	Single-port 10/100 Fast Ethernet card Four-port 10/100 Fast Ethernet card Single-port Gigabit Ethernet, multimode (SX) SC, card VPN Acceleration Card (VAC)

Product Ordering Information

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

Support Services

Support services are available from Cisco partners as well as from Cisco. The Cisco SMARTnet service augments customer support resources. It provides 24x7x 365 access to technical resources (both online and via telephone), the ability to download updated system software, and hardware advance replacement.

Additional Information

For more information, please visit the following links:

Cisco PIX Firewall:

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

Cisco Secure Policy Manager:

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

Cisco VPN Security Management Solution (VMS), CiscoWorks Management Center for Cisco PIX Firewalls and Auto Update Server:

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

Cisco SAFE Blueprint:

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

To download the latest Cisco PIX Firewall OS and Cisco PIX Device Manager software (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: +65 317 7777
Fax: +65 317 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 12/02