CHAPTER 5

VPN and Security

VPN and Security Products at a Glance

Product	Features	Page
Cisco PIX Security Appliance	Market-leading, purpose-built appliances which provide broad range of integrated security services • Robust stateful inspection firewalling with advanced application and protocol inspection • High-performance and scalable remote access and site-to-site VPN • Inline intrusion prevention for real-time response to network attacks • Enhanced routing and network integration • Extensive support for multimedia and VoIP applications • Award-winning firewall stateful failover for enterprise-class resiliency	5-2
Firewall Blade for Catalyst 6500	Firewall Module is a high performance integrated stateful firewall solution for Catalyst 6500 family of switches with performance exceeding 5GB. It is based on proven PIX technology while providing the following benefits to the customers • Investment protection • Low cost of ownership • Ease of use • Operational Consistency • Scalability See the Catalyst 6500 Series Switch in Chapter 2: LAN Switching, page 2-21, for more information	2-21
Cisco VPN 3000 Family	Remote access Virtual Private Network platform • Supports IPsec and SSL (WebVPN) remote connectivity • Has models for all size companies, from small to large enterprise organizations • Reduces communications expenditures • Enables users to easily add capacity and throughput	5-5
Cisco Security Agent	Provides threat protection for desktop and server computing systems by identifying and preventing malicious activity: • Aggregates and extends multiple endpoint security functions • Protects against know and unknown attacks on both servers and desktops; Protects against entire classes of attacks including Port Scans, Buffer Overflows, Trojan Horses, Malformed Packets, malicious HTML requests and e-mail worms • Stops new and unknown attacks without needing signature update, and reduces security management cost associated with deploying updates • Scalable to 100,000 agents per management server • Compliant with SDN/NAC Cisco Trust Agent. Integrated management with Cisco PIX, Cisco Secure IDS, and Cisco VPN security devices and built-in Cisco Secure VPN "Are You There" (AYT)	5-9
Cisco Secure Access Control Server (ACS) for Windows	Provides a comprehensive identity networking solution and secure user experience for Cisco intelligent information networks. It is the integration and control layer among all enterprise users, administrators, and the resources of the network infrastructure	5-10
Cisco Secure Access Control Server (ACS) Solution Engine	A high-performance and highly scalable user and administrative access control solution that operates as a centralized RADIUS or TACACS+ server system in a turnkey security-hardened solution	5-12
Cisco Secure User Registration Tool (URT)	Identifies users within the network and creates user registration policy bindings that help support mobility and tracking: • Ensures that users are associated with their authorized subnet/VLAN • Addresses the challenges associated with campus user mobility • Supports Web-based authentication for Windows, Macintosh, and Linux client platforms • Secure user access to the VLAN with MAC address-based security option • Option to allow multiple users connected to a hub to access a VLAN served by a single switch port	5-13

Product	Features	Page
CiscoWorks VPN/Security Management Solution	Combines general device management tools for configuring, monitoring, and troubleshooting enterprise networks with powerful security solutions for managing virtual private networks (VPNs), firewalls, and network and host-based intrusion detection systems (IDS). An integral part of the Cisco SAFE Blueprint for Enterprise, this bundle also delivers network device inventory, change audit and software distribution features. CiscoWorks VMS is organized into several functional areas: Firewall Management, IDS Management, network and host-based, VPN Router Management, Security Monitoring, VPN Monitoring, and Operational Management See Chapter 9-1—IOS Software & Network Management for more information on CiscoWorks VPN/Security Management Solution	9-12
CiscoWorks Security Information Management Solution and CiscoWorks Security Information Management Solution Engine	A solution that collects, analyzes, and correlates security event data from across the enterprise- letting you detect and respond to security events as they occur. • Event monitoring of multivendor security environments • Extensive reporting for operators and high-level administrators • Risk assessment information to understand overall vulnerability of critical network assets within the enterprise; Forensics tools to investigate attacks • Traffic utilization reports and graphs to understand changes in traffic patterns See Chapter 9-1—IOS Software & Network Management for more information on CiscoWorks Security Information Management Solution	9-14
Cisco IOS Firewall	• Tightly integrated with IOS VPN and advanced routing technologies • Application aware stateful packet inspection via context-based access control (CBAC) for TCP, UDP, SIP, Skinny, H.323 and others • Supports user authentication for https, ftp and telnet connections • URL filtering through router exclusive domains or use of external Websense and N2H2 servers • Inline intrusion prevention for real-time response to network attacks supporting 100 common attack signatures • Dynamic, network-to network, per-user authentication and authorization via TACACS+ and RADIUS	5-14
Cisco Security Router Bundles	Cisco 800, 1700, 1800, 2600, 2800 , 3700, 3800 7200 and 7301 Security Router Bundles with Enhanced Integrated Network Security. See individual product pages for more detail (page 1-1)	1-1
Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200, and 7301	Wide variety of modular router platforms with options for Cisco IOS-based and hardware-enabled VPN, Cisco IOS Firewall, Intrusion Prevention, Network Admission Control (NAC), and security support.	1-1

Cisco PIX Security Appliance Series

The world-leading Cisco PIX® Security Appliance Series provides enterprise-class, integrated network security services including stateful inspection firewalling, protocol and application inspection, virtual private networking (VPN), in-line intrusion protection, rich multimedia and voice security in cost-effective, easy-to-deploy solutions. Ranging from compact, “plug-and-play” desktop firewalls for small offices to carrier-class gigabit firewalls for the most demanding enterprise and service-provider environments, Cisco PIX Security Appliances provide robust security, performance, and reliability for network environments of all sizes.

When to Sell

Sell This Product	When a Customer Needs These Features
PIX 501	• Small Office / Home Office desktop integrated security appliance • Up to 60 Mbps of firewall throughput • Up to 3 Mbps of 3DES and 3.4 Mbps of AES-256 IPsec VPN throughput[1] • Hardware VPN client (Easy VPN Remote) • VPN concentrator services (Easy VPN Server) for up to 10 remote users • Integrated four port 10/100 Mbps switch
PIX 506E	• Remote Office / Branch Office desktop integrated security appliance • Up to 100 Mbps of firewall throughput • Up to 16 Mbps of 3DES and 30 Mbps of AES-256 IPsec VPN throughput[1] • Hardware VPN client (Easy VPN Remote) • VPN concentrator services (Easy VPN Server) for up to 25 remote users • Maximum of two 10BASE-T Ethernet interfaces • OSPF dynamic routing support

Sell This Product	When a Customer Needs These Features
PIX 515E	• Small-to-Medium Business (SMB) integrated security appliance • Up to 190 Mbps of firewall throughput[1] • Up to 130 Mbps of 3DES/AES-256 VPN throughput[1] using hardware acceleration (integrated in select models, optional for others) • VPN concentrator services (Easy VPN Server) for up to 2,000 remote users • Up to six 10/100 FE interfaces • VLAN trunking (802.1q tag-based) and OSPF dynamic routing support • Active/standby firewall stateful failover support
PIX 525	• Enterprise-class integrated security appliance • Up to 330 Mbps of firewall throughput[1] • Up to 145 Mbps of 3DES and 135 Mbps of AES-256 VPN throughput[1] using hardware acceleration (integrated in select models, optional for others) • VPN concentrator services (Easy VPN Server) for up to 2,000 remote users • Gigabit Ethernet support; Up to eight 10/100 FE or three Gigabit Ethernet interfaces • VLAN trunking (802.1q tag-based) and OSPF dynamic routing support • Active/standby firewall stateful failover support
PIX 535	• Carrier class large enterprise and service provider firewall appliance • Up to 1.7 Gbps of firewall throughput[1] • Up to 425 Mbps of 3DES/AES-256 VPN throughput using hardware acceleration (integrated in select models, optional for others) • VPN concentrator services (Easy VPN Server) for up to 2,000 remote users • Gigabit Ethernet throughput; Up to ten 10/100 FE or nine Gigabit Ethernet interfaces • VLAN trunking (802.1q tag-based) and OSPF dynamic routing support • Redundant, hot-swappable power supplies • Active/standby firewall stateful failover support

1. At 1400-byte packets

Key Features

- Security—Purpose-built appliance with a proprietary, hardened operating system
- Performance—Stateful inspection firewall capable of up to 500,000 concurrent connections and 1.7 Gbps of throughput (at 1400-byte packets on Cisco PIX 535 Security Appliances)
- High availability—Award-winning, active/standby firewall stateful failover provides enterprise-class, cost-effective resiliency
- Virtual Private Networking (VPN)—Supports both standards-based IPsec and L2TP/PPTP-based VPN services
- Optional PIX VPN Accelerator Card+—Scales 3DES/AES-256 VPN throughput up to 495 Mbps, using specialized co-processors designed for accelerating cryptographic operations
- Free software Cisco VPN Client provides secure connectivity across a broad range of platforms including Windows, Mac OS X, Linux and Solaris
- Network Address Translation (NAT) and Port Address Translation (PAT)—Conceals internal IP addresses and expands network address space
- Denial-of-Service (DoS) Attack Protection—Protects the firewall, internal servers and clients from disruptive hacking attempts
- OSPF dynamic routing support for improved network reliability and performance
- VLAN trunking (802.1q tag) support for simplified deployment in switched network environments
- Multimedia and VoIP support for widely popular standards, H.232 v4, TAPI, JTAPI, RTSP, SIP, MGCP and SCCP
- Web-Based PIX Device Manager (PDM)—For simplified configuration, real-time and historical reports, performance baselines and security events information
- Auto Update, SSH, SNMP, TFTP, HTTPS, and telnet for remote management
- Support from two 10/100 Ethernet interfaces to up to nine Gigabit Ethernet interfaces

Competitive Products

- Check Point Software: FireWall-1 / VPN-1
- NetScreen: NetScreen Security Appliances
- Nokia: IP-Series Security Appliances
- SonicWALL: SonicWALL Security Appliances
- WatchGuard Technologies: Firebox-series and V-series Security Appliances

Specifications

Feature	PIX 501	PIX 506E	PIX 515E	PIX 525	PIX 535
Processor	133 MHz	300 MHz	433 MHz	600 MHz	1.0 GHz
RAM	16 MB	32 MB	32 or 64 MB	128 or 256 MB	512 MB or 1 GB
Flash Memory	8 MB	8 MB	16 MB	16 MB	16 MB
PCI Slots	None	None	2	3	9
Fixed Interfaces (Physical)	Four port 10/100 switch (inside), One 10Base-T Ethernet (outside)	Two 10Base-T Ethernet	Two 10/100 Fast Ethernet	Two 10/100 Fast Ethernet	None
Maximum Interfaces (Physical and Virtual)	Four port 10/100 switch (inside), One 10Base-T Ethernet (outside)	Two 10Base-T Ethernet or 2 VLANs	Six 10/100 Fast Ethernet (FE) or 8 VLANs	Eight 10/100 FE or GE or 10 VLANs	Ten-10/100 FE or GE or 24 VLANs
VPN Accelerator Card+ (VAC+) Option	No	No	Yes, integrated in select models	Yes, integrated in select models	Yes, integrated in select models
Failover Support	No	No	Yes, UR/FO models only	Yes, UR/FO models only	Yes, UR/FO models only
Size	Desktop	Desktop	1 RU	2 RU	3 RU

Selected Part Numbers and Ordering Information[1]

Cisco PIX Bundles

PIX-535-UR-BUN	PIX 535 Unrestricted Bundle (Chassis, unrestricted software, two 10/100 ports, VPN Accelerator Card+)
PIX-535-R-BUN	PIX 535 Restricted Bundle (Chassis, restricted software, two 10/100 ports)
PIX-535-FO-BUN	PIX 535 Failover Bundle (Chassis, failover software, two 10/100 ports, VPN Accelerator Card+)
PIX-525-UR-GE-BUN	PIX 525 Unrestricted GE Bundle (Chassis, unrestricted software, two GE ports, two 10/100 ports, VPN Acceleration Card+)
PIX-525-FO-GE-BUN	PIX 525 Failover GE Bundle (Chassis, failover software, two GE ports, two 10/100 ports, VPN Acceleration Card+)
PIX-525-UR-BUN	PIX 525 Unrestricted Bundle (Chassis, unrestricted software, two 10/100 ports, VPN Accelerator Card+)
PIX-525-R-BUN	PIX 525 Restricted Bundle (Chassis, restricted software, two 10/100 ports)
PIX-525-FO-BUN	PIX 525 Failover Bundle (Chassis, failover software, two 10/100 ports, VPN Accelerator Card+)
PIX-515E-UR-FE-BUN	PIX 515E Unrestricted Bundle (Chassis, unrestricted software, six 10/100 ports, VPN Accelerator Card+)
PIX-515E-FO-FE-BUN	PIX 515E Failover Bundle (Chassis, failover software, six 10/100 ports, VPN Accelerator Card+)
PIX-515E-UR-BUN	PIX 515E Unrestricted Bundle (Chassis, unrestricted software, two 10/100 ports, VPN Accelerator Card+)
PIX-515E-R-BUN	PIX 515E Restricted Bundle (Chassis, restricted software, two 10/100 ports)
PIX-515E-FO-BUN	PIX 515E Failover Bundle (Chassis, failover software, two 10/100 ports, VPN Accelerator Card+)
PIX-515E-R-DMZ-BUN	PIX 515E DMZ Bundle (Chassis, restricted software, three 10/100 ports)
PIX-506E-BUN-K9	PIX 506E 3DES/AES Bundle (Chassis, software, 3DES/AES license, two 10-BaseT ports)2
PIX-501-BUN-K9	PIX 501 10 User/3DES/AES Bundle (Chassis, SW, 10 user/3DES/AES license, 4 port 10/100 switch)
PIX-501-50-BUN-K9	PIX 501 50 User/3DES/AES Bundle (Chassis, SW, 50 user/3DES/AES license, 4 port 10/100 switch)
PIX-501-UL-BUN-K9	PIX 501 Unlimited User/3DES/AES Bundle (Chassis, SW, Unlimited Users 3DES/AES license, 4 port 10/100 switch)

Cisco PIX Interfaces and Cards

PIX-1GE-66	PIX 66-MHz Single-port Gigabit Ethernet interface card (multimode fiber, SC connector)
PIX-4FE-66	PIX 66-MHz Four-port 10/100 Fast Ethernet interface card, RJ45
PIX-1FE	PIX Single-port 10/100 Fast Ethernet interface card
PIX-VPN-ACCEL	PIX DES/3DES VPN Accelerator Card (VAC)
PIX-VPN-PLUS	PIX DES/3DES/AES VPN Accelerator Card+ (VAC+)

PIX Accessories	
PIX-506E-PWR-AC	Redundant AC power supply for PIX 506E
PIX-515-PWR-DC	Redundant DC power supply for PIX 515/515E

1. This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the PIX Security Appliance Web site: **http://www.cisco.com/go/pix**

Cisco VPN 3000 Family

The Cisco VPN 3000 Series Concentrator is a best-in-class, remote-access VPN solution for enterprise-class deployment. A standards-based, easy-to-use VPN client and scalable VPN tunnel termination devices are included, as well as a management system that enables corporations to easily install, configure, and monitor their remote access VPNs. Remote connections can be established either from a SSL-capable Web browser or an installed VPN Client, allowing for maximum flexibility and application access without the need to deploy and manage multiple unique devices for secure corporate or partner application access. Incorporating the most advanced, high-availability capabilities with a unique purpose-built, remote-access architecture, it allows corporations to build high-performance, scalable, and robust VPN infrastructures to support their mission-critical, remote-access applications.

Unique to the industry, it is the only scalable platform to offer components that are field-swappable and can be upgraded by the customer. These components, called Scalable Encryption Processing (SEP/SEP-E) modules, enable users to easily add capacity and throughput.

The Cisco VPN 3000 Series Concentrator supports the widest range of connectivity options, including WebVPN (Clientless using a Web browser), the Cisco VPN Client, the Microsoft L2TP/IPSec, and Microsoft PPTP.

When to Sell

Sell This Product	When a Customer Needs These Features
VPN 3005 and 3015 Concentrators	Cisco VPN 3005 Concentrator • Designed for small to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4 Mbps maximum performance) with support for up to 200 simultaneous IPSec sessions or 50 simultaneous clientless sessions • Encryption processing is performed in software • Does not have built-in upgrade capability Cisco VPN 3015 Concentrator • Designed for small- to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4 Mbps maximum performance) and up to 100 simultaneous IPSec sessions or 75 simultaneous clientless sessions • Encryption processing is performed in software • Field-upgradable to the Cisco VPN 3030 and 3060 models
VPN 3020 Concentrator	• Designed for medium to large organizations with bandwidth requirements from full T1/E1 through T3/E3 (50 Mbps maximum performance) with support for up to 750 simultaneous IPSec sessions or 200 simultaneous clientless sessions • Specialized SEP modules (SEP-E) perform hardware-based acceleration • Cannot be upgraded to other products in the family • Redundant and nonredundant configurations are available

Sell This Product	When a Customer Needs These Features
VPN 3030 and 3060 Concentrators	Cisco VPN 3030 Concentrator • Designed for medium to large organizations with bandwidth requirements from full T1/E1 through T3/E3 (50 Mbps maximum performance) with support for up to 1,500 simultaneous IPSec sessions or 500 simultaneous clientless sessions • Specialized SEP modules perform hardware-based acceleration • Field upgradeable to the Cisco VPN 3060 • Redundant and nonredundant configurations are available Cisco VPN 3060 Concentrator • Designed for large organizations demanding the highest level of performance and reliability, with high-bandwidth requirements from fractional T3 through full T3/E3 or greater (100 Mbps maximum performance) with support for up to 5,000 simultaneous IPSec sessions or 500 simultaneous clientless sessions • Specialized SEP modules perform hardware-based acceleration • Redundant and nonredundant configurations are available
VPN 3080 Concentrator	• Optimized to support large enterprise organizations that demand the highest level of performance combined with support for up to 10,000 simultaneous IPSec sessions or 500 simultaneous clientless sessions • Specialized SEP modules perform hardware-based acceleration • Available in a fully redundant configuration only
VPN Client	• Simple to deploy and operate • Used to establish secure, end-to-end encrypted tunnels to the Cisco VPN 3000 Concentrator and other Cisco Easy VPN compliant devices • Thin design, IPSec-compliant implementation is provided • Licensed for an unlimited number of users • Client can be pre-configured for mass deployments and the initial logons require very little user intervention • VPN access policies are created and stored centrally and pushed to the client when a connection is established • Provided at no charge, installs on PCs and is available for Windows, Mac OS X and Linux Intel/Solaris UltaSparc environments
VPN 3002 Hardware Client	• Emulates the software client in hardware • Ideal for mixed operating system environments and where a corporation does not own/control remote PCs or for very large applications requiring large number of devices due to ease of deployment, upgradability & scalability

Key Features

- Cisco VPN 3000 Concentrators Series
  - Support for industry standard IPSec DES/3DES/AES and Cisco IPSec/NAT for VPN Access through Port Address Translation firewalls
  - Unlimited-use license for Cisco VPN Client distribution included at no cost with multiple OS support including Windows, MAC OS X, Linux and Solaris; also integrates with Zone Alarms personal firewall
  - Supports standard authentication: RADIUS, SDI Tokens, and Digital Certificates
  - VPN load balancing allows for multiple units to cluster as a single shared pool
- Cisco VPN 3002 Hardware Client supports up to 253 users/stations per VPN 3002
  - Works with most operating systems including Windows, Linux, Solaris, and MAC OS X
  - Auto-upgrade capability automates upgrades with no user intervention required
  - Client technology employs push policy and automatic address assignment from the central site concentrator, enabling virtually unlimited scalability

Competitive Products

- Nortel: Contivity products (IPsec)
- Juniper (Neoteris): SSL VPN Secure Access products
- Juniper (Netscreen): LAN to LAN environments
- Nokia

Specifications

Cisco VPN 3000 Series Concentrators

Feature	VPN 3005	VPN 3015	VPN 3020	VPN 3030	VPN 3060	VPN 3080
Simultaneous IPSec Users	200	100	750	1500	5000	10000
Simultaneous WebVPN (Clientless) Users	50	75	200	500	500	500
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	50 Mbps	100 Mbps	100 Mbps
Encryption Method	Software	Software	Hardware	Hardware	Hardware	Hardware
Encryption (SEP) Module	0	0	1	1	2	4
Redundant SEP	No	No	Optional	Optional	Optional	Yes
Expansion Slots	0	4	1 (Redundant)	3	2	N/A
Upgradeable	No	Yes		Yes	N/A	N/A
Memory	32/64 MB (fixed)	128 MB	256 MB	128-512 MB	256/512 MB	256/512MB
Hardware Configuration	1U, Fixed	2U, Scalable	Fixed 2U	2U, Scalable	2U, Scalable	2U
Power Supply	Single	Single, with a dual option	Single, with a dual option	Single, with a dual option	Single, with a dual option	Dual
Client License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
LAN-to-LAN Connections (internal user database)	100	100	250	500	1000	1000
Dimensions (HxWXD)	1.75 x 17.5 x 11.5 in.	3.5 x 17.5 x 14.5 in.	3.5 x 17.5 x 14.5 in.	3.5 x 17.5 x 14.5 in.	3.5 x 17.5 x 14.5 in.	3.5 x 17.5 x 14.5 in.

Cisco VPN 3002 Hardware Client

Feature	VPN 3002 Hardware Client
Hardware Processor	Motorola PowerPC processor; Dual flash image architecture
Network Interfaces	CPVN3002-K9: One Public 10/100Mbps RJ-45 Ethernet Interface and One Private Port 10/100Mbps RJ-45 Ethernet Interface
	CVPN3002-8E-K9: One Public 10/100Mbps RJ-45 Ethernet Interface and Eight Private Port 10/100Mbps RJ-45 Ethernet Interfaces via AUTO-MDIX switch
Physical Dimensions	1.967 x 8.6 x 6.5 in. (5 x 8.6 x 16.51 cm)
Power Supply	External AC Operation: 100-240V at 50/60 Hz with universal power factor correction; 4 foot cord included and international "pigtail" power cord selection
Tunneling Protocol Support	IPsec with IKE key management
Monitoring & Configuration	Event logging; SNMP MIB-II support
	Embedded management interface is accessible via console port or local web browser; SSH/SSL
Encryption Algorithms, Key Management & Authentication Algorithms	56-bit DES (IPsec); 168-bit Triple DES (IPsec); AES 128 & 256-bit (IPsec)
Authentication and Accounting Servers	Support for redundant external authentication servers including RADIUS
	Microsoft NT Domain authentication, X.509v3 Digital Certs (PKC7-PKCS10)
Configuration Modes	Client Mode—acts as client, receives random IP address from Concentrator Pool; Uses NAPT to hide stations 3002; Network behind 3002 is unroutable; few configuration parameters
	Network Extension Mode—acts as site-to-site device; Uses NAPT to hide stations only to Internet (stations visible to central site); Network behind 3002 is routable; additional configuration parameters

Selected Part Numbers and Ordering Information[1]

Cisco VPN 3000 Concentrator

CVPN3005-E/FE-BUN	VPN3005:Chassis, 2FE, 200 user, client, SW, US PWR
CVPN3015-NR-BUN	VPN3015:Chassis, 3FE, 100 user, client, SW, US PWR
CVPN3020E-NRBUN-K9	VPN3020:Chassis, 3FE, SEP-E, 750 user, client, SW, US PWR
CVPN3020E-RDBUN-K9	VPN3020:Chassis, 3FE, 2SEP-E, 750 user, client, SW, 2 US PWR
CVPN3030E-NRBUN-K9	VPN3030:Chassis, 3FE, SEP-E, 1500 user, client, SW, US PWR
CVPN3030E-RDBUN-K9	VPN3030:Chassis, 3FE, 2SEP-E, 1500 user, client, SW, 2 US PWR
CVPN3060E-NRBUN-K9	VPN3060:Chassis, 3FE, 2SEP-E, 5k user, client, SW, US PWR
CVPN3060E-RDBUN-K9	VPN3060:Chassis, 3FE, 4SEP-E, 5k user, client, SW, 2 US PWR
CVPN3080E-RDBUN-K9	VPN3080:Chassis, 3FE, 4SEP-E, 10k user, client, SW, 2 US PWR

Cisco VPN 3000 Series Upgrades

CVPN3000-UKITA-K9=	1SEP-E,1PS,512MB memory,4.0 OS and boot,client SW
CVPN3000-UKITB-K9=	2SEP-E,1PS,512MB memory,4.0 OS and boot,client SW
CVPN3000-UKITC-K9=	3SEP-E,1PS,512MB memory,4.0 OS and boot,client SW
CVPN3000-UKITD-K9=	4SEP-E,1PS,512MB memory,4.0 OS and boot,client SW

Cisco VPN 3000 Series Accessories	
CVPN3000-PWR=	Cisco VPN 3000 Concentrator Power Supply
CVPN30XX-MEMKITK9=	VPN 3030, 3060, 3080: 2x256MB RAM
Cisco VPN 3000 Series Basic Maintenance	
CON-SNT-PKG4	SMARTnet Maintenance for Cisco CVPN3005-E/FE-BUN
CON-SNT-PKG8	SMARTnet Maintenance for Cisco CVPN3015-NR-BUN
CON-SNT-PKG11	SMARTnet Maintenance for Cisco CVPN3030-NR-BUN
CON-SNT-PKG13	SMARTnet Maintenance for Cisco CVPN3030-RED-BUN
CON-SNT-PKG14	SMARTnet Maintenance for Cisco CVPN3060-RED-BUN
Cisco VPN Client	
CVPN-CLIENT-K9=	Cisco VPN Client CD (included with Concentrator purchase)

For More Information

See the Cisco VPN 3000 series Web site: **http://www.cisco.com/go/vpn3000**

Cisco Security Router Bundles with Integrated Network Security

The Cisco Security Router Bundles are based on the Cisco 800, 1700, 1800, 2600XM, 2691, 2800, 3700, 3800 7200 and 7301 router platforms. They include the Entry Security bundles, Enhanced Security bundles for added performance and scale, and V3PN bundles for combined Security and IPCommunications.

Key Features

- Single part number when ordering a Cisco router with all the necessary Security components at a reduced price compared to ordering each component separately
- All Security bundles come pre-installed with Router and Security Device Manager (SDM) for fast and easy deployment based on Cisco TAC and ICSA Labs recommended router security configurations
- Offers bundled Cisco IOS since Cisco 800 Series, 1711and 1712 offer embedded VPN acceleration
- Cisco 1700, 2600XM, 2691, 3700, 7200 and 7301 bundles include the selected router platform, a VPN hardware card, additional memory, and the Cisco IOS to run IPSec 3DES or AES encryption
- Cisco 2600XM, 2800, 3700, and 3800 Series now have Advanced Security Network Modules available for ULR Filtering and hardware-based IDS(Intrusion Detection System)
- For modular platforms, each Security bundle has optional modules

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco VPN Security Router Bundles	• Combatting worms, viruses or threats from every gateway to the network (NAC, firewall, IPS) • Deploying VPN on routers and want to have future option for VPN • Planning to use the Internet for remote business communications (remote access VPN) • When migrating from leased lines to VPN • Need encryption to protect customer data (i.e HIPAA, Sarbanes-Oxley) • Needs to integrate Voice and VPN Services (V3PN) • New Integrated Services Routers (Cisco 1800, 2800, and 3800) have embedded VPN acceleration, so corresponding Security bundles are necessary to enable the 3DES or AES encryption functionality

Specifications

Feature	Cisco VPN Security Router Bundles
All Bundles Include	Network Admission Control (NAC) Firewall with IPS; GRE and IPSec; High Availability/Failover; VPN QoS; AES in Hardware (excluding C1700 Bundles)
IPPCP Compression	Software: C800, C1700 Bundles Hardware: Cisco 1800 bundles, C2600XM, C2691-VPN, Cisco 2800 bundles, C3725-VPN, C3745-VPN, Cisco 3800, 7200, 7301 Bundles
Max Tunnel	C800 - 10, C1700: 100; Cisco 1800: 800,C2600XM, C2691-VPN: 800; Cisco 2800: 1500; C3725-VPN, C3745-VPN: 2000; Cisco 3800: 2500; 7200/7301 Bundles: 5000
Firewall Performance	C800 - 10Mbps, C1700: 20Mbps; Cisco 1800: 125 Mbps,C2600XM: 35Mbps; C2691-VPN: 197Mbps; Cisco 2800: 530Mbps; C3725-VPN, C3745-VPN: 197 Mbps; Cisco 3825: 855Mbps; Cisco 3845:1 Gbps, 7200/7301 Bundles: 1Gbps

For More Information

See Chapter 1: Routing for more details.

Cisco Security Agent

The next-generation Cisco Security Agent network security software provides threat protection for server and desktop computing systems, also known as “endpoints.” The Cisco Security Agent goes beyond conventional host and desktop security solutions by identifying and preventing malicious behavior that threaten enterprise networks and applications before it can occur. It aggregates and extends multiple endpoint security functions by providing host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation all within a single agent package.

The Cisco Security Agent analyzes behavior rather than relying on signature matching, its solution provides robust protection with reduced operational costs. It provides patch relief to reduce the system administration workload allowing companies to wait for “roll-ups” and Service Packs, which come better qualified from the vendor. Testing and implementation of updates can be scheduled without undue change control interruption. Fewer updates reduce the cost of ownership.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Security Agent	• Host intrusion protection, distributed firewall, malicious mobile code protection, operating system hardening, file integrity and/or audit log consolidation. The Cisco Security Agent provides all of these features in one integrated package • Protection against both known and unknown attacks • Protection for servers and/or desktops/laptops • A solution that is scalable to protect thousands of servers and desktops for large enterprise deployments • Provides endpoint protection enabling businesses to participate in e-commerce securely and take advantage of the Internet economy

Key Features

- Provides industry-leading protection for Unix and Windows servers
- Multiple security functions in a single agent
- Open, extensible architecture offers the capability to define and enforce security according to corporate policy
- “Zero Update” prevention for known and unknown attacks
- Integrates with Cisco Network Security Products
- Provides application inventory and use tracking, hotfix and Service Pack status checking, and antivirus DAT version check for Symantec and McAfee antivirus agents
- A key component of the SAFE blueprint for secure e-business

Competitive Products

- Internet Security Systems (ISS)
- Symantec: Intruder Alert
- Enterasys: Squire
- Sana Security: Primary Response
- NAI: Entercept
- NFR (Centrax)

Specifications

Feature	Cisco Security Server Agent	Cisco Security Desktop Agent	Cisco Security Agent Manager
Platforms	Windows 2000 Server and Advanced Server (up to Service Pack 3)	Windows NT v4.0 Workstation (Service Pack 5 or later)	Microsoft Windows 2000 Server and Advanced Server (up to SP 2)
	Windows NT v4.0 Server and Enterprise Server (Service Pack 5 or later)	Windows 2000 Professional (up to Service Pack 3)	
	Solaris 8 SPARC architecture (64-bit kernel)	Windows XP Professional (up to Service 1)	

Selected Part Numbers and Ordering Information[1]

Cisco Security Agent Options

CSA-SRVR-K9=	Cisco Security Server Agent (Win + Sol), 1 Agent
CSA-B10-SRVR-K9	Cisco Security Server Agent (Win + Sol), 10 Agent Bundle
CSA-B25-SRVR-K9	Cisco Security Server Agent (Win + Sol), 25 Agent Bundle
CSA-B50-SRVR-K9	Cisco Security Server Agent (Win + Sol), 50 Agent Bundle
CSA-B100-SRVR-K9	Cisco Security Server Agent (Win + Sol), 100 Agent Bundle
CSA-B25-DTOP-K9	Cisco Security Desktop Agent (Win + Sol), 25 Agent Bundle
CSA-B100-DTOP-K9	Cisco Security Desktop Agent (Win + Sol), 100 Agent Bundle
CSA-B250-DTOP-K9	Cisco Security Desktop Agent (Win + Sol), 250 Agent Bundle
CSA-B500-DTOP-K9	Cisco Security Desktop Agent (Win + Sol), 500 Agent Bundle
CSA-B500-SRVR-K9	Cisco Security Server Agent (Win + Sol), 500 Agent Bundle
CSA-B1000-DTOP-K9	Cisco Security Desktop Agent (Win + Sol), 1000 Agent Bundle
CSA-B5000-DTOP-K9	Cisco Security Desktop Agent (Win + Sol), 5000 Agent Bundle
CSA-PROFILER-K9	Cisco Security Agent Profiler

Note **Export Considerations:** The Cisco Security Agent is subject to export controls. Please refer to the export compliance Web site at **http://www.cisco.com/wwl/export/crypto** for guidance. For specific export questions, please contact **export@cisco.com**.

For More Information

See the Cisco Security Agent Web site: **http://www.cisco.com/go/csa**

Cisco Secure Access Control Server (ACS) for Windows

Cisco Secure ACS is a highly scalable, high-performance access control server that operates as a centralized RADIUS server or TACACS+ server. It extends access security by combining authentication, user or administrator access, and policy control from a centralized identity networking solution, allowing greater flexibility and mobility, increased security, and user productivity gains. It reduces the administrative and management burden involved in scaling user and network administrative access to your network. By using a central database for all user accounts, it centralizes the control of all user privileges and distributes them to hundreds or thousands of access points throughout the network. As an accounting service, the Cisco Secure ACS reduces IT operating costs by providing detailed reporting and monitoring capabilities of network users' behavior and by keeping a record of every access connection and device configuration change across the entire network. The Cisco Secure ACS supports a wide array of access connection types, including wired and wireless LAN, dialup, broadband, content, storage, voice over IP, firewalls, and VPNs.

The Cisco Secure ACS is a key component of the Cisco Identity-Based Networking Services (IBNS) architecture and of Cisco Network Admission Control (NAC).

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Secure Access Control Server (ACS) for Windows	• Centrally manage who can log in to the network from wired or wireless connections • Privileges each user has in the network • Accounting information recorded in terms of security audits or account billing • What access and command controls are enabled for each configuration administrator • Virtual VSA for Aironet rekey • Secure server authentication and encryption • Simplified firewall access and control through Dynamic Port Assignment • Same User AAA services

Key Features

- Cisco NAC support—Using policies that you configure, it evaluates the credentials sent to it by Cisco Trust Agent, determines the state of the host, and sends the AAA client ACLs that are appropriate to the host state; records the results of policy evaluation for use with your monitoring system
- Supports the new, publicly accessible IEEE 802.1X EAP type developed by Cisco to support customers who cannot enforce a strong password policy and who wish to deploy an 802.1X EAP; Does not require digital certificates, and supports a variety of user and password database types, password expiration and change, and is flexible, easy to deploy, and easy to manage
- Downloadable IP access control lists (ACLs)—Extends per-user ACL support to any Layer 3 network device that supports this feature; Allows for custom defined sets of ACLs that can be applied per user or per group
- Certification Revocation List (CRL) comparison for EAP-Transport Layer Security (TLS) authentication—Adds support for certificate revocation using the X.509 CRL profile; Cisco Secure ACS fails the authentication and denies access to the user if the certificate presented by the user during an EAP-TLS authentication is present in the retrieved CRL
- Machine Access Restrictions (MARs) that complement 802.1X machine authentication—Ability to use MARs to control authorization of EAP-TLS and Microsoft Protected Extensible Authentication Protocol (PEAP) users who authenticate with a Windows external user database
- Network access filtering (NAF) as a new shared profile component—Introduces granular application of network access restrictions and downloadable ACLs, both of which previously supported only the use of the same access restrictions or ACLs to all devices
- Allows replication of the user and group databases separately

Competitive Products

- Funk: Steel Belted RADIUS
- Lucent/Avaya: Security Management Server (LSMS)
- Nortel: Preside RADIUS Server (OEM of Funk product)

Specifications

Feature	Cisco Secure Access Control Server (ACS) for Windows
Hardware	• Pentium processor, 550 MHz or faster • 256 MB RAM • 250 MB free disk space, more if you are running your database on the same device • Minimum resolution of 800 x 600 with 256 colors

Selected Part Numbers and Ordering Information[1]

Cisco Secure Access Control Server (ACS) for Windows

CSACS-3.3-WIN-K9	Cisco Secure ACS 3.3 for Windows
CSACS-3.3-WINUP-K9	Upgrade to CSACS 3.3 for Windows from ACS versions 1.x, 2.x, and Cisco Secure ACS for Unix version 2.x
CSACS-3.3-WINMR-K9	Minor update kit for customers on ACS 3.x that do not have SAS support contracts; Includes minor update release for ACS 3.3

1. This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco Secure ACS for Windows Web site: **http://www.cisco.com/go/acs**

Cisco Secure Access Control Solution Engine

The Cisco Secure ACS Solution Engine is a highly secure, OS-independent, and dedicated platform that offers a highly manageable access control solution with an increasingly reduced setup and troubleshooting time. It provides plug-and-play deployment, a highly reliable authentication, authorization, and accounting (AAA) solution, and increased total cost of ownership (TCO) protection. A Cisco Secure ACS remote agent is available with each Cisco Secure ACS Solution Engine to enable remote logging and Windows authentication.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Secure Access Control Solution Engine	• Need a dedicated, security-hardened, application-specific appliance package • Simplified day-to-day management with overall reliability and security of the Cisco Secure ACS service • Suitable alternative for Cisco Secure ACS UNIX customers not willing to install or manage Cisco Secure ACS on the Windows OS

Key Features

- Dedicated to run only the Cisco Secure ACS service preventing any appliance-based OS changes, additions, or configuration modifications
- A serial console interface is provided for initial configuration, subsequent management of IP connections, access to the Cisco Secure ACS HTML interface, and applying upgrade and recovery procedures
- Solution Engine-specific management tools provide generic appliance management capabilities including backup, recovery, software upgrades, monitoring, maintenance, and troubleshooting functions
- Provides authentication against Windows domains and remote logging capabilities of user accounting records
- A packet-filtering service to block traffic on all but the necessary Cisco Secure ACS-specific TCP and User Datagram Protocol ports
- Preinstalled, standalone Cisco Security Agent helps protects Cisco Secure ACS Solution Engine from day-zero attacks
- Built-in NTP functions to maintain network timing synchronization and consistency with other Cisco Secure ACS appliances or network devices

Specifications

Feature	Cisco Secure Access Control Solution Engine[1]
Processor speed	Pentium IV, 3.2 GHz
Memory	1 GB RAM
Hard Drive	80 GB free disk space
Interfaces	2 built-in 10/100 Ethernet controllers and 1 floppy disk drive

1. Specific to Cisco ACS Solution Engine. Additional features are found under Cisco Secure Access Control Server (ACS) for Windows, page 5-10

Selected Part Numbers and Ordering Information[1]

Cisco Secure ACS Solution Engine

CSACSE-1112-K9	Cisco Secure ACS 3.3 Solution; includes HW and SW
CSACSE-1112-UP-K9	Upg. for ACS 3.X open server or 1111 to Cisco 1112 w/ACS 3.3
CSACSE-3.3-SWMR-K9	Minor Release update for CSACS Sol. Eng. SW 3.3-Jul04

1. This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco Secure ACS Solution Engine Web site:
http://www.cisco.com/en/US/products/sw/secursw/ps5338/index.html

Cisco Secure User Registration Tool

Cisco Secure URT is a virtual LAN (VLAN) assignment service that provides LAN security by actively identifying and authenticating users and then associating them only to the specific network services and resources they need through dynamic VLAN assignments to Cisco Catalyst® Switch networks. URT v2.5 introduces many innovative features, including a Web-based logon from Windows, Macintosh, and Linux clients, RADIUS and Lightweight Directory Access Protocol (LDAP) authentication, and a secure link between the client and the VLAN Policy Server (VPS). It also includes a security feature based on the Media Access Control (MAC) address that prevents users from accessing the network if they are not using authorized machines. Web based LAN authentication allows for user mobility within the LAN environment.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Secure User Registration Tool (URT)	• Web-based LAN authentication for Windows, Macintosh, and Linux client platforms—ideal for mobile users within the LAN environment • Extended security to protect user access to the logon VLAN from unregistered PCs through MAC-based security option • RADIUS authentication and accounting support • Multiple user access per port

Key Features

- Web Client Logon Interface—Supports customizable Web-based authentication for Windows, Macintosh, and Linux client platforms
- MAC-Based Security Option—Provides extended security to protect user access to the logon VLAN from unregistered PCs
- RADIUS Authentication and Accounting Support—RADIUS authentication is offered for Web logon
- Secure Link Between Cisco Secure URT Client and VPS Server—Security authentication and data encryption have been added to URT v2.5 to enable a more secure connection from the user
- LDAP Support (Active Directory and NDS directories)—Cisco Secure URT v2.5 supports Windows' Active Directory and Novell's NDS LDAP servers
- Multiple Users Per Port—Previous versions of Cisco Secure URT support only a single user logon on a single port
- Display of Windows NT Groups—The URT Administrator interface is enhanced to display the users belonging to a Windows NT group
- MAC Address Events History—With URT v2.5 MAC-address-based logon/logoff events are added as an option and reported to the history events tool

Specifications

Feature	Cisco Secure User Registration Tool (URT)
Hardware	Windows 2000 (SP2) server, professional, and Windows XP Professional-Min H/W (Pentium III, 512MB DRAM, 65 MB of disk space)
Browser for Web Login	Netscape version 4.79 and 6.2; IE version 5.5 (SP2) or 6.0
Client Software Requirements	Windows 98 (2ndE), Windows NT4 Workstation/Server (SP6A), Windows 2000 (SP2) Professional/server, Windows XP Professional, Windows XP Home (Web Client Only), Mac OS 10.1 (Web client only), Linux Redhat/ SuSE/ Mandrake/ VA (Web Client only)-Min H/W for Web client (Pentium II, 256MB DRAM, 65 MB of disk space), Min H/W for traditional client (Pentium II, 64MB DRAM, 1MB of disk space)
Supported Cisco Products (latest tested version)	1900 series (1912, 1924), v9.00.05; C2800 series (2822, 2828), v9.00.05; C2900XL series (2908XL, 2916XL, 2912XL, 2912LRE-XL, 2924XL, 2924LRE-XL), v12.0(5)WC3b; C2948GL3 series (2948GL3, 4232) v12.0(18)W5(22b); C2950 series, v12.1.6.EA2c; C3500XL series (3508XL, 3512XL, 3524XL, 3548XL, 3550XL), v12.0(5)WC3b; C3550 series, v12.1.8.EA1c; C4000 series (4003, 4006, 4912g), v7.1(2); C5000 series (2900, 2926, 2948, 5000, 5002, 5500, 5505, 5509), v6.3(5); C6000 series (6006, 6009, 6506, 6509, 6513), v7.1(3)

Selected Part Numbers and Ordering Information[1]

Cisco Secure User Registration Tool (URT)

CSURT-1102-K9	Starter Kit: includes one (1) User Registration Tool 2.5 Software license, and one (1) Cisco 1102 VLAN Policy Server (VPS) appliance
URT-1102-HW-K9	Hardware Only; Cisco 1102 VPs appliance; additional appliance needed for backup, use in distributed deployments, or deployments requiring Web logon capabilities
CSURT-2.5-SWMR-K9	Minor update kit for customers on URT 2.x that do not have SAS support contracts; Includes minor update release for URT 2.5.

1. This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco Secure User Registration Tool Web site: **http://www.cisco.com/go/urt**

Cisco IOS Firewall

The Cisco IOS Firewall enriches Cisco IOS Software security capabilities, integrating robust firewall functionality and intrusion detection for every network perimeter. When combined with Cisco IOS IPSec software and other Cisco IOS Software-based technologies such as L2TP tunneling and quality of service (QoS), it provides a complete, integrated virtual private network solution. Because it is available for a wide range of Cisco routers, it gives customers the flexibility to choose a solution that meets their bandwidth, LAN/WAN density, and multiservice requirements, while benefiting from advanced security.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco IOS Firewall	• An integrated stateful firewall solution with powerful security and multiprotocol routing all on the same platform • Scalability options from the Cisco 800 up to the Cisco 7500 and the Catalyst 6000 • Low cost solution that leverages existing infrastructure • For secure extranet and intranet perimeters and Internet connectivity for branch and remote offices • Secure remote access or data transfer via a Cisco IOS Software-based VPN solution • Real-time (inline) integrated Cisco IOS Intrusion Prevention System (IPS) to complement firewall or existing IDS (Cisco Secure IDS) solutions • Security and access to the network on a per-user basis

Key Features

- Context-based access control (CBAC) provides secure, stateful, application-based packet inspection, supporting the latest protocols and advanced applications
- Cisco IOS Inline Intrusion Prevention for real-time monitoring, interception, and response to network misuse for over 740 attack signatures
- Supports URL Filtering either local on the router through exclusive domains as well as use of external Websense and N2H2 servers.
- Dynamic, per-user authentication/authorization for LAN, WAN, and VPN clients
- Authentication proxy for https, ftp and telnet connections
- Supports Cisco Router and Security Device Manager (SDM)
- Graphical configuration and management via the VPN/Security Management Solution (VMS) and the IP Solution Center (ISC)
- Provides strong perimeter security for a complete Cisco IOS Software-based VPN solution, including IPSec, QoS, and tunnelling

Competitive Products

- Nortel: BaySecure Firewall-1
- Checkpoint, Nokia, Netscreen, etc

Specifications

Feature	Cisco IOS Firewall
Supported Network Interfaces	All network interfaces on supported platforms
Supported Platforms	Cisco 1720, 1800, 2600/2600XM, 2800, 3700, 3800, 7100, 7200, and 7301 series router platforms (supports full feature set) Cisco 800, UBR900, 1600, and 2500 series router platforms include all firewall features with exception of intrusion detection/prevention and authentication proxy
Simultaneous Sessions	No maximum; dependent on platform, network connection, and traffic
Cisco IOS Firewall Performance	C800 - 10Mbps, C1700: 20Mbps; Cisco 1800: 125 Mbps,C2600XM: 35Mbps; C2691-VPN: 197Mbps; Cisco 2800: 530Mbps; C3725-VPN, C3745-VPN: 197 Mbps; Cisco 3825: 855Mbps; Cisco 3845:1 Gbps, 7200/7301 Bundles: 1Gbps

Part Numbers and Ordering Information

For Cisco IOS Images containing firewall (FW) and intrusion prevention (IPS) capabilities, see individual product pages of supported platforms and the Cisco IOS Feature Navigator at http://www.cisco.com/go/fn (CCO login required) for part numbers and more info.

For More Information

See the Cisco IOS Firewall Feature Set Web site: **http://www.cisco.com/go/firewall**