CISCO PIX 525 SECURITY APPLIANCE

The Cisco® PIX® 525 Security Appliance delivers enterprise-class security for medium-to-large enterprise networks, in a reliable, purpose-built appliance. Its modular two-rack unit (2RU) design incorporates two 10/100 Fast Ethernet interfaces and supports a combination of up to six additional 10/100 Fast Ethernet interfaces or three additional Gigabit Ethernet interfaces, making it an ideal choice for businesses requiring a high performance, Gigabit Ethernet-ready solution that provides solid investment protection. Part of the market-leading Cisco PIX Security Appliance Series, the Cisco PIX 525 Security Appliance provides a wide range of rich, integrated security services, hardware VPN acceleration, and powerful remote management capabilities in a cost-effective, highly-resilient solution.
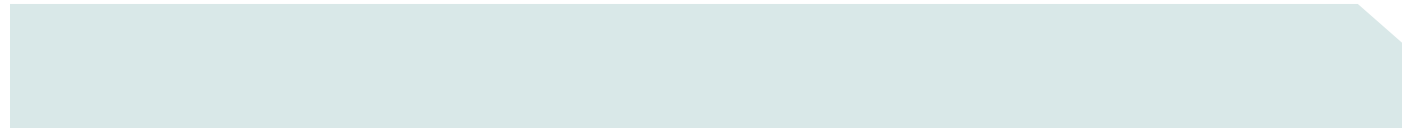
Figure 1
Cisco PIX 525 Security Appliance

ENTERPRISE-CLASS SECURITY FOR MEDIUM-TO-LARGE ENTERPRISE NETWORKS

The Cisco PIX 525 Security Appliance provides delivers a multilayered defense for medium-to-large enterprise networks through rich, integrated security services, including stateful inspection firewall services, advanced application and protocol inspection, site-to-site and remote access VPN, inline 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 more than 24 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 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 numerous 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 OFFICES AND MOBILE USERS

Using the full-featured VPN capabilities of the Cisco PIX 525 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. Certain Cisco PIX 525 Security Appliance models have integrated hardware VPN acceleration capabilities, delivering highly scalable, high-performance VPN services.

INTEGRATED INTRUSION PREVENTION GUARDS AGAINST POPULAR INTERNET THREATS

The integrated inline intrusion prevention capabilities of the Cisco PIX 525 Security Appliance can protect medium-to-large enterprise 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.

AWARD-WINNING RESILIENCY PROVIDES MAXIMUM BUSINESS UPTIME

Select models of Cisco PIX 525 Security Appliances provide stateful failover capabilities that help to ensure resilient network protection for enterprise network environments. Employing a cost-effective, active-standby, high-availability architecture, Cisco PIX Security Appliances that are configured as a failover pair continuously synchronize their connection state and device configuration data. Synchronization can take place over a high-speed LAN connection, providing another layer of protection through the ability 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.

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 support of 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 525 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-based 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 large numbers 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 525 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 525 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 (ASA) 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 more than 24 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 Server	• Provides remote access VPN concentrator services for up to 2000 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 Port Address Translation (PAT), via support of Internet Engineering Task Force (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
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 or 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)
	  – ICSA Labs Firewall 4.0 Certification, Corporate RSSP Category
	  – ICSA Labs IPSec 1.0B Certification

Robust Network Services and Network Integration	
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 10 total VLANs on a Cisco PIX 525 Security Appliance
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 plaintext 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 Control Protocol (DHCP) server	• 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 rich dynamic, static and policy-based NAT, and PAT services
Rich Remote Management Options	
CiscoWorks VMS	• Provides a 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

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 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 • Integrates with CiscoWorks 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 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 Cisco PIX Security Appliances (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	• Provides remote monitoring and logging capabilities, with integration into Cisco and third-party management applications
Flexible Expansion Capabilities	
Fast Ethernet and Gigabit Ethernet expansion options	• Supports easy installation of additional network interfaces via three PCI expansion slots • Supports expansion cards including single-port Fast Ethernet, four-port Fast Ethernet, and single-port Gigabit Ethernet cards
Hardware VPN acceleration options	• Delivers high speed VPN services through the addition of either a VPN Accelerator Card (VAC) or a VPN Accelerator Card+ (VAC+)

License Options

The Cisco PIX 525 Security Appliance is available in three primary models that provide different levels of interface density, failover capabilities, and VPN throughput. Optional encryption licenses are also available that enable various strengths of encryption technology within the Cisco PIX 525 Security Appliance.

Restricted Software License

The Cisco PIX 525 Restricted (PIX 525-R) model provides an excellent value for organizations looking for robust Cisco PIX Security Appliance services with Gigabit Ethernet support, medium interface density and moderate VPN throughput requirements. It includes 128 MB of RAM, two 10/100 Fast Ethernet interfaces, and support for up to four additional 10/100 Fast Ethernet or three Gigabit Ethernet interfaces.

Unrestricted Software License

The Cisco PIX 525 Unrestricted (PIX 525-UR) model extends the capabilities of the security appliance with support for stateful failover, additional LAN interfaces, and increased VPN throughput via integrated hardware-based VPN acceleration. It includes an integrated VAC or VAC+ hardware VPN accelerator, 256 MB of RAM, two 10/100 Fast Ethernet interfaces, and support for up to six additional 10/100 Fast Ethernet or three Gigabit Ethernet interfaces. The Cisco PIX 525-UR also adds the ability to share state information with a hot-standby Cisco PIX Security Appliance for resilient network protection.

Failover Software License

The Cisco PIX 525 Failover (PIX 525-FO) model is designed for use in conjunction with a PIX 525-UR, providing a cost-effective, high-availability solution. It operates in hot-standby mode acting as a complete redundant system that maintains current session state information. With the same hardware configuration as the Cisco PIX 525-UR, it delivers the ultimate in high availability for a fraction of the price.

3DES/AES and DES Encryption Licenses

The Cisco PIX 525 Security Appliance has two optional encryption licenses—one license (PIX-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 525 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 330 Mbps

Concurrent connections: 280,000

168-bit 3DES IPSec VPN throughput: Up to 145 Mbps with VAC+ or 72 Mbps with VAC

128-bit AES IPSec VPN throughput: Up to 135 Mbps with VAC+

256-bit AES IPSec VPN throughput: Up to 135 Mbps with VAC+

Simultaneous VPN tunnels: 2000

Technical Specifications

Processor: 600-MHz Intel Pentium III Processor

RAM: 128 or 256 MB of SDRAM

Flash memory: 16 MB

Cache: 256 KB level 2 at 600 MHz

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

Environmental Operating Ranges

Operating

Temperature: –25 to 104ºF (–5 to 40ºC)

Relative humidity: 5 to 95 percent noncondensing

Altitude: 0 to 6500 ft (2000 m)

Shock: 1.14 m/sec (45 in./sec) 1/2 sine input

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

Acoustic noise: 45 dBa maximum

Nonoperating

Temperature: –13 to 158ºF (–25 to 70ºC)

Relative humidity: 5 to 95 percent noncondensing

Altitude: 0 to 15000 ft (4570 m)

Shock: 30 G

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

Power

Input (per power supply)

Range line voltage: 100V to 240V AC or 48V DC to 60V DC

Nominal line voltage: 100V to 240V AC or 48V DC to 60V DC

Current: 5-2.5A AC or 12A DC

Frequency: 50 to 60 Hz, single phase

Output

Steady state: 50W

Maximum peak: 65W

Maximum heat dissipation: 410 BTU/hr, full power usage (65W)

Physical Specifications

Dimensions and Weight Specifications

Form factor: 2 RU, standard 19-in. rack mountable

Dimensions (H x W x D): 3.5 x 17.5 x 18.25 in. (8.89 x 44.45 x 46.36 cm)

Weight (with power supply): 32 lb (14.5 kg)

Expansion

Three 32-bit/33-MHz PCI slots

Two 168-pin DIMM RAM slots

Interfaces

Console port: RS-232, 9600 bps, RJ-45

Failover port: RS-232, 115 Kbps, DB-15 (special Cisco PIX failover cable required)

Two integrated 10/100 Fast Ethernet interfaces, auto-negotiate (half/full duplex), RJ45

Regulatory and Standards Compliance

Safety

UL 1950, CSA C22.2 No. 950, EN 60950 IEC 60950, AS/NZS3260, TS001

Electromagnetic Compatibility (EMC)

CE marking, FCC Part 15 Class A, AS/NZS 3548 Class A, VCCI Class A, EN55022 Class A, CISPR22 Class A, EN61000-3-2, EN61000-3-3

Product Ordering Information

Table 2 lists ordering information for the Cisco PIX 525 Security Appliances and related products.

Table 2.   Ordering Information

Product Number	Product Description
PIX-525	Cisco PIX 525 Chassis (chassis, software, 2 10/100 interfaces)
PIX-525-DC	Cisco PIX 525 DC Chassis (chassis, software, 2 10/100 interfaces)
PIX-525-R-BUN	Cisco PIX 525 Restricted Bundle (chassis, restricted license, software, 2 10/100 interfaces, 128 MB RAM)
PIX-525-UR-BUN	Cisco PIX 525 Unrestricted Bundle (chassis, unrestricted license, software, two 10/100 interfaces, 256 MB RAM, VAC or VAC+)
PIX-525-UR-GE-BUN	Cisco PIX 525 Unrestricted 2 GE + 2 FE Bundle (chassis, unrestricted license, software, 2 Gigabit Ethernet + 2 10/100 interfaces, 256 MB RAM, VAC or VAC+)
PIX-525-FO-BUN	Cisco PIX 525 Failover Bundle (chassis, failover license, software, 2 10/100 interfaces, 256 MB RAM, VAC or VAC+)
PIX-525-FO-GE-BUN	Cisco PIX 525 Failover 2 GE + 2 FE Bundle (chassis, failover license, software, 2 Gigabit Ethernet + 2 10/100 interfaces, VAC or VAC+)
PIX-525-HW=	Cisco PIX 525 rack-mount kit, console cable, and failover cable
PIX-FO=	Cisco PIX failover cable
PIX-1FE	Cisco PIX single-port 10/100 Fast Ethernet interface card, RJ-45
PIX-4FE-66	Cisco PIX 64-bit/66-MHz 4-port 10/100 Fast Ethernet interface card, RJ-45
PIX-1GE-66	Cisco PIX 64-bit/66-MHz single-port Gigabit Ethernet interface card, Multimode (SX) SC
PIX-VPN-ACCEL	Cisco PIX DES/3DES VPN Accelerator Card (VAC)
PIX-VAC-PLUS	Cisco PIX DES/3DES/AES VPN Accelerator Card+ (VAC+)
PIX-VPN-DES	Cisco PIX DES VPN/SSH/SSL encryption license
PIX-VPN-3DES	Cisco PIX 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 3 lists ordering information for Cisco SMARTnet support services.

Table 3. Cisco SMARTnet Ordering Information

Product Number	Product Description
CON-SNT-PIX525	Cisco SMARTnet 8x5xNBD service for Cisco PIX 525 chassis only
CON-SNT-PIX525R	Cisco SMARTnet 8x5xNBD service for Cisco PIX 525-R bundle
CON-SNT-PIX525UR	Cisco SMARTnet 8x5xNBD service for Cisco PIX 525-UR bundle
CON-SNT-PIX525GE	Cisco SMARTnet 8x5xNBD service for Cisco PIX-525-UR-GE bundle
CON-SNT-PIX525FO	Cisco SMARTnet 8x5xNBD service for Cisco PIX 525-FO bundle
CON-SNT-PIX525FG	Cisco SMARTnet 8x5xNBD service for Cisco PIX-525-FO-GE bundle
CON-SNTE-PIX525	Cisco SMARTnet 8x5x4 service for Cisco PIX 525 chassis only
CON-SNTE-PIX525R	Cisco SMARTnet 8x5x4 service for Cisco PIX 525-R bundle
CON-SNTE-PIX525UR	Cisco SMARTnet 8x5x4 service for Cisco PIX 525-UR bundle
CON-SNTE-PIX525GE	Cisco SMARTnet 8x5x4 service for Cisco PIX-525-FO-GE bundle
CON-SNTE-PIX525FO	Cisco SMARTnet 8x5x4 service for Cisco PIX 525-FO bundle
CON-SNTE-PIX525FG	Cisco SMARTnet 8x5x4 service for Cisco PIX-525-FO-GE bundle
CON-SNTP-PIX525	Cisco SMARTnet 24x7x4 service for Cisco PIX 525 chassis only
CON-SNTP-PIX525R	Cisco SMARTnet 24x7x4 service for Cisco PIX 525-R bundle
CON-SNTP-PIX525UR	Cisco SMARTnet 24x7x4 service for Cisco PIX 525-UR bundle
CON-SNTP-PIX525GE	Cisco SMARTnet 24x7x4 service for Cisco PIX-525-UR-GE bundle
CON-SNTP-PIX525FO	Cisco SMARTnet 24x7x4 service for Cisco PIX 525-FO bundle
CON-SNTP-PIX525FG	Cisco SMARTnet 24x7x4 service for Cisco PIX-525-FO-GE bundle
CON-S2P-PIX525R	Cisco SMARTnet 24x7x2 service for Cisco PIX 525-R bundle
CON-S2P-PIX525UR	Cisco SMARTnet 24x7x2 service for Cisco PIX 525-UR bundle
CON-S2P-PIX525FO	Cisco SMARTnet 24x7x2 service for Cisco PIX 525-FO bundle
CON-OS-PIX525	Cisco SMARTnet On-Site 8x5xNBD service for Cisco PIX 525 chassis only
CON-OS-PIX525R	Cisco SMARTnet On-Site 8x5xNBD service for Cisco PIX 525-R bundle
CON-OS-PIX525UR	Cisco SMARTnet On-Site 8x5xNBD service for Cisco PIX 525-UR bundle
CON-OS-PIX525GE	Cisco SMARTnet On-Site 8x5xNBD service for Cisco PIX-525-UR-GE bundle
CON-OS-PIX525FO	Cisco SMARTnet On-Site 8x5xNBD service for Cisco PIX 525-FO bundle
CON-OS-PIX525FG	Cisco SMARTnet On-Site 8x5xNBD service for Cisco PIX-525-FO-GE bundle
CON-OSE-PIX525	Cisco SMARTnet On-Site 8x5x4 service for Cisco PIX 525 chassis only
CON-OSE-PIX525R	Cisco SMARTnet On-Site 8x5x4 service for Cisco PIX 525-R bundle
CON-OSE-PIX525UR	Cisco SMARTnet On-Site 8x5x4 service for Cisco PIX 525-UR bundle
CON-OSE-PIX525GE	Cisco SMARTnet On-Site 8x5x4 service for Cisco PIX-525-UR-GE bundle
CON-OSE-PIX525FO	Cisco SMARTnet On-Site 8x5x4 service for Cisco PIX 525-FO bundle
CON-OSE-PIX525FG	Cisco SMARTnet On-Site 8x5x4 service for Cisco PIX-525-FO-GE bundle
CON-OSP-PIX525	Cisco SMARTnet On-Site 24x7x4 service for Cisco PIX 525 chassis only
CON-OSP-PIX525R	Cisco SMARTnet On-Site 24x7x4 service for Cisco PIX 525-R bundle
CON-OSP-PIX525UR	Cisco SMARTnet On-Site 24x7x4 service for Cisco PIX 525-UR bundle
CON-OSP-PIX525GE	Cisco SMARTnet On-Site 24x7x4 service for Cisco PIX 525-UR-GE bundle
CON-OSP-PIX525FO	Cisco SMARTnet On-Site 24x7x4 service for PIX 525-FO bundle
CON-OSP-PIX525FG	Cisco SMARTnet On-Site 24x7x4 service for PIX 525-FO-GE bundle

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

CISCO SYSTEMS

Corporate Headquarters	European Headquarters	Americas Headquarters	Asia Pacific Headquarters
Cisco Systems, Inc.	Cisco Systems International BV	Cisco Systems, Inc.	Cisco Systems, Inc.
170 West Tasman Drive	Haarlerbergpark	170 West Tasman Drive	168 Robinson Road
San Jose, CA 95134-1706	Haarlerbergweg 13-19	San Jose, CA 95134-1706	#28-01 Capital Tower
USA	1101 CH Amsterdam	USA	Singapore 068912
www.cisco.com	The Netherlands	www.cisco.com	www.cisco.com
Tel: 408 526-4000	www-europe.cisco.com	Tel: 408 526-7660	Tel: +65 6317 7777
800 553-NETS (6387)	Tel: 31 0 20 357 1000	Fax: 408 527-0883	Fax: +65 6317 7799
Fax: 408 526-4100	Fax: 31 0 20 357 1100		

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