DATA SHEET

CISCO PIX 515E SECURITY APPLIANCE

The Cisco® PIX® 515E Security Appliance delivers enterprise-class security for small-to-medium business and enterprise networks, in a modular, purpose-built appliance. Its versatile one-rack unit (1RU) design supports up to six 10/100 Fast Ethernet interfaces, making it an excellent choice for businesses requiring a cost-effective, resilient security solution with DMZ support. Part of the market-leading Cisco PIX Security Appliance Series, the Cisco PIX 515E Security Appliance provides a wide range of rich integrated security services, hardware VPN acceleration, and powerful remote management capabilities in an easy-to-deploy, high-performance solution.

Figure 1
Cisco PIX 515E Security Appliance

ENTERPRISE-CLASS SECURITY FOR SMALL-TO-MEDIUM BUSINESS AND ENTERPRISE NETWORKS

The Cisco PIX 515E Security Appliance delivers a multilayered defense for small-to-medium business and enterprise networks through rich integrated security services including stateful inspection firewalling, advanced application and protocol inspection, virtual private networking (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 to provide stateful inspection firewall services by tracking the state of all authorized network communications and 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 Layer 4–7 inspection of network flows for many of today's popular applications and protocols. To defend networks from a wide variety of application layer attacks and give businesses more control over applications/protocols in their environments, these inspection engines combine extensive application/protocol knowledge with a variety of security enforcement technologies ranging from protocol conformance checking, application/protocol state tracking, Network Address Translation (NAT) services, as well as an array of attack detection/mitigation techniques such as protocol field length checking, URL length checking, and much more.

Administrators can easily create custom security policies using the many flexible access control technologies provided by Cisco PIX Security Appliances including network/service object groups, turbo access control lists (ACLs), user/group-based policies, and more than 100 predefined applications and protocols. By leveraging these flexible access control technologies together 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 VOICE-OVER-IP SECURITY SERVICES PROTECT NEXT-GENERATION CONVERGED NETWORKS

Cisco PIX Security Appliances also 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

Businesses can securely extend their networks across low-cost Internet connections to mobile users, business partners, and remote offices worldwide using the full-featured VPN capabilities provided by the Cisco PIX 515E Security Appliance. Solutions supported range from standards-based site-to-site VPN leveraging 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 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. Certain Cisco PIX 515E 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 515E Security Appliance can protect small-to-medium business and 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 515E Security Appliances provide stateful failover capabilities that 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 leveraging native support of 802.1q-based Virtual LANs (VLANs). Cisco IP Phones can benefit from the “zero-touch provisioning” services provided by Cisco PIX Security Appliances, which help Cisco IP 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 515E 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 a number of 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 “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

Additionally, Cisco offers 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, as well as on-going configuration and monitoring of a Cisco PIX 515E 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 515E Security Appliances using a command-line interface (CLI). Secure CLI access is available using a variety of methods including Secure Shell (SSH), 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), SQL*Net, Microsoft Networking (SMB), 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
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, ensuring the latest corporate security policies are enforced • Extends VPN reach into environments using NAT or 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/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 (SA) for comprehensive endpoint security
Site-to-site VPN	• Supports IKE and IPSec VPN standards • Extends networks securely over the Internet by ensuring data privacy/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 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

Feature	Benefit
AAA support	• Integrates with popular authentication, authorization, and accounting 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
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/Integration	
Virtual LAN (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 • Support for up to eight total VLANs on a Cisco PIX 515E Security Appliance
Open Shortest Path First (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 Network Address Translation (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
DHCP server	• Provides DHCP Server services on one or more interfaces for 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 Network Address Translation (NAT), as well as Port Address Translation (PAT) services
Rich Management Capabilities	
CiscoWorks VPN/Security Management Solution (CiscoWorks VMS)	• Comprehensive management suite for large scale Cisco security product deployments • Integrates policy management, software maintenance, and security monitoring into a single management console

Feature	Benefit
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 • 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 (CLI)	• Allows customers to use existing Cisco IOS CLI knowledge for easy installation and management without additional training • 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
Flexible Expansion Capabilities	
Fast Ethernet expansion options	• Supports easy installation of additional network interfaces via two PCI expansion slots • Supports expansion cards including single-port Fast Ethernet and four-port Fast Ethernet cards
Hardware VPN acceleration options	• Delivers high performance VPN services via addition of either a VPN Accelerator Card (VAC) or a VPN Accelerator Card+ (VAC+)

License Options

The Cisco PIX 515E Security Appliance is available in three primary models that provide different levels of interface density, failover capabilities, and VPN throughput.

Restricted Software License

The Cisco PIX 515E "Restricted" (PIX 515E-R) model provides an excellent value for organizations looking for robust Cisco PIX Security Appliance services with minimal interface density and modest VPN throughput requirements. It includes 32 MB of RAM, two 10/100 Fast Ethernet interfaces, and support for one additional 10/100 Fast Ethernet interface.

Unrestricted Software License

The PIX 515E "Unrestricted" (PIX 515E-UR) model extends the capabilities of the family 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, 64 MB of RAM, two 10/100 Fast Ethernet interfaces, and support for up to four additional 10/100 Fast Ethernet interfaces. The Cisco PIX 515E-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 515E "Failover" (PIX 515E-FO) model is designed for use in conjunction with a PIX 515E-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 515E-UR, it delivers the ultimate in high availability for a fraction of the price.

Performance Summary

Cleartext throughput: Up to 190 Mbps

Concurrent connections: 130,000

168-bit 3DES IPSec VPN throughput: Up to 135 Mbps with VAC+ or 63 Mbps with VAC

128-bit AES IPSec VPN throughput: Up to 130 Mbps with VAC+

256-bit AES IPSec VPN throughput: Up to 130 Mbps with VAC+

Simultaneous VPN tunnels: 2000

Technical Specifications

Processor: 433-MHz Intel Celeron Processor

Random access memory: 32 MB or 64 MB of SDRAM

Flash memory: 16 MB

Cache: 128 KB level 2 at 433 MHz

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

Environmental Operating Ranges

Operating

Temperature: –25º to 131ºF (–5º to 55ºC)

Relative Humidity: 5% to 95% noncondensing

Altitude: 0 to 9843 ft (3000 m)

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

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

Acoustic Noise: 45 dBa maximum

Nonoperating

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

Relative Humidity: 5% to 95% noncondensing

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

Shock: 30 G

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

Power

Input (per power supply)

Range Line Voltage: 100V to 240V AC or 48V DC

Nominal Line Voltage: 100V to 240V AC or 48V DC

Current: 1.5 Amps

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: 1 RU, standard 19-in. rack mountable

Dimensions (H x W x D): 1.72 x 16.82 x 11.8 in. (4.37 x 42.72 x 29.97 cm)

Weight (with power supply): 11 lb (4.11 kg)

Expansion

Two 32-bit/33-MHz PCI slots

Two 168-pin DIMM RAM slots, supporting up to 64 MB memory maximum

Interfaces

Console Port: RS-232, 9600 bps, RJ45

Failover Port: RS-232, 115 Kbps, DB-15 (special 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, IEC60825, EN 60825, 21CFR1040

Electro Magnetic Compatibility (EMC)

FCC Part 15 (CFR 47) Class A, ICES-003 Class A with UTP, EN55022 Class A with UTP, CISPR 22 Class A with UTP, AS/NZ 3548 Class A with UTP, VCCI Class A with UTP, EN55024, EN50082-1 (1997), CE marking, EN55022 Class B with FTP, Cispr 22 Class B with FTP, AS/NZ 3548 Class B with FTP, VCCI Class B with FTP

PRODUCT ORDERING INFORMATION

Product Number	Product Description
PIX-515E	PIX 515E Chassis (chassis, software, 2 10/100 interfaces)
PIX-515E-DC	PIX 515E DC Chassis (chassis, software, 2 10/100 interfaces)
PIX-515E-R-BUN	PIX 515E Restricted Bundle (chassis, restricted license, software, 2 10/100 interfaces, 32 MB RAM)
PIX-515E-R-DMZ-BUN	PIX 515E DMZ Bundle (chassis, restricted license, software, 3 10/100 interfaces, 32 MB RAM)
PIX-515E-UR-BUN	PIX 515E Unrestricted Bundle (chassis, unrestricted license, software, 2 10/100 ports, 64 MB RAM, VAC or VAC+)
PIX-515E-UR-FE-BUN	PIX 515E Unrestricted 6-port Fast Ethernet Bundle (chassis, unrestricted license, software, 6 10/100 ports, 64 MB RAM, VAC or VAC+)
PIX-515E-FO-BUN	PIX 515E Failover Bundle (chassis, failover license, software, 2 10/100 interfaces, 64 MB RAM, VAC or VAC+)
PIX-515E-FO-FE-BUN	PIX 515E Failover 6-port Fast Ethernet Bundle (chassis, failover license, software, 6 10/100 interfaces, VAC or VAC+)
PIX-515E-DC-R-BUN	PIX 515E DC Restricted Bundle (chassis, restricted license, software, 2 10/100 interfaces, 32 MB RAM)
PIX-515E-DC-UR-BUN	PIX 515E DC Unrestricted Bundle (chassis, unrestricted license, software, 2 10/100 interfaces, 64 MB RAM, VAC or VAC+)
PIX-515E-DC-FO-BUN	PIX 515E DC Failover Bundle (chassis, failover license, software, 2 10/100 interfaces, 64 MB RAM, VAC or VAC+)
PIX-515E-HW=	PIX 515E rack mount kit, console cable, failover cable
PIX-FO=	PIX failover cable

Product Number	Product Description
PIX-4FE-66	PIX 64-bit/66-MHz 4-port 10/100 Fast Ethernet interface card, RJ45
PIX-1FE	PIX single-port 10/100 Fast Ethernet interface card, RJ45
PIX-VPN-ACCEL	PIX DES/3DES VPN Accelerator Card (VAC)
PIX-VAC-PLUS	PIX DES/3DES/AES VPN Accelerator Card+ (VAC+)
PIX-515-VPN-3DES	PIX 3DES/AES VPN/SSH/SSL encryption license
PIX-VPN-DES	PIX DES 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

Product Number	Product Description
CON-SNT-PIX515E	SMARTnet 8x5xNBD service for PIX 515E chassis only
CON-SNT-PIX515ER	SMARTnet 8x5xNBD service for PIX 515E-R bundle
CON-SNT-PIX515EUR	SMARTnet 8x5xNBD service for PIX 515E-UR bundle
CON-SNT-PIX515FE	SMARTnet 8x5xNBD service for PIX 515E-UR-FE bundle
CON-SNT-PIX515EFO	SMARTnet 8x5xNBD service for PIX 515E-FO bundle
CON-SNT-PIX515FF	SMARTnet 8x5xNBD service for PIX 515E-FO-FE bundle
CON-SNTE-PIX515E	SMARTnet 8x5x4 service for PIX 515E chassis only
CON-SNTE-PIX515ER	SMARTnet 8x5x4 service for PIX 515E-R bundle
CON-SNTE-PIX515EUR	SMARTnet 8x5x4 service for PIX 515E-UR bundle
CON-SNTE-PIX515FE	SMARTnet 8x5x4 service for PIX 515E-UR-FE bundle
CON-SNTE-PIX515EFO	SMARTnet 8x5x4 service for PIX 515E-FO bundle
CON-SNTE-PIX515FF	SMARTnet 8x5x4 service for PIX 515E-FO-FE bundle
CON-SNTP-PIX515E	SMARTnet 24x7x4 service for PIX 515E chassis only
CON-SNTP-PIX515ER	SMARTnet 24x7x4 service for PIX 515E-R bundle
CON-SNTP-PIX515EUR	SMARTnet 24x7x4 service for PIX 515E-UR bundle
CON-SNTP-PIX515FE	SMARTnet 24x7x4 service for PIX 515E-UR-FE bundle
CON-SNTP-PIX515EFO	SMARTnet 24x7x4 service for PIX 515E-FO bundle
CON-SNTP-PIX515FF	SMARTnet 24x7x4 service for PIX 515E-FO-FE bundle
CON-OS-PIX515E	SMARTnet On-Site 8x5xNBD service for PIX 515E chassis only
CON-OS-PIX515ER	SMARTnet On-Site 8x5xNBD service for PIX 515E-R bundle
CON-OS-PIX515EUR	SMARTnet On-Site 8x5xNBD service for PIX 515E-UR bundle
CON-OS-PIX515FE	SMARTnet On-Site 8x5xNBD service for PIX 515E-UR-FE bundle
CON-OS-PIX515EFO	SMARTnet On-Site 8x5xNBD service for PIX 515E-FO bundle
CON-OS-PIX515FF	SMARTnet On-Site 8x5xNBD service for PIX 515E-FO-FE bundle

Product Number	Product Description
CON-OSE-PIX515E	SMARTnet On-Site 8x5x4 service for PIX 515E chassis only
CON-OSE-PIX515ER	SMARTnet On-Site 8x5x4 service for PIX 515E-R bundle
CON-OSE-PIX515EUR	SMARTnet On-Site 8x5x4 service for PIX 515E-UR bundle
CON-OSE-PIX515FE	SMARTnet On-Site 8x5x4 service for PIX 515E-UR-FE bundle
CON-OSE-PIX515EFO	SMARTnet On-Site 8x5x4 service for PIX 515E-FO bundle
CON-OSE-PIX515FF	SMARTnet On-Site 8x5x4 service for PIX 515E-FO-FE bundle
CON-OSP-PIX515E	SMARTnet On-Site 24x7x4 service for PIX 515E chassis only
CON-OSP-PIX515ER	SMARTnet On-Site 24x7x4 service for PIX 515E-R bundle
CON-OSP-PIX515EUR	SMARTnet On-Site 24x7x4 service for PIX 515E-UR bundle
CON-OSP-PIX515FE	SMARTnet On-Site 24x7x4 service for PIX 515E-UR-FE bundle
CON-OSP-PIX515EFO	SMARTnet On-Site 24x7x4 service for PIX 515E-FO bundle
CON-OSP-PIX515FF	SMARTnet On-Site 24x7x4 service for PIX 515E-FO-FE 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 Access Control Server (ACS):

http://www.cisco.com/go/acs

CiscoWorks VPN Security Management Solution (VMS), Management Center for Firewalls, Auto Update Server Software, and Security Monitor:

http://www.cisco.com/go/vms

CiscoWorks Security Information Management Solution (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/LW6067 07/04

Printed in the USA