Cisco PIX 506E Security Appliance

The Cisco® PIX® 506E Security Appliance delivers enterprise-class security for remote office, branch office, and small-to-medium business (SMB) networks, in a high-performance, easy-to-deploy purpose-built appliance. Its unique desktop design supports two 10/100 Fast Ethernet interfaces and two 802.1q-based virtual interfaces, making it an exceptional choice for businesses requiring a cost-effective security solution with DMZ support. Part of the market-leading Cisco PIX Security Appliance Series, the Cisco PIX 506E Security Appliance provides a wide range of rich, integrated security services, advanced networking services, and powerful remote management capabilities in a compact, all-in-one security solution.

Figure 1. Cisco PIX 506E Security Appliance

Enterprise-Class Security

The Cisco PIX 506E Security Appliance provides delivers a multilayered defense for remote office, branch office, and small-to-medium business network environments through rich, integrated security services including stateful inspection firewall services, advanced application and protocol inspection, site-to-site and remote access VPN, in-line intrusion prevention, and robust multimedia and voice security—all in a single, integrated solution.

Cisco PIX Security Appliances incorporate the state-of-the-art Cisco Adaptive Security Algorithm, which provides stateful inspection firewall services by tracking the state of all authorized network communications and by preventing unauthorized network access. As an additional layer of security, Cisco PIX Security Appliances integrate over two dozen purpose-built inspection engines that perform in-depth Layers 4–7 inspection of network traffic flows for many of today's popular applications and protocols. To defend networks from application-layer attacks and to give businesses more control over applications and protocols in their environments, these inspection engines combine extensive application and protocol knowledge with security enforcement technologies that range from protocol conformance checking, application and protocol state tracking, Network Address Translation (NAT) services, and attack detection and mitigation techniques such as protocol field length checking and URL length checking.

Administrators can easily create custom security policies using the many flexible access control technologies provided by Cisco PIX Security Appliances including network and service object groups, turbo access control lists (ACLs), user- and group-based policies, and more than 100 predefined applications and protocols. By combining these flexible access control technologies with the powerful stateful inspection firewall services and advanced application and protocol inspection services that Cisco PIX Security Appliances provide, businesses can easily enforce their network security policies and protect their networks from attack.

Market-Leading VoIP Security Services Protect Next-Generation Converged Networks

Cisco PIX Security Appliances provide market-leading protection for a wide range of voice-over-IP (VoIP) and multimedia standards, enabling businesses to securely take advantage of the many benefits that converged data, voice, and video networks deliver. By combining VPN 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 to remote office environments for lower total cost of ownership, improved productivity, and increased competitive advantage.

Flexible VPN Services Extend Networks Economically to Remote Offices and Mobile Users

Using the full-featured VPN capabilities of the Cisco PIX 506E Security Appliance, businesses can securely extend their networks across low-cost Internet connections to mobile users, business partners, and remote offices worldwide. 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 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, easy-to-manage remote-access VPN architecture that eliminates the operational costs associated with maintaining the remote-device configurations that are typically required by traditional VPN solutions. 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.

Integrated Intrusion Prevention Guards Against Popular Internet Threats

The integrated in-line intrusion prevention capabilities of the Cisco PIX 506E Security Appliance can protect remote office, branch office, and small-to-medium business networks from many popular forms of attacks, including Denial-of-Service (DoS) attacks and malformed packet attacks. Using a wealth of advanced intrusion-prevention 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 provide real-time notification to administrators.

Rich Network Integration Improves Network Resiliency and Simplifies Deployment

Cisco PIX Security Appliances include a variety of advanced networking features for smooth integration into today's diverse enterprise 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 phones 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. Companies can also 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.

Robust Remote-Management Solutions Lower Total Cost of Ownership

The Cisco PIX 506E Security Appliance is a reliable, easy-to-maintain platform that provides numerous configuration, monitoring, and troubleshooting methods. Management solutions range from centralized policy-management tools to integrated, Web-based management to support for remote monitoring standards such as Simple Network Management Protocol (SNMP) and syslog.

Administrators can easily manage a large number of remote Cisco PIX Security Appliances using the CiscoWorks VPN/Security Management Solution (VMS). This suite consists of several integrated software 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 configuration inheritance based on "Smart Rules"
- 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

Additionally, Cisco offers the CiscoWorks Security Information Management Solution (SIMS), a highly scalable security event management solution that collects, analyzes, and correlates security event data from across the enterprise—enabling you to identify and respond to high priority security events as they occur.

The integrated Cisco PIX Device Manager provides an intuitive, Web-based management interface that greatly simplifies the deployment, ongoing configuration, and monitoring of a Cisco PIX 506E Security Appliance—without requiring any software (other than a standard Web browser) 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 real-time dashboard, provide vital device and network health details at a glance.

Alternatively, administrators can remotely configure, monitor, and troubleshoot their Cisco PIX 506E Security Appliances using a command-line interface (CLI). Secure CLI access is available using several methods, including Secure Shell (SSH) Protocol, Telnet over IPSec, and out of band through a console port.

Table 1. Product Features and Benefits

Feature	Benefit
Enterprise-Class Security	
Reliable, purpose-built security appliance	• Uses a proprietary, hardened operating system that eliminates the security risks associated with general-purpose operating systems • Combines Cisco product quality with no moving parts to provide a highly reliable security platform
Stateful inspection firewall	• Provides perimeter network security to prevent unauthorized network access • Uses state-of-the-art Cisco Adaptive Security Algorithm for robust stateful inspection firewall services • Provides flexible access-control capabilities for more than 100 predefined applications, services, and protocols, with the ability to define custom applications and services • Simplifies management of security policies by giving administrators the ability to create re-usable network and service object groups that can be referenced by multiple security policies, simplifying initial policy definition and on-going policy maintenance
Advanced application and protocol inspection	• Integrates over two dozen specialized inspection engines for protocols such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Domain Name System (DNS), Simple Network Management Protocol (SNMP), SQL*Net, Network File System (NFS), H.323 Versions 1–4, Session Initiation Protocol (SIP), Cisco Skinny Client Control Protocol (SCCP), Real-Time Streaming Protocol (RTSP), Internet Locator Service (ILS), and many more
Cisco Easy VPN Remote (hardware VPN client)	• Enables dramatically simplified VPN rollouts to remote office and branch office environments by eliminating the provisioning complexities of traditional site-to-site VPN deployments • Downloads VPN policy dynamically from a Cisco Easy VPN Server upon connection, ensuring the latest corporate security policies are enforced • Provides robust client-side VPN resiliency with support for up to 10 Cisco Easy VPN Servers with automatic failover, in addition to Dead Peer Detection (DPD) support • Supports optional authentication of 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) • Extends VPN reach into environments using NAT or Port Address Transmitter (PAT), via support of Internet Engineering Task Force (IETF) UDP-based draft standard for NAT traversal • Supports both split and non-split tunneling environments • Provides intelligent, transparent DNS proxy capabilities for access to both corporate and public DNS servers
Cisco Easy VPN Server	• Provides remote access VPN concentrator services for up to 25 remote software- or hardware-based VPN clients • Pushes VPN policy dynamically to Cisco Easy VPN Remote-enabled solutions (such as the Cisco VPN Client) upon connection, helping to ensure that the latest corporate security policies are enforced • Extends VPN reach into environments using NAT or PAT, via support of IETF UDP-based draft standard for NAT traversal
Cisco VPN Client	• Includes a free unlimited license for the highly acclaimed, industry-leading Cisco VPN Client • Available on wide-range of platforms, including Microsoft Windows 98, ME, NT, 2000, and XP; Sun Solaris; Intel-based Linux distributions; and Apple Macintosh OS X • Provides many innovative features including dynamic security policy downloading from Cisco Easy VPN Server-enabled products, automatic failover to backup Easy VPN Servers, administrator customizable distributions, and more • Integrates with the award-winning Cisco Security Agent (CSA) for comprehensive endpoint security
Site-to-site VPN	• Supports IKE and IPSec VPN standards • Extends networks securely over the Internet by helping to ensure data privacy, data integrity, and strong authentication with remote networks and remote users • Supports 56-bit DES, 168-bit 3DES, and up to 256-bit AES data encryption to ensure data privacy
Intrusion prevention	• Provides protection from more than 55 different types of popular network-based attacks ranging from malformed packet attacks to DoS attacks • Integrates with Cisco Network Intrusion Detection System (IDS) sensors to identify and dynamically block/shun hostile network nodes
Authentication, authorization, and accounting (AAA) support	• Integrates with popular AAA services via TACACS+ and RADIUS • Provides tight integration with Cisco Secure Access Control Server (ACS) for user and administrator authentication, dynamic per-user/per-group policies, and administrator access privileges
X.509 certificate and CRL support	• Supports Simple Certificate Enrollment Protocol (SCEP)-based enrollment with leading X.509 solutions from Baltimore, Entrust, Microsoft, and VeriSign

Feature	Benefit
Integration with leading third-party solutions	• Supports Cisco AVVID (Architecture for Voice, Video and Integrated Data) partner solutions that provide URL filtering, content filtering, virus protection, scalable remote management, and more
Industry certifications and evaluations	• Earned numerous leading industry certifications and evaluations, including: ◦ Common Criteria Evaluated Assurance Level 4 (EAL4) ◦ FIPS 140-2, Level 2 Validation
Robust Remote Office and Branch Office Networking	
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, with support for multiple VLAN trunks per Cisco PIX Security Appliance • Supports up to 2 VLANs on a Cisco PIX 506E Security Appliance, providing a low-cost DMZ-enabled security solution that enables businesses to securely host Web servers, e-mail servers, and other services with the Internet or extranet environments
OSPF dynamic routing	• Provides comprehensive OSPF dynamic routing services 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 NAT through tight integration with Cisco PIX Security Appliance NAT services • Supports MD5-based OSPF authentication in addition to plain-text 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
Dynamic Host Configuration Protocol (DHCP) client and server	• Obtains IP address for outside interface of appliance automatically from service provider • Provides DHCP server services on one or more interfaces, allowing devices to obtain IP addresses dynamically • Includes extensions for support of Cisco IP phones and Cisco SoftPhone IP telephony solutions
DHCP relay	• Forwards DHCP requests from internal devices to an administrator-specified DHCP server, enabling centralized distribution, tracking and maintenance of IP addresses
NAT/PAT support	• Provides dynamic, static, and policy-based NAT, and PAT services • Allows multiple users to share a single broadband connection using a single public IP address
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
PPPoE	• Ensures compatibility with networks that require PPP over Ethernet (PPPoE) support
Rich Management Capabilities	
CiscoWorks VMS	• Provides a comprehensive management suite for large scale Cisco security product deployments • Integrates policy management, software maintenance, and security monitoring in a single management console
Cisco PIX Device Manager (PDM)	• Intuitive, Web-based GUI enables simple, secure remote management of Cisco PIX Security Appliances • Provides a wide range of informative, real-time, and historical reports which give critical insight into usage trends, performance baselines, and security events
Auto Update	• Provides “touchless” secure remote management of Cisco PIX Security Appliance configuration and software images via a unique “push/pull” management model • Next-generation secure Extensible Markup Language (XML) over HTTPS management interface can be used by Cisco and third-party management applications for remote Cisco PIX Security Appliance configuration management, inventory, software image management/deployment, and monitoring • Supports dynamically addressed appliances in addition to appliances with static IP addresses • Integrates with Management Center for Firewalls and Auto Update Server for robust, scalable remote management of up to 1000 Cisco PIX Security Appliances (per management server)

Feature	Benefit
Cisco PIX CLI	• Allows customers to use existing Cisco IOS Software CLI knowledge for easy installation and management without additional training • Accessible through numerous methods including console port, Telnet, and SSH
Command-level authorization	• Gives businesses the ability to create up to 16 customizable administrative roles/profiles for managing a Cisco PIX Security Appliance (monitoring only, read-only access to configuration, VPN administrator, firewall/NAT administrator, etc.) • Uses either the internal administrator database or outside sources via TACACS+, such as Cisco Secure ACS
SNMP and syslog support	• Provide remote monitoring and logging capabilities, with integration into Cisco and third-party management applications

Table 2. Product Specifications

Feature	Specifications
Software Licenses	• 3DES/AES and DES Encryption Licenses ◦ The Cisco PIX 506E Security Appliance has two optional encryption licenses—one license (PIX-506-SW-3DES) enables 168-bit 3DES and up to 256-bit AES encryption, the other license (PIX-VPN-DES) enables 56-bit DES encryption. Both are available either at the time of ordering the Cisco PIX 506E Security Appliance, or can be obtained subsequently through Cisco.com. Note that an encryption license must be installed to activate encryption services which are required before using certain features including VPN and secure remote management.
Performance Summary	• Cleartext throughput: Up to 100 Mbps • Concurrent connections: 25,000 • 56-bit DES IPSec VPN throughput: Up to 20 Mbps • 168-bit 3DES IPSec VPN throughput: Up to 16 Mbps • 128-bit AES IPSec VPN throughput: Up to 30 Mbps • 256-bit AES IPSec VPN throughput: Up to 25 Mbps • Simultaneous VPN peers: 25* * Maximum number of simultaneous site-to-site or remote access IKE Security Associations (SAs) supported
Technical Specifications	• Processor: 300-MHz Intel Celeron Processor • Random access memory: 32 MB of SDRAM • Flash memory: 8 MB • Cache: 128 KB level 2 at 300 MHz • System bus: Single 32-bit, 33-MHz PCI
Environmental Operating Ranges	• Operating ◦ Temperature: 23 to 104°F (–5 to 40°C) ◦ Relative humidity: 10 to 95 percent, noncondensing ◦ Altitude: 0 to 6500 feet (2000 m) ◦ Shock: 250 G, < 2 ms ◦ Vibration: 0.41 Grms2 (5 to 500 Hz) random input • Nonoperating ◦ Temperature: –13 to 158°F (–25 to 70°C) ◦ Relative humidity: 10 to 95 percent, noncondensing ◦ Altitude: 0 to 15000 feet (4570 m) ◦ Shock: 60 G, 11 ms ◦ Vibration: 0.41 Grms2 (5 to 500 Hz) random input
Power	• Autoswitching: 100V to 240V RMS • Current: 0.7 – 0.4A • Frequency: 50–60 Hz, single phase • Heat dissipation PIX 506E chassis: 102.4 BTU/hr, full power usage (30W) • Heat dissipation PIX 506E plus power adapter: 204.6 BTU/hr, full power usage (60 VA)
Physical Specifications	• Dimensions and Weight Specifications ◦ Dimensions (H x W x D): 1.72 x 8.5 x 11.8 in. (4.37 x 21.59 x 29.97 cm) ◦ Weight: 6 lb (2.71 kg) • Interfaces ◦ Console port: RS-232, 9600 bps, RJ-45 ◦ Outside: Integrated 10/100 Fast Ethernet port, auto-negotiate (half/full duplex), RJ-45 ◦ Inside: Integrated 10/100 Fast Ethernet port, auto-negotiate (half/full duplex), RJ-45

Feature	Specifications
Regulatory and Standards Compliance	• Regulatory Compliance ◦ Products bear CE Marking indicating compliance with the 89/366/EEC and 73/23/EEC directives, which includes the following safety and EMC standards. • Safety ◦ UL 1950, CAN/CSA-C22.2 No. 950, EN 60950, IEC 60950, IEC 60825-1, IEC 60825-2, EN 60825-1, EN 60825-2, 21 CFR 1040 • Electromagnetic Compatibility (EMC) ◦ FCC Part 15 (CFR 47) Class A, ICES-003 Class A, EN55022 Class A with UTP Class B with STP, CISPR22 Class A with UTP Class B with STP, AS/NZS 3548 Class A with UTP Class B with STP, VCCI Class A with UTP Class B with STP, EN55024, ETS 300 386-2, EN50082-1, EN61000-3-2, EN61000-3-3

Product Ordering Information

Table 3 lists ordering information for the Cisco PIX 506E security appliances and related products.

Table 3. Ordering Information

Product Number	Product Description
PIX-506E	PIX 506E Chassis (chassis, software, 2 10/100 interfaces)
PIX-506E-BUN-K9	PIX 506E 3DES/AES Bundle (chassis, software, 2 10/100 interfaces, 3DES/AES license)
PIX-506E-PWR-AC=	Spare AC power supply for PIX 506E
PIX-VPN-DES	PIX DES VPN/SSH/SSL encryption license
PIX-506-SW-3DES	PIX 506/506E 3DES/AES VPN/SSH/SSL encryption license

Support Services

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

Support Ordering Information

Table 4 lists ordering information for Cisco SMARTnet support services.

Table 4. 4Cisco SMARTnet Ordering Information

Product Number	Product Description
CON-SNT-PIX506E	Cisco SMARTnet 8x5xNBD service for Cisco PIX 506E
CON-SNTE-PIX506E	Cisco SMARTnet 8x5x4 service for Cisco PIX 506E
CON-SNTP-PIX506E	Cisco SMARTnet 24x7x4 service for Cisco PIX 506E
CON-S2P-PIX506E	Cisco SMARTnet 24x7x2 service for Cisco PIX 506E
CON-OS-PIX506E	Cisco SMARTnet On-Site 8x5xNBD service for Cisco PIX 506E
CON-OSE-PIX506E	Cisco SMARTnet On-Site 8x5x4 service for Cisco PIX 506E
CON-OSP-PIX506E	Cisco SMARTnet On-Site 24x7x4 service for Cisco PIX 506E
CON-PREM-PIX506E	Cisco SMARTnet On-Site 24x7x2 service for Cisco PIX 506E

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/pixd3_ds.pdf
- Current list of Cisco product security certifications: http://www.cisco.com/go/securitycert
- 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
- CiscoWorks SIMS: http://www.cisco.com/go/sims
- 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 (USA) Pte. Ltd.
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.**

Printed in USA C78-448036-00 12/07