DATA SHEET

CISCO PIX 501 SECURITY APPLIANCE

The Cisco® PIX® 501 Security Appliance delivers enterprise-class security for small office and teleworker environments, in a reliable, easy-to-deploy purpose-built appliance. Its compact, high performance design incorporates a four-port 10/100 Fast Ethernet switch, making it ideal for securing high-speed broadband Internet connections. Part of the market-leading Cisco PIX Security Appliance Series, the Cisco PIX 501 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 501 Security Appliance

ENTERPRISE-CLASS SECURITY FOR SMALL OFFICE ENVIRONMENTS

The Cisco PIX 501 Security Appliance delivers a multi layered defense for small office 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 environment, these inspection engines incorporate extensive application and protocol knowledge and employ 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 home office and remote office environments for lower total cost of ownership, improved productivity, and increased competitive advantage.

FLEXIBLE VPN SERVICES EXTEND NETWORKS ECONOMICALLY TO REMOTE NETWORKS AND MOBILE USERS

Using the full-featured VPN capabilities of the Cisco PIX 501 Security Appliance, businesses can securely extend their networks across low-cost Internet connections to mobile users, business partners, and corporate networks 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, and 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 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-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.

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 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 today’s 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 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 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 501 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 501 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 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 over 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 which can be referenced by multiple security policies, thus 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 small office/teleworker 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 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 10 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, ensuring the latest corporate security policies are enforced • Supports award-winning Cisco VPN Client on multiple platforms including Microsoft Windows 98/ME/NT/2000XP, Sun Solaris, Intel-based Linux distributions, and Apple Macintosh OS X (available separately)
Site-to-site VPN	• Supports IKE and IPSec VPN industry standards • Extends networks securely over the Internet by ensuring data privacy/integrity and strong authentication with remote networks • Supports 56-bit DES, 168-bit 3DES, and up to 256-bit AES data encryption to ensure data privacy

Feature	Benefit
Intrusion prevention	• Provides protection from over 55 different types of popular network-based attacks ranging from malformed packet attacks to denial-of-service (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/administrator authentication, dynamic per-user/group policies, and administrator access privileges
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)
Industry certifications and evaluations	• Earned numerous leading industry certifications and evaluations, including: – Common Criteria Evaluated Assurance Level 4 (EAL4) – ICSA Labs Firewall 4.0 Certification, Corporate RSSP Category
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
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, and policy-based NAT, as well as 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 support	• 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 wide range of informative, real-time, and historical reports which give critical insight into usage trends, performance baselines, and security events

Feature	Benefit
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 command-line interface	• Allows customers to use existing Cisco IOS CLI knowledge for easy installation and management with little additional training needed • Accessible through variety of 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 (for example, monitoring only, read-only access to configuration, VPN administrator, firewall/NAT administrator, etc.) • 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 Cisco PIX 501 10-user license supports up to 10 concurrent source IP addresses from your internal network to traverse through the Cisco PIX 501. The integrated DHCP server supports up to 32 DHCP leases. As your needs grow, both 50 user and unlimited user upgrade licenses are available, allowing you to extend your investment in Cisco PIX 501 equipment.

50-User License

The Cisco PIX 501 50-user license supports up to 50 concurrent source IP addresses from your internal network to traverse through the Cisco PIX 501. The integrated DHCP server supports up to 128 DHCP leases. As your needs grow, a 50-to-unlimited user upgrade license is also available, allowing you to further extend your investment in Cisco 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 Cisco PIX 501. The integrated DHCP server supports up to 256 DHCP leases.

3DES/AES and DES Encryption Licenses

The Cisco PIX 501 Security Appliance has two optional encryption licenses—one license (PIX-501-VPN-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 501 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 60 Mbps

Concurrent connections: 7,500

56-bit DES IPsec VPN throughput: Up to 6 Mbps

168-bit 3DES IPsec VPN throughput: Up to 3 Mbps

128-bit AES IPsec VPN throughput: Up to 4.5 Mbps

Simultaneous VPN peers: 10*

* Maximum number of simultaneous site-to-site or remote access IKE Security Association (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 percent, 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 percent, noncondensing

Altitude: 0 to 15000 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: 0.051A (at 115V)

Frequency: 50–60 Hz, single phase

Power: 5.9W

Output

Nominal Line Voltage: 3.3V DC

Current: 1.5A

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, 9600 bps, RJ-45

Outside: Integrated 10/100 Fast Ethernet port, auto-negotiate (half/full duplex), RJ-45

Inside: Integrated auto-sensing, auto-MDIX 4-port 10/100 Fast Ethernet switch, RJ-45

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 Electro Magnetic Compatibility (EMC) standards.

Safety

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

Electromagnetic Compatibility (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

Table 2 lists ordering information for the Cisco PIX 501 security appliances and related products.

Table 2. Ordering Information

Product Number	Product Description
PIX-501	Cisco PIX 501 chassis, software, 10-user license, integrated 4-port 10/100 switch and 10/100 port
PIX-501-BUN-K9	Cisco 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	Cisco 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	Cisco 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-SW-10	10-user license for Cisco PIX 501
PIX-501-SW-50	50-user license for Cisco PIX 501
PIX-501-SW-UL	Unlimited user license for Cisco PIX 501
PIX-501-SW-10-50=	10-to-50 user upgrade license for Cisco PIX 501
PIX-501-SW-10-UL=	10-to-unlimited user upgrade license for Cisco PIX 501 (requires Cisco PIX Security Appliance Software Version 6.3)
PIX-501-SW-50-UL=	50-to-unlimited user upgrade license for Cisco PIX 501 (requires Cisco PIX Security Appliance Software Version 6.3)
PIX-501-PWR-AC=	Spare AC power supply for Cisco PIX 501
PIX-VPN-DES	Cisco PIX DES VPN/SSH/SSL encryption license
PIX-501-VPN-3DES	Cisco PIX 501 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, 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

Table 3 lists ordering information for Cisco SMARTnet support services.

Table 3. Cisco SMARTnet Ordering Information

Product Number	Product Description
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

Product Number	Product Description
CON-S2P-PIX501-50	SMARTnet 24x7x2 service for PIX 501 50-user bundle
CON-SNT-PIX501UL	SMARTnet 8x5xNBD service for PIX 501 Unlimited-user bundle
CON-SNTE-PIX501UL	SMARTnet 8x5x4 service for PIX 501 Unlimited-user bundle
CON-SNTP-PIX501UL	SMARTnet 24x7x4 service for PIX 501 Unlimited-user bundle
CON-S2P-PIX501UL	SMARTnet 24x7x2 service for PIX 501 Unlimited-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

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

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

BU/LW6712 09/04

Printed in USA