



PRODUCT BULLETIN NO. 2783

## CISCO SECURITY STARTER BUNDLE

**The Cisco® Security Starter Bundle is a cost-effective solution for identifying and preventing threats in small and medium-sized businesses and enterprise networks, providing advanced multilayered network security services. The bundle delivers full-featured site-to-site and remote-access VPN technology to cost-effectively connect networks and mobile users. Components of this solution include the market-leading Cisco PIX® 515E Security Appliance for robust perimeter security, Cisco Security Agent software for unsurpassed server and desktop protection, and the scalable CiscoWorks VPN/Security Management Solution (VMS) for centrally managing these security services..**

Using the Cisco Security Starter Bundle, businesses can:

- Quickly identify and block worms and other malicious applications and network traffic
- Protect critical servers and desktops from known and unknown attacks at “day zero”
- Block spyware without requiring signature updates
- Deploy enterprise-class security via stateful inspection firewall services and advanced application inspection to mitigate internal and external threats
- Extend networks economically to remote offices and mobile users through robust VPN services
- Lower operational costs by managing and monitoring all components of this solution via a single, scalable Web-based application
- Upgrade solution components to high-availability firewall services, integrated hardware-based VPN acceleration, additional LAN interfaces, and the ability to manage more security devices

### ENDPOINT THREAT PROTECTION MITIGATES WORM ATTACKS AND PROPAGATION

Cisco Security Agent protects mission-critical servers and desktops, also known as network endpoints, against worms, viruses, and other attacks. It goes beyond conventional endpoint security solutions, such as personal firewalls and host-based intrusion detection systems (IDSs), by analyzing behavior rather than relying on signature matching. This day-zero threat prevention technology helps to identify and block damaging activity before it can occur, removing potential known and unknown security risks that threaten networks and applications. Cisco Security Agent ships with predefined policies that prevent most types of malicious activity from occurring, providing personal firewall, day-zero virus and worm protection, intrusion prevention system (IPS), spyware blocking, and operating system hardening functions. Agents are centrally managed and controlled by the CiscoWorks Management Center, a component of CiscoWorks VMS. The Cisco Security Starter Bundle includes CiscoWorks VMS Basic, one Cisco Security Agent license for a server, and 10 additional licenses for desktops. As business needs grow, additional Cisco Security Agent licenses can be purchased for servers and desktops.

**Figure 1.** Cisco PIX 515E Security Appliance



### **ADVANCED FIREWALL SERVICES DELIVER STRONG BUSINESS PROTECTION AND RICH APPLICATION CONTROL**

The Cisco PIX 515E Security Appliance (Figure 1) delivers a wealth of advanced security and networking services for small-to-medium business and enterprise networks, in a modular, purpose-built appliance. Part of the market-leading Cisco PIX Security Appliance Series, the Cisco PIX 515E Security Appliance provides robust user and application policy enforcement, multi-vector attack protection, and security connectivity services through a wide range of rich security and networking services. Cisco PIX Security Appliances integrate a broad range of advanced firewall services to protect businesses from the constant barrage of threats on the Internet and in many business network environments. As a secure foundation, Cisco PIX Security Appliances provide rich stateful inspection firewall services, tracking the state of all network communications and preventing unauthorized network access. Building upon those services, Cisco PIX Security Appliances deliver strong application layer security through 30 intelligent, application-aware inspection engines that examine network flows at Layers 4-7. To defend networks from application layer attacks and to give businesses more control over applications and protocols used in their environment, these inspection engines incorporate extensive application and protocol knowledge and employ security enforcement technologies that include protocol anomaly detection, application and protocol state tracking, Network Address Translation (NAT) services, and attack detection and mitigation techniques such as application/protocol command filtering, content verification, and URL deobfuscation. These inspection engines also give businesses control over instant messaging, peer-to-peer file sharing, and tunneling applications, enabling businesses to enforce usage policies and protect network bandwidth for legitimate business applications.

Administrators can easily create custom security policies using the many flexible access control technologies provided by Cisco PIX 515E Security Appliances, including network and service object groups, user and group-based policies, and more than 100 predefined applications and protocols. Using the powerful Modular Policy Framework introduced in Cisco PIX Security Appliance Software v7.0, administrators can define granular flow-based and class map-based policies, which apply a set of customizable security services, such as inspection engine policies, Quality of Service (QoS) policies, connection timers, and more, to each administrator-specified traffic flow/class. By combining these flexible access control and per-flow/class security services, the powerful stateful inspection and application-aware firewall services, and the multi-vector attack protection services that Cisco PIX Security Appliances deliver, businesses can enforce comprehensive security policies to protect themselves from attack.

### **FLEXIBLE VPN SERVICES ECONOMICALLY EXTEND NETWORKS TO REMOTE OFFICES 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 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 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 typical operational costs associated with maintaining remote-device configurations. The Cisco Security Starter Bundle includes unlimited licenses of Cisco VPN Client software. Additional copies of the software can be downloaded from [cisco.com](http://cisco.com) at no cost.

## SCALABLE, CENTRALIZED SECURITY MANAGEMENT ENABLES OPERATIONAL EFFICIENCY

The security services delivered by the Cisco Security Starter Bundle are managed by CiscoWorks VMS Basic v2.2, an entry-level scalable security management solution. CiscoWorks VMS Basic is a suite of integrated Web-based tools for configuring, monitoring, and troubleshooting security services, including VPNs, firewalls, and network- and host-based IDSs and IPSs for small and medium-sized businesses. It provisions and monitors the Cisco PIX 515E Security Appliance and Cisco Security Agent solutions that are part of this bundle, as well as other Cisco security solutions, including Cisco IPS sensor appliances. CiscoWorks VMS supports up to three Cisco security devices and an unlimited number of Cisco Security Agents. As business networks grow to more devices, CiscoWorks VMS grows through upgrade licenses.

## PRODUCT AND SUPPORT ORDERING INFORMATION

Table 1 lists ordering information for the Cisco Security Starter Bundle and associated Cisco SMARTnet<sup>®</sup> service part numbers.

**Table 1.** Ordering Information for Cisco Security Starter Bundle and Support Contracts

Part Number	Product Description
PIX515E-DMZ-CSA-K9	The Cisco Security Starter Bundle includes: <ul style="list-style-type: none"><li>• One Cisco PIX 515E Security Appliance with three 10/100 Fast Ethernet ports and a Restricted Software License</li><li>• One Cisco Security Agent license for Servers</li><li>• Ten Cisco Security Agent licenses for Desktops</li><li>• CiscoWorks VPN/Security Management Solution (VMS) Basic</li><li>• Unlimited Cisco VPN Client software licenses</li></ul>
CON-SNT-PXDMZCSA	Cisco SMARTnet 8x5xNBD Threat Defense Bundle
CON-SNTE-PXDMZCSA	Cisco SMARTnet 8x5x4 Threat Defense Bundle
CON-S2P-PXDMZCSA	Cisco SMARTnet 24x7x2 Threat Defense Bundle
CON-SNTP-PXDMZCSA	Cisco SMARTnet 24x7x4 Threat Defense Bundle
CON-OS-PXDMZCSA	Cisco SMARTnet Onsite 8x5xNBD Threat Defense Bundle
CON-OSE-PXDMZCSA	Cisco SMARTnet Onsite 8x5x4 Threat Defense Bundle
CON-PREM-PXDMZCSA	Cisco SMARTnet Onsite 24x7x2 Threat Defense Bundle
CON-OSP-PXDMZCSA	Cisco SMARTnet Onsite 24x7x4 Threat Defense Bundle

## EXPORT CONSIDERATIONS

Cisco Threat Defense bundles are subject to export controls. Export compliance guidance is available at: <http://www.cisco.com/wwl/export/crypto/>

For specific export questions, contact: [export@cisco.com](mailto:export@cisco.com)

## FOR MORE INFORMATION

For more information, please visit the following links:

Cisco PIX 515E Security Appliance: <http://www.cisco.com/go/pix>

Cisco PIX Device Manager: <http://www.cisco.com/go/pdm>

Cisco Security Agent Software: <http://www.cisco.com/go/csa>

CiscoWorks VMS, CiscoWorks Management Center, and Cisco Security Agent: <http://www.cisco.com/go/vms>

Cisco VPN Client Software: <http://www.cisco.com/go/vpnclient>

Cisco Threat Defense System: <http://www.cisco.com/go/tds>



### Corporate Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://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](http://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](http://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](http://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](http://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

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R) 205227.d\_ETMG\_MH\_3.05

