DATA SHEET

CISCO PIX SECURITY APPLIANCE SOFTWARE VERSION 7.0

RELEASE HIGHLIGHTS

ADVANCED FIREWALL SERVICES

- Deep inspection firewall services for HTTP, FTP, ESMTP, and more
- Instant messaging, peer-to-peer, and tunneling application blocking
- Cisco Modular Policy Framework with flow-based security policies
- Virtual firewall services
- Layer 2 transparent firewall
- 3G Mobile Wireless security services

ROBUST IPSEC VPN SERVICES

- VPN client security posture enforcement
- Automatic VPN client software updating
- OSPF dynamic routing over VPN tunnels

HIGH AVAILABILITY SERVICES

- Active/Active failover with asymmetric routing support
- Remote-access and site-to-site VPN stateful failover
- Zero-downtime software upgrades

INTELLIGENT NETWORK SERVICES

- PIM multicast routing
- Quality of service (QoS)
- IPv6 networking

FLEXIBLE MANAGEMENT SOLUTIONS

- SSHv2 and SNMPv2c
- Configuration rollback
- Usability enhancements

The market-leading Cisco PIX® Security Appliance Series delivers robust user and application policy enforcement, multi-vector attack protection, and secure connectivity services in cost-effective, easy-to-deploy solutions.

These purpose-built appliances provide a wealth of integrated security and networking services, including:

- Advanced application-aware firewall services
- Market-leading voice over IP (VoIP) and multimedia security
- Robust site-to-site and remote-access IPSec VPN connectivity
- Award-winning resiliency
- Intelligent networking services
- Flexible management solutions

Ranging from compact, “plug-and-play” desktop appliances for small and home offices to modular gigabit appliances with superior investment protection for enterprise and service-provider environments, Cisco PIX Security Appliances provide robust security, performance, and reliability for network environments of all sizes.

ADVANCED FIREWALL SERVICES DELIVER STRONG BUSINESS PROTECTION AND RICH APPLICATION CONTROL

Robust Stateful Inspection and Application-Layer Security

Cisco PIX Security Appliances integrate a broad range of advanced firewall services to protect businesses from the constant barrage of threats on the Internet and in business network environments. As a secure foundation, Cisco PIX Security Appliances provide rich stateful inspection firewall services, tracking the state of all network communications and preventing unauthorized network access. Building upon those services, Cisco PIX Security Appliances deliver strong application layer security through intelligent, application-aware inspection engines that examine network flows at Layers 4–7. To defend networks from application-layer attacks and to give businesses more control over the applications and protocols used in their environments, these inspection engines incorporate extensive application and protocol knowledge and employ security enforcement technologies that include protocol anomaly detection, application and protocol state tracking, Network Address Translation (NAT) services, and attack detection and mitigation techniques such as application/protocol command filtering, content verification, and URL deobfuscation. These inspection engines also give businesses control over instant messaging, peer-to-peer file sharing, and tunneling applications, enabling businesses to enforce usage policies and free up network bandwidth for legitimate business applications.

Multi-Vector Attack Protection

Cisco PIX Security Appliances incorporate multi-vector attack protection services to further defend businesses from many popular forms of attacks, including denial of service (DoS) attacks, fragmented attacks, replay attacks, and malformed packet attacks. Using a wealth of advanced attack protection features such as TCP stream reassembly, traffic normalization, DNSGuard, FloodGuard, FragGuard, MailGuard, IPVerify, and TCP intercept, Cisco PIX Security Appliances identify and stop a wide range of attacks, and can provide real-time alerts to administrators.

Flexible Access Control and Powerful Flow-Based Policies

Administrators can also easily create custom security policies using the flexible access control technologies provided by Cisco PIX Security Appliances, including network and service object groups, user- and group-based policies, and more than 100 predefined applications and protocols. Using the powerful Modular Policy Framework introduced in Cisco PIX Security Appliance Software Version 7.0, administrators can define granular flow- and class-based policies, which apply a set of customizable security services, such as inspection engine policies, quality of service (QoS) policies, connection timers, and more, to each administrator-specified traffic flow or class. By combining these flexible access control and per-flow/per-class security services, powerful stateful inspection and application-aware firewall services, and multi-vector attack protection services that Cisco PIX Security Appliances deliver, businesses can enforce comprehensive security policies to protect themselves from attack.

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) other multimedia standards. This allows businesses to securely take advantage of the many benefits that converged data, voice, and video networks provide, including improved productivity, lower operational costs, and increased competitive advantage. By combining VPNs and Quality of Service (QoS) with the advanced protocol inspection services that Cisco PIX Security Appliances provide for these converged networking standards, businesses can securely extend voice and multimedia services and the benefits they deliver to remote offices, home offices, and mobile users.

Voice over IP and multimedia standards supported by Cisco PIX Security Appliances include 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), helping businesses secure deployments of a wide range of current and next-generation Voice over IP and multimedia applications. Cisco PIX Security Appliances also provide security services for Telephony Application Programming Interface (TAPI)-based and Java TAPI (JTAPI)-based applications when these applications use Computer Telephony Interface Quick Buffer Encoding (CTIQBE) as the network transport mechanism, such as the Cisco IP SoftPhone and the Cisco Customer Response Solution (CRS).

ROBUST IPSEC VPN SERVICES COST-EFFECTIVELY CONNECT NETWORKS AND MOBILE USERS

Using the new full-featured VPN capabilities of Cisco PIX Security Appliances, businesses can securely connect networks and mobile users worldwide across low-cost Internet connections. Solutions supported range from standards-based site-to-site VPN using the Internet Key Exchange (IKE) and IP Security (IPSec) VPN standards to the innovative Cisco Easy VPN remote-access capabilities found in Cisco PIX Security Appliances and other Cisco Systems security solutions—such as Cisco IOS® routers and Cisco VPN 3000 Series Concentrators. Cisco Easy VPN delivers a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture that eliminates the operational costs associated with maintaining the remote-device configurations typically required by traditional VPN solutions. Cisco Easy VPN provides feature-rich remote-access VPN services, including enforcing VPN client security posture requirements and performing automated software updates of Cisco VPN Clients, to deliver secure, easy-to-manage remote access to corporate networks. 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. Certain Cisco PIX Security Appliance models have integrated hardware VPN acceleration, delivering highly scalable, high-performance VPN services.

AWARD-WINNING RESILIENT ARCHITECTURE PROVIDES MAXIMUM BUSINESS UPTIME

Select Cisco PIX Security Appliance models provide award-winning stateful failover services that help ensure resilient network protection for enterprise network environments. Businesses can deploy Cisco PIX Security Appliances using either an Active/Standby failover design or a more advanced Active/Active failover design, which supports complex network environments that require asymmetric routing support. Failover pairs continuously synchronize their connection state and device configuration data, providing an easy-to-manage high-availability solution. Synchronization can take place over a high-speed LAN connection, providing another layer of protection by enabling businesses to geographically separate the failover pair. In the event of a system or network failure, network sessions are automatically transitioned between appliances, with complete transparency to users.

INTELLIGENT NETWORKING SERVICES ENABLE SIMPLIFIED DEPLOYMENT AND SEAMLESS NETWORK INTEGRATION

Cisco PIX Security Appliances take advantage of more than 20 years of Cisco networking leadership and innovation, and deliver a wide range of intelligent networking services for seamless integration into today's diverse network environments. Administrators can easily integrate Cisco PIX Security Appliances into switched network environments by taking advantage of native 802.1q-based VLAN support. Cisco IP phone deployments can benefit from the "zero-touch provisioning" services provided by Cisco PIX Security Appliances, which help the phones automatically register with the appropriate Cisco CallManager and download any additional configuration information and software images. Businesses can improve their overall network resiliency by taking advantage of the robust Open Shortest Path First (OSPF) dynamic routing services provided by Cisco PIX Security Appliances, which can detect network outages within seconds and route around them. Mission-critical real-time enterprise applications, collaborative computing applications, and streaming multimedia services can be securely delivered using the comprehensive Protocol Independent Multicast (PIM)-Sparse Mode v2 and bidirectional PIM routing support provided by Cisco PIX Security Appliances. Businesses can secure deployments of next-generation IPv6 networks using the advanced IPv6 security services provided by Cisco PIX Security Appliances, while securing existing IPv4 environments with the same appliances during the transition toward an IPv6 infrastructure.

FLEXIBLE MANAGEMENT SOLUTIONS LOWER OPERATIONAL COSTS

Cisco PIX Security Appliances deliver a wealth of configuration, monitoring, and troubleshooting options, giving businesses the flexibility to use the methods that best meet their needs. 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 provide up to 16 levels of customizable administrative roles, so that businesses can grant administrators and operations personnel the appropriate level of access to each appliance (monitoring-only access, read-only access to the configuration, network configuration only, or firewall configuration only, for example). Cisco PIX Security Appliances also include robust Auto Update capabilities, a set of secure remote-management services that help ensure that appliance configurations and software images are automatically kept up to date.

Next-Generation Centralized Management Solutions

Cisco PIX Security Appliances running Cisco PIX Security Appliance Software Version 7.0 can be centrally managed using the upcoming follow-up software release to CiscoWorks VPN/Security Management Solution (VMS) 2.3. This highly scalable, next-generation, three-tiered management solution includes:

- 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
- Intelligent discovery and optimization of security policies and object groups
- "Touchless" software image management for remote Cisco PIX Security Appliances
- Support for dynamically addressed appliances

Attack Mitigation and Event Monitoring Solutions

Network-based attacks can be easily and accurately identified, managed, and eliminated within commercial or enterprise environments using the Cisco Security Monitoring, Analysis, and Response System (CS-MARS) product family. CS-MARS appliances analyze and correlate security events, syslog, and NetFlow data from numerous desktop, server, and network security solutions to determine actual attack paths and provide mitigation options, simplifying security incident management for environments where dedicated security analysts may not be available.

Cisco also offers the CiscoWorks Security Information Management Solution (SIMS), which is well-suited for large enterprises and managed security services providers with dedicated security analysts that require in-depth data collection, forensic analysis, audit and compliance, and reporting for complex, multi-vendor networks.

World-Class Device Management Solutions

The integrated Cisco Adaptive Security Device Manager (ASDM) provides a world-class Web-based management interface that greatly simplifies the deployment, ongoing configuration, and monitoring of a single Cisco PIX Security Appliance—without requiring any software (other than a standard Web browser and Java plug-in) to be installed on an administrator's computer. Intelligent setup and VPN wizards provide easy integration into any network environment, while informative monitoring features, including a dashboard and real-time syslog viewer, provide vital device/network health status and event monitoring at a glance.

Alternatively, administrators can remotely configure, monitor, and troubleshoot their Cisco PIX Security Appliances using a command-line interface (CLI). Secure CLI access is available using several methods, including Secure Shell (SSHv2) Protocol, Telnet over IPSec, and out-of-band through a console port.

NEW FEATURES IN CISCO PIX SECURITY APPLIANCE SOFTWARE VERSION 7.0

Cisco PIX Security Appliance Software Version 7.0 provides a wealth of new features, including those detailed in Table 1. A complete list of features is available in the Cisco PIX Security Appliance Software Version 7.0 Release Notes.

Table 1. New Features and Benefits

Feature	Benefit
Advanced Firewall Services	
Cisco Modular Policy Framework	• Provides a powerful, highly flexible framework for defining flow- or class-based policies, enabling administrators to identify a network flow or class based on different conditions, and then apply a set of customizable services to each flow or class • Improves control over applications by introducing the ability to have flow- or class-specific firewall/inspection policies, QoS policies, connection limits/timers, and more
Advanced Web Security Services	• Debuts new deep inspection services for Web traffic, which provide granular control over HTTP sessions for improved protection from a wide range of Web-based attacks • Gives businesses precise control over what HTTP commands or methods can be used on a per-flow basis (different policy for traffic coming from Internet vs. traffic coming from a staging Web server to production Web server, for example), thus protecting businesses from a variety of Web-based attacks, including unauthorized deletion or modification of Web content • Delivers a wide range of additional powerful HTTP security services, including RFC compliance enforcement, protocol anomaly detection, protocol state tracking, response validation, MIME type validation and content control, and Uniform Resource Identifier (URI) length enforcement, and more

Feature	Benefit
Tunneling Application Control	• Introduces new inspection services to detect and optionally block instant messaging, peer-to-peer file sharing, and other applications tunneling through Web application ports • Blocks popular instant messaging applications such as AOL Instant Messenger, Microsoft Messenger, and Yahoo Messenger • Stops peer-to-peer file sharing applications such as KaZaA and Gnutella • Thwarts tunneling applications such as GoToMyPC
Security Contexts	• Enables creation of multiple security contexts (virtual firewalls) within a single Cisco PIX Security Appliance, with each context having its own set of security policies, logical interfaces, and administrative domains • Supports four licensed levels of security contexts: 5, 10, 20, and 50 (the maximum number of contexts supported is based on the Cisco PIX Security Appliance model) • Provides businesses a convenient way of consolidating multiple firewalls into a single physical appliance or failover pair, while retaining the ability to separately manage each of these virtual instances • Enables service providers to deliver resilient multitenant firewall services with a pair of redundant appliances
Layer 2 Transparent Firewall	• Supports deployment of a Cisco PIX Security Appliance in a secure Layer 2 bridging mode, providing rich Layer 2–7 firewall security services for the protected network while remaining “invisible” to devices on each side of it • Simplifies Cisco PIX Security Appliance deployments in existing network environments by not requiring businesses to readdress the protected networks • Supports creation of Layer 2 security perimeters by enforcing administrator defined Ethertype-based access control policies for Layer 2 network traffic
FTP Session Command Filtering	• Builds upon existing FTP inspection services provided by Cisco PIX Security Appliances, including protocol anomaly detection, protocol state tracking, NAT/Port Address Translation (PAT) support, and dynamic port opening and closing, to give administrators greater control over the use of numerous FTP commands, enforcing what operations users and groups can perform within FTP sessions (such as FTP gets and puts) • Introduces server obfuscation techniques and additional attack signatures to further protect FTP servers from attack
Extended Simple Mail Transport Protocol (ESMTP) E-mail Inspection Services	• Extends SMTP inspection engine to support ESMTP, providing security services that include protocol anomaly detection, protocol state tracking, and support for the following new commands introduced in ESTMP protocol: AUTH, DATA, EHLO, ETRN, HELO, HELP, MAIL, NOOP, QUIT, RCPT, RSET, SAML, SEND, SOML, and VRFY • Protects businesses from malicious SMTP and ESTMP commands with automatic command filtering
3G Mobile Wireless Security Services	• Delivers rich security services for 3G Mobile Wireless environments that provide packet switched data services using the General Packet Radio Service (GPRS) Tunneling Protocol standard (GTP) • Provides advanced GTP inspection services that enable Mobile Wireless providers to have secure interactions with roaming partners through robust filtering capabilities based on GTP specific parameters, such as International Mobile Subscriber Identity (IMSI) prefixes and access point name (APN) values, and more **Note:** This is a separately licensed feature

Feature	Benefit
Sun RPC/NIS+ Inspection Services	• Improves support for port-hopping UNIX applications through new stateful inspection and NAT services for Sun RPC and NIS+ sessions transactions that use Portmapper v2 or RPCBind v3/v4
Internet Control Message Protocol (ICMP) Inspection Services	• Enables secure usage of ICMP for troubleshooting and improved network performance by providing state tracking services for ICMP connections, as well as providing additional controls for ICMP error messages
Enhanced TCP Security Engine	• Introduces several new foundational capabilities to assist in detecting protocol and application-layer attacks • Provides TCP stream reassembly and analysis services to help detect attacks that are spread across a series of packets • Offers TCP traffic normalization services for additional techniques to detect attacks, including advanced flag and option checking, TCP packet checksum verification, detection of data tampering in retransmitted packets, and more
Outbound Access Control Lists (ACLs)	• Delivers improved flexibility for defining access control policies by adding support for outbound ACLs (in addition to existing inbound ACLs), allowing access controls to be enforced as network traffic enters or exits an interface
Time-Based ACLs	• Gives administrators greater control over resource usage by defining when certain ACL entries are active, with custom time ranges applied to selected ACLs
Enable/Disable Individual 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
Improved Websense URL Filtering Performance	• Delivers significantly enhanced scalability for concurrent URL filtering lookups with Websense Enterprise Employee Internet Management (EIM) solutions
Voice over IP and Multimedia Security Services	
T.38 Fax Over IP (FoIP)	• Enhances H.323 inspection services to include support for the T.38 protocol, an ITU standard that defines how to transmit FoIP in real time
Gatekeeper Routed Control Signaling (GKRCS)	• Extends H.323 inspection services to support GKRCS, in addition to the Direct Call Signaling method (DCS) method currently supported • Enables Cisco PIX Security Appliances to support call signaling messages exchanged directly between H.323 gatekeepers
Fragmented and Segmented Multimedia Stream Inspection	• Introduces inspection of H.323, SIP, and SCCP-based voice and multimedia streams that have been fragmented or segmented
MGCP Address Translation Services	• Builds upon rich MGCP security services provided by Cisco PIX Security Appliances, adding NAT/PAT-based address translation services for MGCP-based connections between media gateways and call agents or media gateway controllers
RTSP Address Translation Services	• Delivers NAT-based address translation services for RTSP media streams for improved support in diverse networking environments

Feature	Benefit
Robust IPSec VPN Services	
VPN Client Security Posture Enforcement	• Introduces the ability to perform VPN client security posture checks when a VPN connection attempt is received, including enforcing usage of authorized host-based security products (such as the Cisco Security Agent) and verifying their version numbers and status prior to allowing remote users to access the corporate network
VPN Client Blocking by Operating System and Type	• Adds the ability to restrict the different types of VPN clients (software client, router, VPN 3002, or Cisco PIX, for example) that are allowed to connect based on the type of client, operating system installed, and version of VPN client software • Supports restricting or preventing access to noncompliant VPN clients
Automatic VPN Client Software Updates	• Introduces support for automatic software updates of Cisco VPN clients and Cisco VPN 3002 hardware clients, with the ability to trigger updates when VPN connections are established, or on-demand for currently connected VPN clients
Improved Support for Non-Split Tunneling Remote-Access VPN Environments	• Enables remote-access VPN connections to be terminated on the outside interface of a Cisco PIX Security Appliance, allowing Internet-destined traffic from remote-access user VPN tunnels to leave through the same interface it arrived at (after firewall rules, URL filtering policies, and other security checks have been optionally applied)
Enhanced VPN NAT Transparency	• 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 • 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
Native Integration with Popular User Authentication Services	• Provides convenient method for authenticating VPN users through native integration with popular authentication services, including Microsoft Active Directory, Microsoft Windows Domains, Kerberos, Lightweight Directory Access Protocol (LDAP), and RSA SecurID (without requiring a separate RADIUS/TACACS+ server to act as an intermediary)
OSPF Dynamic Routing over VPN Tunnels	• Extends comprehensive OSPF dynamic routing services to support neighbors across IPSec VPN tunnels, providing improved network reliability for VPN connected networks • Supports OSPF reverse-route injection for improved network performance and reliability
Enhanced Spoke-to-Spoke VPN Support	• Improves support for spoke-to-spoke VPN communications, when a Cisco PIX Security Appliance is acting as a hub, by allowing VPN traffic to enter and leave through the same interface
Enhanced X.509 Certificate Support	• Introduces the ability to manually enroll into X.509 certificate authorities through support for Public Key Cryptography Standard (PKCS) #10 formatted certificate requests • Supports manually importing certificates using PKCS #7, and importing certificates with private keys using PKCS #12 • Enables deployment in environments with a multilevel certificate authority hierarchy through support for n-tier certificate chaining • Extends RSA key support to sizes ranging up to 4096 bits • Adds support for DSA (Digital Signature Algorithm)-based X.509 certificates with key sizes ranging up to 1024 bits

Feature	Benefit
Cisco IOS Software Certificate Authority Support	• Introduces support for online enrollment into the new certificate authority in Cisco IOS Software, a lightweight X.509 certificate authority that simplifies the rollout of public key infrastructure (PKI)-enabled site-to-site VPNs
High Availability Services	
Active/Active Stateful Failover	• Provides a complementary solution to award-winning Cisco PIX Security Appliance Active/Standby failover, where both systems in an Active/Active failover pair actively pass network traffic simultaneously—effectively doubling the throughput of the failover pair for bursty network traffic conditions • Supports bidirectional state sharing between Active/Active failover pair members for support of advanced network environments with asymmetric routing topologies, allowing flows to enter through one Cisco PIX Security Appliance and exit through the other, if required **Note:** This feature is only available on Unrestricted and Failover-Active/Active models only; upgrade licenses can be purchased to convert Failover models to Failover-Active/Active models
VPN Stateful Failover	• Maximizes VPN connection uptime with new Active/Standby stateful failover for VPN connections • Synchronizes all security association state information and session key material between failover pair members, providing a highly resilient VPN solution **Note:** This feature is available on Unrestricted, Failover, and Failover-Active/Active models only
Improved Failover Transition Times	• Introduces support for subsecond failover for environments using serial-cable-based failover, and three-second failover for environments using LAN-based failover, through support for more granular control over heartbeat/state sharing intervals between failover partners
Zero-Downtime Software Upgrades	• Enables businesses to perform software maintenance release upgrades on Cisco PIX Security Appliance failover pairs without affecting network uptime or connections, through the support of state sharing between mixed Cisco PIX Security Appliance Software versions (running Version 7.0(1) or higher)
Intelligent Networking Services	
PIM Multicast Routing	• Streamlines the delivery of multimedia traffic in videoconferencing, collaborative computing, and mission-critical real-time enterprise applications through full PIM-Sparse Mode v2 and bidirectional PIM routing support (based on Cisco IOS multicast technology)
QoS Services	• Delivers per-flow, policy-based QoS services, with support for Low-Latency Queuing (LLQ) and traffic policing for prioritizing latency-sensitive network traffic and limiting bandwidth usage of administrator-specified applications • Enables businesses to have end-to-end QoS policies for their extended networks
IPv6 Networking	• Provides access control and deep inspection firewall services for native IPv6 network environments and mixed IPv4/IPv6 network environments through dual-stack support • Delivers IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and UDP • Supports SSHv2, Telnet, HTTP/Secure HTTP (HTTPS), and ICMP-based management over IPv6

Feature	Benefit
Common Security Level for Multiple Interfaces	• Extends the Cisco PIX Security Appliance interface security-level concept to allow multiple interfaces to share a common security level • Simplifies deployment of Cisco PIX Security Appliances in intranet environments by allowing administrators to define custom security policies for traffic flowing between interfaces at the same security level, without any type of automatic traffic flow being intrinsically permitted
Improved VLAN Capacity	• Increases the number of 802.1q VLAN-based virtual interfaces supported on Cisco PIX Security Appliances for improved port density on each platform • Enables businesses to further segment their networks into different security zones for improved security • Supports up to 25 VLANs on Cisco PIX 515 and 515E Security Appliances, up to 100 VLANs on Cisco PIX 525 Security Appliances, and up to 150 VLANs on Cisco PIX 535 Security Appliances
Optional Address Translation Services	• Simplifies deployment of Cisco PIX Security Appliances by eliminating the 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
Flexible Management Solutions	
Improved SNMP Monitoring	• Introduces support for SNMPv2c, providing increased visibility into the status of Cisco PIX Security Appliances • Provides new services such as 64-bit counters (for improved monitoring of Gigabit Ethernet interfaces) and support for bulk MIB data transfers • Adds support for many additional SNMP MIBs, including the SNMPv2 MIB (RFC 1907), the Interfaces Group MIB (RFCs 1573 and 2233), the IP MIB (RFC 2011), and the Entity MIB (RFC 2737) • Provides complete visibility into VPN connections with detailed per-tunnel statistics, including tunnel uptime, bytes/packets transferred, and more, through support for the Cisco IPSec Flow Monitoring MIB
SSHv2 and Secure Copy Protocol (SCP)	• Adds support for using SSHv2 to remotely manage Cisco PIX Security Appliances, providing improved compatibility with third-party SSH tools • Introduces SCP support as another secure method for transferring files, such as configuration and software images, to and from Cisco PIX Security Appliances
Storage of Multiple Configurations in Flash Memory	• Enables administrators to perform configuration rollback through the introduction of a new Flash file system and the ability to store and use multiple configurations in Flash
Secure Asset Recovery	• Prevents unauthorized access to sensitive configuration data, certificates, and key material stored on Cisco PIX Security Appliances by automatically wiping Flash contents in the event of an asset recovery/password reset procedure, if preconfigured to do so
Scheduled System Reloads	• Allows administrators to schedule a reload on a Cisco PIX Security Appliance either at a specific time or at an offset from the current time, making it simpler to schedule network downtime and notify remote-access VPN users of an impending reboot

Feature	Benefit
Dedicated Out-of-Band Management Interface	• Enables businesses to implement the best practice of using out-of-band management for their Cisco PIX Security Appliances, as described in the SAFE Blueprint from Cisco, through the new ability to designate a specific interface to only act as an out-of-band management interface
Enhanced ICMP Ping Services	• Delivers useful new troubleshooting methods through added support for IPv6 addresses and extended ICMP options, including data pattern, df-bit, repeat count, datagram size, timeout interval, verbose output, and sweep range of sizes
CLI Usability Enhancements	• Enhances the Cisco PIX Security Appliance CLI user experience by incorporating many popular Cisco IOS command-line services such as command completion, context-sensitive help, and aliasing
SMTP E-mail Alerts	• Provides a convenient method for alerting administrators when critical events are encountered, by sending e-mail alert messages to administrator-defined e-mail addresses
Administrative TACACS+ Accounting	• Introduces the ability to generate TACACS+ authentication, authorization, and accounting (AAA) records for tracking administrative access to Cisco PIX Security Appliances, as well as tracking all configuration changes that are made during an administrative session—complementing the existing syslog support for administrative logging that Cisco PIX Security Appliances already support
RADIUS Accounting to Multiple Servers	• Adds support for sending accounting information to multiple RADIUS servers simultaneously

TECHNICAL SPECIFICATIONS

Tables 2–4 provide information on compatibility between Cisco PIX Security Appliances and VPN clients, VPN products, and certain cryptographic standards.

Cisco VPN Client Compatibility

Cisco PIX Security Appliances support numerous software- and hardware-based Cisco VPN clients, including those listed in Table 2.

Table 2. Compatibility Between Cisco PIX Security Appliances and VPN Clients

Cisco VPN Client	Supported Software Versions
Software IPSec VPN Clients	• Cisco VPN Client for Windows, Version 3.6 and later • Cisco VPN Client for Linux, Version 3.6 and later • Cisco VPN Client for Solaris, Version 3.6 and later • Cisco VPN Client for Mac OS X, Version 3.6 and later
Hardware IPSec VPN clients (Cisco Easy VPN Remote)	• 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 Software versions 6.2 and 6.3

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:

Table 3. Site-to-Site VPN Compatibility Between Cisco PIX Security Appliances and VPN Products

Cisco VPN Product	Supported Software Versions
Cisco IOS Routers	Cisco IOS Software Release 12.1(6)T and later
Cisco PIX Security Appliances	Cisco PIX Security Appliance Software Version 6.0(1) and later
Cisco VPN 3000 Concentrators	Cisco VPN 3000 Concentrator Software Version 3.0 and later

Cryptographic Standards Supported

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

Table 4. Cryptographic Standards and Products Supported by Cisco PIX Security Appliances

Cryptographic Standards and Products	Description
Asymmetric (Public Key) Encryption Algorithms	• RSA public/private key pairs, 512 to 4096 bits • DSA public/private key pairs, 512 to 1024 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 • Group 7: 163 bits (Elliptic Curve Diffie-Hellman)
Hash Algorithms	• MD5: 128 bits • SHA-1: 160 bits
X.509 Certificate Authorities	• Baltimore UniCERT • Cisco IOS Software • Entrust Authority • iPlanet/Netscape CMS • Microsoft Certificate Services • RSA KEON • VeriSign OnSite
X.509 Certificate Enrollment Methods	• Simple Certificate Enrollment Protocol (SCEP) • Manual (PKCS #7 and #10)

SYSTEM REQUIREMENTS

Table 5 lists system requirements for Cisco PIX Security Appliances running Cisco PIX Security Appliance Software Version 7.0.

Table 5. System Requirements

System Requirement	Description
Platforms Supported	• Cisco PIX 515 Security Appliance • Cisco PIX 515E Security Appliance • Cisco PIX 525 Security Appliance • Cisco PIX 535 Security Appliance
Minimum RAM	**Cisco PIX 515/515E Security Appliance** • 64 MB on Restricted models • 128 MB Unrestricted, Failover, and Failover-Active/Active models **Note:** This release requires more memory for Cisco PIX 515/515E Security Appliances than previous software releases—a memory upgrade may be required
	Cisco PIX 525 Security Appliance • 128 MB on Restricted models • 256 MB on Unrestricted, Failover, and Failover Active/Active models
	Cisco PIX 535 Security Appliance • 512 MB on Restricted models • 1024 MB on Unrestricted, Failover, and Failover-Active/Active models
Minimum Flash Memory	• 16 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) • VPN Acceleration Card+ (VAC+)

PRODUCT ORDERING INFORMATION

Table 6 lists ordering information for the Cisco PIX Security Appliance Software.

Table 6. Ordering Information

Part Number	Description
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 Adaptive Security Device Manager: http://www.cisco.com/go/asdm

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 Adaptive Security 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.
168 Robinson Road
#28-01 Capital Tower
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 Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus 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

204177.u_ETMG_MH_2.05

Printed in the USA