Data Sheet

Cisco PIX 501 Security Appliance

The Cisco PIX® 501 Security Appliance delivers enterprise-class security for small offices and teleworkers in a reliable, plug-and-play purpose-built appliance. Ideal for securing high-speed "always on" broadband environments, the Cisco PIX 501 Security Appliance, which is part of the world-leading Cisco PIX Security Appliance Series, provides robust integrated security capabilities, small office networking features, and powerful remote management capabilities in a compact, all-in-one solution.

Enterprise-Class Security for Small Office Environments

The Cisco PIX 501 Security Appliance delivers a multilayered defense for small offices through rich security services including stateful inspection firewalling, protocol and application inspection, virtual private networking (VPN), in-line intrusion protection, and rich multimedia and voice security in a single device. 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.

Small offices benefit from an additional layer of security via intelligent, "application-aware" security services that examine packet streams at Layers 4–7, using inspection engines specialized for many of today's popular applications. Administrators can also easily create custom security policies for firewall traffic by using the flexible access control methods and the more than 100 predefined applications, services, and protocols that Cisco PIX Security Appliances provide.

Figure 1
Cisco PIX 501 Security Appliance

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) and multimedia standards, allowing businesses to securely take advantage of the many benefits that converged data, voice, and video networks deliver. By combining VPN with the rich stateful inspection firewall services that Cisco PIX Security Appliances provide for these converged networking standards, businesses can securely extend voice and multimedia services to home office and small office environments for additional cost savings, improved productivity, and competitive advantage.

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

The Cisco PIX 501 Security Appliance provides several options for securing all network communications between mobile users, small offices, and corporate networks over low-cost Internet connections. Solutions range from standards-based site-to-site VPN leveraging the Internet Key Exchange (IKE) and IP security (IPsec) VPN standards, to the innovative Easy VPN capabilities found in Cisco PIX Security Appliances and other Cisco security solutions—such as Cisco IOS® routers and Cisco VPN 3000 Series Concentrators. Easy VPN delivers a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture that eliminates the operational costs associated with maintaining remote-device configurations 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 Protection Guards Against Popular Internet Threats

The integrated in-line intrusion-protection capabilities of the Cisco PIX 501 Security Appliance can protect small office networks from many popular forms of attacks, including Denial-of-Service (DoS) attacks and malformed packet attacks. Using a wealth of advanced intrusion-protection features, including DNSGuard, FloodGuard, FragGuard, MailGuard, IPVerify and TCP intercept, in addition to looking for more than 55 different attack "signatures," Cisco PIX Security Appliances keep a vigilant watch for attacks, can optionally block them, and can notify administrators about them in real time.

By packing all the same security features found in the other Cisco PIX Security Appliances, the Cisco PIX 501 Security Appliance provides the rich, consistent protection that all broadband users look for in an easy-to-use and easy-to-deploy solution.

Simple, High-Speed Small Office Networking

The Cisco PIX 501 Security Appliance provides a convenient way for multiple computers to share a single broadband connection via its integrated, high-performance four-port 10/100-Mbps switch. Furthermore, Cisco PIX Security Appliances provide Network Address Translation (NAT) and Port Address Translation (PAT) features to hide the actual network addresses of devices on your network. Users can also enjoy plug-and-play networking by taking advantage of the built-in Dynamic Host Configuration Protocol (DHCP) server within PIX, which automatically assigns their computers network addresses when they are powered on. The Cisco PIX 501 Security Appliance provides all the features necessary to seamlessly integrate into most broadband networking environments.

Robust Remote-Management Solutions Lower Total Cost of Ownership

The Cisco PIX 501 Security Appliance is a reliable, easy-to-maintain platform that provides a wide variety of methods for configuring, monitoring, and troubleshooting. Management solutions range from centralized, policy-based management tools to integrated, Web-based management to support for remote monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog.

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

- Comprehensive configuration and software image management
- Device hierarchy with "Smart Rules"-based configuration inheritance
- Customizable administrative roles and access privileges
- Comprehensive enterprise change management and auditing
- "Touchless" software image management for remote Cisco PIX Security Appliances
- Support for dynamically addressed appliances

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

The integrated Cisco PIX Device Manager provides an intuitive, Web-based management interface for remotely configuring, monitoring, and troubleshooting a Cisco PIX 501 Security Appliance—without requiring any software (other than a standard Web browser) to be installed on an administrator's computer. A setup wizard is provided for easy installation into any network environment.

Alternatively, through methods including Telnet and Secure Shell (SSH), or out of band through a console port, administrators can remotely configure, monitor, and troubleshoot Cisco PIX Security Appliances using a command-line interface (CLI).

Table 1 Key Product Features and Benefits

Key Features	Benefit
Enterprise-Class Security	
True security appliance	• Uses a proprietary, hardened operating system that eliminates security risks associated with general purpose operating systems • Cisco quality and no moving parts provide a highly reliable security platform
Stateful inspection firewall	• Provides perimeter network security to prevent unauthorized network access • Uses state-of-the-art Cisco ASA for robust stateful inspection firewall services • Provides flexible access-control capabilities for over 100 predefined applications, services and protocols, with the ability to define custom applications and services • Includes numerous application-aware inspection engines that secure advanced networking protocols such as H.323 Version 4, Session Initiation Protocol (SIP), Cisco Skinny Client Control Protocol (SCCP), Real-Time Streaming Protocol (RTSP), Internet Locator Service (ILS), and more • Includes content filtering for Java and ActiveX applets

Table 1 Key Product Features and Benefits

Key Features	Benefit
Easy VPN Remote (hardware VPN client)	• Enables dramatically simplified VPN rollouts to small office/teleworker environments by 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 10 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 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
Easy VPN Server	• Provides remote access VPN concentrator services for up to 10 remote software or hardware-based VPN clients • Pushes VPN policy dynamically to Cisco Easy VPN Remote-enabled solutions upon connection, ensuring the latest corporate security policies are enforced • Supports award-winning Cisco VPN Client on multiple platforms including Microsoft Windows, Apple Mac OS X, Red Hat Linux, and Sun Solaris
Site-to-site VPN	• Supports IKE and IPsec VPN industry standards • Ensures data privacy/integrity and strong authentication to remote networks over the Internet • Supports 56-bit DES, 168-bit 3DES and up to 256-bit AES data encryption to ensure data privacy
Intrusion protection	• Provides protection from over 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 for the ability to dynamically block/shun hostile network nodes via the firewall
AAA support	• Integrates with popular authentication, authorization, and accounting services via TACACS+ and RADIUS support
X.509 certificate and CRL support	• Supports SCEP-based enrollment with leading X.509 solutions from Baltimore, Entrust, Microsoft, and VeriSign
Integration with leading third-party solutions	• Supports the broad range of Cisco AVVID (Architecture for Voice, Video and Integrated Data) partner solutions that provide URL filtering, content filtering, virus protection, scalable remote management, and more
Integrated security lock slot	• Provides ability to physically secure the Cisco PIX 501 Security Appliance using a standard notebook security cable lock (lock not included)
Robust Small Office Networking	
Integrated 4-port 10/100 switch	• Provides convenient, high-speed networking environment for small office environments in a single compact platform • Auto-MDIX support eliminates the need to use crossover cables with devices connected to the switch

Table 1 Key Product Features and Benefits

Key Features	Benefit
DHCP client/server	• Obtains IP address for outside interface of appliance automatically from service provider • Provides IP addresses to devices on inside network of the appliance • Delivers "zero touch provisioning" of Cisco IP Phones via automated bootstrapping of CallManager contact information through DHCP server extensions
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 NAT and PAT capabilities • 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 support	• Ensures compatibility with networks that require PPP over Ethernet (PPPoE) support
Rich Management Capabilities	
CiscoWorks VPN/ Security Management Solution (CiscoWorks VMS)	• Comprehensive management suite for large scale deployments • Integrates policy management, software maintenance, and security monitoring
PIX Device Manager (PDM)	• Intuitive, Web-based GUI enables simple, secure remote management of Cisco PIX Security Appliances • Provides 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 XML/HTTPS management interface can be leveraged 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 firewalls with static IP addresses • Integrates seamlessly 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)
Cisco PIX CLI	• Allows customers to use existing PIX CLI knowledge for easy installation and management without additional training • Accessible through variety of methods including console port, Telnet, and SSH
Command-level authorization	• Enables businesses to create up to 16 customizable administrative roles/profiles for accessing Cisco PIX Security Appliances (for example, monitoring only, read-only access to configuration, VPN administrator, firewall/NAT administrator, and so on) • Leverages either the internal administrator database or outside sources via TACACS+, such as Cisco Secure Access Control Server (ACS)
SNMP and syslog support	• Provide remote monitoring and logging capabilities, with integration into Cisco and third-party management applications

Software Licenses

10-User License

The PIX 501 10-user license supports up to ten concurrent source IP addresses from your internal network to traverse through the PIX 501. The integrated DHCP server supports up to 32 DHCP leases.

50-User License

The PIX 501 50-user license supports up to 50 concurrent source IP addresses from your internal network to traverse through the PIX 501. The integrated DHCP server supports up to 128 DHCP leases. As your needs grow, a 10-to-50 user upgrade license is also available, which allows you to extend your investment in PIX 501 equipment.

Unlimited User License

The PIX 501 unlimited user license supports an unlimited number of devices from your internal network to traverse through the PIX 501. The integrated DHCP server supports up to 256 DHCP leases. As your needs grow, a 10-to-unlimited and 50-to-unlimited user upgrade license is also available, which allows you to maximize your investment in PIX 501 equipment.

3DES/AES and DES Encryption Licenses

The Cisco PIX 501 Security Appliance has two optional encryption licenses—one enables 168-bit 3DES and up to 256-bit AES encryption, the other enables 56-bit DES encryption. Both are available either at the time of ordering the appliance, or as an upgrade that can be purchased later.

Performance Summary

Cleartext throughput: 60 Mbps

Concurrent connections: 7500

56-bit DES IPsec VPN throughput: 6 Mbps

168-bit 3DES IPsec VPN throughput: 3 Mbps

128-bit AES IPsec VPN throughput: 4.5 Mbps

Simultaneous VPN peers: 10*

* Maximum number of simultaneous VPN/IKE Security Associations (SAs) supported

Technical Specifications

Processor: 133-MHz AMD SC520 Processor

Random access memory: 16 MB of SDRAM

Flash memory: 8 MB

System bus: Single 32-bit, 33-MHz PCI

Environmental Operating Ranges

Operating

Temperature: 32 to 104 F (0 to 40 C)

Relative humidity: 10 to 90%, noncondensing

Altitude: 0 to 6500 feet (2000 m)

Shock: 250 G, < 2 ms

Vibration: 0.41 Grms2 (3–500 Hz) random input

Nonoperating

Temperature: –4 to 149 F (–20 to 65 C)

Relative humidity: 10 to 90%, noncondensing

Altitude: 0 to 15,000 feet (4570 m)

Shock: 65 G, 8 ms

Vibration: 1.12 Grms2 (3–500 Hz) random input

Power

Input

Range Line Voltage: 100V to 240V AC

Nominal Line Voltage: 100V to 240V AC

Current: 0.051 Amps (at 115V)

Frequency: 50–60 Hz, single phase

Power: 5.9W

Output

Nominal Line Voltage: 3.3V DC

Current: 1.5 Amps

Steady State: 5W

Maximum Peak: 5W

Maximum Heat Dissipation: 17.0 BTU/hr, full power usage (5W)

Physical Specifications

Dimensions and Weight Specifications

Dimensions (H x W x D): 1.0 x 6.25 x 5.5 in. (2.54 x 15.875 x 13.97 cm)

Weight: 0.75 lb (0.34 kg)

Interfaces

Console Port: RS-232 (RJ-45) 9600 baud

Outside: Integrated 10/100 Fast Ethernet port, auto-negotiate (half/full duplex), RJ45

Inside: Integrated auto-sensing, auto-MDIX 4-port 10/100 Fast Ethernet switch, RJ45

Regulatory and Standards Compliance

Products bear CE Marking indicating compliance with the 89/366/EEC and 73/23/EEC directives, which includes the following safety and Electro Magnetic Compatibility (EMC) standards.

Safety

UL1950, CAN/CSA-C22.2 No. 60950-00, IEC60950, EN60950

EMC

EN55022 Class B, CISPR22 Class B, AS/NZS 3548 Class B, VCCI Class B, EN55024, EN50082-1, EN61000-3-2, EN61000-3-3

Product Ordering Information

PIX-501-BUN-K9	PIX 501 10-user bundle (chassis, latest PIX software, 10-user and 3DES licenses, integrated 4-port 10/100 switch and 10/100 port)
PIX-501-50-BUN-K9	PIX 501 50-user bundle (chassis, latest PIX software, 50-user and 3DES licenses, integrated 4-port 10/100 switch and 10/100 port)
PIX-501-UL-BUN-K9	PIX 501 unlimited user bundle (chassis, latest PIX software, unlimited user and 3DES licenses, integrated 4-port 10/100 switch and 10/100 port)
PIX-501	PIX 501 chassis, software, 10-user license, integrated 4-port 10/100 switch and 10/100 port
PIX-501-SW-10	10-user license for PIX 501
PIX-501-SW-50	50-user license for PIX 501
PIX-501-SW-UL	Unlimited user license for PIX 501
PIX-501-SW-10-50=	10-to-50 user upgrade license for PIX 501
PIX-501-SW-10-UL=	10-to-unlimited user upgrade license for PIX 501 (requires Cisco PIX Security Appliance Software Version 6.3)
PIX-501-SW-50-UL=	50-to-unlimited user upgrade license for PIX 501 (requires Cisco PIX Security Appliance Software Version 6.3)
PIX-501-PWR-AC=	Spare AC power supply for PIX 501
PIX-501-VPN-3DES	168-bit 3DES and up to 256-bit AES encryption software license
PIX-501-VPN-3DES=	168-bit 3DES and up to 256-bit AES encryption software license
PIX-VPN-DES	56-bit DES encryption software license
PIX-VPN-DES=	56-bit DES encryption software license

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.

Support Ordering Information

CON-SNT-PIX501-10	SMARTnet 8x5xNBD service for PIX 501 10-user bundle
CON-SNTE-PIX501-10	SMARTnet 8x5x4 service for PIX 501 10-user bundle
CON-SNTP-PIX501-10	SMARTnet 24x7x4 service for PIX 501 10-user bundle
CON-S2P-PIX501-10	SMARTnet 24x7x2 service for PIX 501 10-user bundle
CON-SNT-PIX501-50	SMARTnet 8x5xNBD service for PIX 501 50-user bundle
CON-SNTE-PIX501-50	SMARTnet 8x5x4 service for PIX 501 50-user bundle
CON-SNTP-PIX501-50	SMARTnet 24x7x4 service for PIX 501 50-user bundle
CON-S2P-PIX501-50	SMARTnet 24x7x2 service for PIX 501 50-user bundle
CON-SNT-PIX501	SMARTnet 8x5xNBD service for PIX 501 configurable chassis
CON-SNTE-PIX501	SMARTnet 8x5x4 service for PIX 501 configurable chassis
CON-SNTP-PIX501	SMARTnet 24x7x4 service for PIX 501 configurable chassis
CON-S2P-PIX501	SMARTnet 24x7x2 service for PIX 501 configurable chassis

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

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

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

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

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

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

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

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

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

RD/LW3946 04/03