



Data Sheet

Cisco PIX Security Appliance Software Version 7.1

PRODUCT OVERVIEW

The market-leading Cisco® PIX® Security Appliance Series delivers robust user and application policy enforcement, multivector 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 IP Security (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.

Multivector Attack Protection

Cisco PIX security appliances incorporate multivector 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 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 Cisco's powerful Modular Policy Framework, 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. With this combination of flexible access control and per-flow/per-class security services, powerful stateful inspection and application-aware firewall services, and multivector attack protection services, 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 VoIP and 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 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.

VoIP 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 VoIP 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.

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 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 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 smooth integration into today's diverse network environments. Network integration services include:

- **Layer 2 transparent firewall**—Provides the ability to rapidly deploy Cisco PIX security appliances into existing networks without requiring any addressing changes, delivers high-performance stealth Layers 2–7 security services, and provides protection against network-layer attacks with integration in complex routing, high-availability, and multicast environments.
- **Services virtualization**—Enables the logical partitioning of a single Cisco PIX security appliance into multiple virtual firewalls, each with its own unique policies and administration. This capability is ideal for enterprises consolidating multiple firewalls into a single Cisco PIX security appliance, or for service providers that offer managed firewall or hosting services.
- **Standard 802.1q-based VLAN support**—Provides easy integration into switched network environments.
- **Open Shortest Path First (OSPF) dynamic routing services**—Improves networking resiliency by detecting network outages within seconds, and routing around them.
- **Protocol Independent Multicast (PIM) Sparse Mode v2 and bidirectional PIM routing support**—Provides secure delivery of mission-critical real-time enterprise applications, collaborative computing applications, and streaming multimedia services.
- **IPv6 support**—Allows secure deployment of next-generation IPv6 networks, as well as hybrid environments that require simultaneous, dual-stack support of IPv4 and IPv6.
- **QoS**—Low-Latency Queuing (LLQ) and traffic policing features support applications with demanding QoS requirements, such as voice or video, helping ensure an end-to-end network QoS policy. Latency-sensitive traffic can be prioritized ahead of file transfer and other more delay-tolerant traffic.
- **IP phone “zero-touch provisioning” services**—Simplifies IP phone deployments by helping the phones register with the correct Cisco CallManager systems and download any additional configuration information and software images.

FLEXIBLE MANAGEMENT SOLUTIONS LOWER OPERATIONS 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 can be centrally managed using the Cisco Security Management Suite. This suite combines the new Cisco Security Manager with the Cisco Security Monitoring, Analysis, and Response System, providing highly scalable, enterprise-class management and monitoring. Cisco Security Manager delivers best-in-class configuration management of firewall, VPN, and intrusion prevention system (IPS) security services across Cisco security appliances, Cisco routers, and Cisco Catalyst® switch services modules. Cisco Security Manager provides:

- 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 MARS solution. Cisco Security MARS appliances analyze and correlate security events, syslog, and NetFlow data from a wide variety of desktop, server, and network security solutions to determine the actual attack path and provide mitigation options, thus simplifying security incident management for environments where dedicated security analysts may not be available.

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 management through a console port.

FEATURES AND BENEFITS OF CISCO PIX SECURITY APPLIANCE SOFTWARE VERSION 7.1

Cisco PIX Security Appliance Software Version 7.1 provides several new features, including those detailed in Table 1. A complete list of features is available in the Cisco PIX Security Appliance Software Version 7.1 Release Notes.

Table 1. Features and Benefits of Cisco PIX Security Appliance Software Version 7.1

Feature	Benefit
Advanced Firewall Services	
Per-Host Connection Limits	Provides new denial of service mitigation capabilities through the ability to enforce limits on the number of concurrent connections and embryonic connections on a per-host basis. These new features complement the existing maximum connection and maximum embryonic connection limits that are applied to overall traffic attempting to traverse the appliance.
VoIP and Multimedia Security Services	
RTSP PAT Support	Delivers Port Address Translation (PAT) services for Real-Time Streaming Protocol (RTSP) streaming media services, such as Apple Quicktime 7 and mobile devices subscribed to PacketVideo streaming services.
Flexible Management Solutions	
Syslog to ACL Entry Correlation	Introduces powerful policy tuning and troubleshooting capabilities through the ability to correlate which specific access control list (ACL) entry is responsible for generating a particular syslog event. This enables businesses to easily identify which ACL may need to be edited to either permit or deny traffic to flow, depending on the situation.

PRODUCT 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	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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 Cisco VPN products listed in Table 3 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 ASA 5500 Series Appliances	Cisco ASA Software Version 7.0.1 and later
Cisco IOS Software-Based 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 Series 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 (Table 4).

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

Cryptographic Standards and Products	Description
Asymmetric (Public Key) Encryption Algorithms	<ul style="list-style-type: none"> • RSA public/private key pairs, 512 to 4096 bits • DSA public/private key pairs, 512 to 1024 bits
Symmetric Encryption Algorithms	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • Group 1: 768 bits • Group 2: 1024 bits • Group 5: 1536 bits • Group 7: 163 bits (Elliptic Curve Diffie-Hellman)
Hash Algorithms	<ul style="list-style-type: none"> • Message Digest Algorithm 5 (MD5): 128 bits • Secure Hash Algorithm 1 (SHA-1): 160 bits
X.509 Certificate Authorities	<ul style="list-style-type: none"> • Baltimore UniCERT • Cisco IOS Software • Entrust Authority • iPlanet/Netscape CMS • Microsoft Certificate Services • RSA KEON • VeriSign OnSite

X.509 Certificate Enrollment Methods	<ul style="list-style-type: none"> • 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 7.1.

Table 5. System Requirements

System Requirement	Description
Platforms Supported	<ul style="list-style-type: none"> • Cisco PIX 515 Security Appliance • Cisco PIX 515E Security Appliance • Cisco PIX 525 Security Appliance • Cisco PIX 535 Security Appliance
Minimum RAM	<p>Cisco PIX 515/515E Security Appliance</p> <ul style="list-style-type: none"> • 64 MB on Restricted models • 128 MB Unrestricted, Failover, and Failover-Active/Active models <p>Note: This release requires more memory for Cisco PIX 515/515E security appliances than Cisco PIX Security Appliance Software Version 6.x—a memory upgrade may be required.</p> <p>Cisco PIX 525 Security Appliance</p> <ul style="list-style-type: none"> • 128 MB on Restricted models • 256 MB on Unrestricted, Failover, and Failover Active/Active models <p>Cisco PIX 535 Security Appliance</p> <ul style="list-style-type: none"> • 512 MB on Restricted models • 1024 MB on Unrestricted, Failover, and Failover- Active/Active models
Minimum Flash Memory	16 MB
Expansion Cards Supported	<ul style="list-style-type: none"> • 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+)

ORDERING INFORMATION

To place an order, visit the [Cisco Ordering Home Page](#) or refer to Table 6.

Table 6. Ordering Information

Product Name	Part Number
Cisco PIX Security Appliance Software one-time upgrade for customers without a current Cisco SMARTnet® support contract	PIX-SW-UPGRADE=

TO DOWNLOAD THE SOFTWARE

Visit the [Cisco Software Center](#) to download Cisco PIX Security Appliance Software (Table 7). This requires log-in.

Table 7. Software Images for the Cisco PIX Family

Product Name
Cisco PIX Security Appliance Software Version 7.1
Cisco Adaptive Security Device Manager Version 5.1

SERVICE AND SUPPORT

Cisco offers a wide range of services programs to accelerate customer success. These innovative service programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, refer to [Cisco Technical Support Services](#) and [Cisco Advanced Services](#).

FOR MORE INFORMATION

For more information, visit the following links:

- **Cisco PIX Security Appliances:** <http://www.cisco.com/go/pix>
- **Cisco ASDM:** <http://www.cisco.com/go/asdm>
- **Cisco Security Manager:** <http://www.cisco.com/go/csmanager>
- **Cisco Secure Access Control Server (ACS):** <http://www.cisco.com/go/acs>
- **SAFE Blueprint from Cisco:** <http://www.cisco.com/go/safe>



Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0705R)