CHAPTER 5

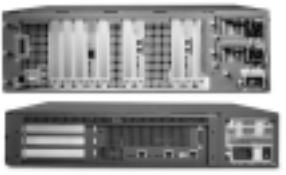
VPN and Security Products

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 application awareness • High-performance and scalable remote access and site-to-site VPN • Intrusion protection with 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 2-22, for more information	2-22
Cisco VPN 3000 Family	Remote access Virtual Private Network platform • 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 IDS Network Sensor	Network-based, real-time intrusion detection system capable of monitoring an entire enterprise network: • Capable of directing and forwarding alarms between local, regional, and headquarters-based monitoring consoles • Scalable architecture to allow the deployment of large numbers of sensors in order to provide comprehensive security coverage in large networks • Tight integration into the network through the delivery of the IDS Network Module for the Cisco Access Routers and the IDSM2 for the Catalyst 6500 switches • CTR (Cisco Threat Response) delivers adaptive scan techniques to minimize false alarms • Broad range of management options	5-8
Cisco Security Agent	The Cisco Security Agent provides threat protection for desktop and server computing systems by identifying and preventing malicious activity. By acting on threats or attacks before they can occur, Cisco Security Agent removes known and unknown security risks to enterprise networks and applications: • The Cisco Security Agent 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 • Protects against know and unknown attacks on both servers and desktops	5-10
Cisco Secure Access Control Server (ACS) for Windows and Cisco Secure Access Control Solution Engine	A centralized identity networking solution that simplifies user-management experience across all Cisco devices and security-management applications. An essential component of the Cisco Identity Based Networking Services (IBNS) architecture, it extends access security by combining authentication, user and administrator access, and policy control from a centralized identity networking framework. This allows greater flexibility and mobility, increased security, and user productivity gains. It helps ensure enforcement of assigned policies by allowing network administrators to control: Who can log in to the network, Privileges each user has in the network, and Security audit or account billing information that is recorded	5-12

Product	Features	Page
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	5-14
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	9-16
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	9-18
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	5-15
Cisco VPN Security Router Bundles	Cisco 1700, 2600, 3600, 3700, and 7200 VPN Security Router Bundles with Enhanced Integrated Network Security. See individual product pages for more detail (page 1-1)	1-1
Cisco 1700, 2600, 3600, and 7200	Wide variety of modular router platforms with options for IOS-based and hardware-enabled VPN and security support. See individual product pages and Cisco IOS Firewall Feature Set (page 5-15).	1-1
Cisco 7100 Series	Large branch and central site VPN router • Comprehensive suite of VPN services, including encryption, tunneling, firewall, and bandwidth management • Embedded I/O for ease of deployment • Service module slot for IPSec and PPTP encryption coprocessing • Dedicated Site-to-Site VPN router	5-16

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
PIX 515E	• Small-to-Medium Business (SMB) integrated security appliance • Up to 188 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	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 Concentrator Series—A family of purpose-built, remote access Virtual Private Network (VPN) platforms that incorporates high availability, high performance and scalability with the most advanced encryption and authentication techniques available today. Customers can greatly reduce costs by leveraging their ISPs' infrastructure and eliminate costly leased lines. This series supports small offices as well as large organizations with up to 10,000 simultaneous remote users per unit. With load balancing configured, multiple units can be clustered to enable unlimited remote access users. It also supports the widest range of VPN clients including Certicom MovianVPN client, Microsoft 2000 L2TP/IPsec Client, and Microsoft PPTP for Windows 95/98/ME/NT/2000/XP.

The Cisco VPN 3002 Hardware Client—Combines the best capabilities of a software client with the reliability and stability of a dedicated hardware platform, and scales to tens of thousands of users. It sets up connections to a variety of Cisco VPN concentrators, including the VPN 3000 series and PIX firewalls.

When to Sell

Sell This Product	When a Customer Needs These Features
VPN 3005 and 3015 Concentrators	• A fixed configuration device 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 remote access sessions • Encryption processing is performed in software • VPN 3015 is field-upgradable to the Cisco VPN 3030 and 3060 models and for redundancy
VPN 3030 and 3060 Concentrators	• VPN 3030 is for medium- to large-sized organizations with bandwidth requirements from full T1/E1 through T3/E3 (50 Mbps max. performance) and up to 1500 simultaneous sessions; field-upgradeable to the Cisco VPN 3060 • VPN 3060 is for large organizations, with high-performance, high-bandwidth requirements from fractional T3 through full T3/E3 or greater (100 Mbps max. performance) and up to 5000 simultaneous remote access sessions • Both have specialized SEP modules to perform hardware-based acceleration
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 remote access sessions • Specialized SEP modules perform hardware-based acceleration
VPN 3000 Client	• Establishes secure, end-to-end encrypted tunnels to the Cisco VPN 3000 Concentrator and other Cisco Easy VPN compliant devices. • Provided at no charge, installs on PCs and is available for Windows, MAC OS X and Linux/Solaris environments
VPN 3002 Hardware Client	• Emulates the software client in hardware • Ideal for mixed operating system environments and where corporation does not own/control remote PC 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
- Netscreen: LAN to LAN environments
- Nokia

Specifications

Cisco VPN 3000 Series Concentrators

Feature	VPN 3005	VPN 3015	VPN 3030	VPN 3060	VPN 3080
Simultaneous Users	100	100	1500	5000	10,000
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	100 Mbps	100 Mbps
Encryption Method	Software	Software	Hardware	Hardware	Hardware
Encryption (SEP) Module	0	0	1	2	4
Redundant SEP	No	No	Optional	Optional	Yes
Expansion Slots	0	4	3	2	N/A
Upgradeable	No	Yes	Yes	N/A	N/A
Memory	32 MB	128 MB	128 MB	256 MB	256 MB
Hardware Configuration	1U, Fixed	2U, Scalable	2U, Scalable	2U, Scalable	2U
Power Supply	Single	Single, with a dual option	Single, with a dual option	Single, with a dual option	Dual
Client License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
LAN-to-LAN Connections (internal user database)	100	100	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.

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)

Feature	VPN 3002 Hardware Client
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	CVPN3005-E/FE hw set, sw, client, & US power cord
CVPN3015-NR-BUN	CVPN3015-NR non-redundant hw set, sw, client, & US power cord
CVPN3030-NR-BUN	CVPN3030-NR non-redundant hw set, sw, client, & US power cord
CVPN3030-RED-BUN	CVPN3030-RED redundant hw set, sw, client, & US power cord
CVPN3060-NR-BUN	CVPN3060-NR non-redundant hw set, sw, client, & US power cord
CVPN3060-RED-BUN	CVPN3060-RED redundant hw set, sw, client, & US power cord
CVPN3080-RED-BUN	CVPN3080-RED redundant hw set, sw, client, & US power cord

Cisco VPN 3000 Series Upgrades

CVPN1530-UPG-RED	Cisco VPN 3015 To 3030 (Redundant) Upgrade Kit
CVPN1560-UPG-NR	Cisco VPN 3015 To 3060 (Non-Redundant) Upgrade Kit
CVPN1560-UPG-RED	Cisco VPN 3015 To 3060 (Redundant) Upgrade Kit
CVPN1580-UPG-RED	Cisco VPN 3015 To 3080 (Redundant) Upgrade Kit
CVPN3030-UPG-RED	Cisco VPN 3030 To 3080 (Redundant) Upgrade Kit
CVPN3060-UPG-NR	Cisco VPN 3030 To 3060 (Non-Redundant) Upgrade Kit
CVPN3080-UPG-R/R	Cisco VPN 3030 (Redundant) to 3080 (Redundant) Upgrade Kit
CVPN3080-UPG-RED	Cisco VPN 3030 To 3080 (Redundant) Upgrade Kit
CVPN3060-UPG-RED	Cisco VPN 3030 To 3060 (Redundant) Upgrade Kit
CVPN6060-UPG-RED	Cisco VPN 3060 To 3060 (Redundant) Upgrade Kit
CVPN6080-UPG-RED	Cisco VPN 3060 To 3080 (Redundant) Upgrade Kit
CVPN3060-UPG-R/R	Cisco VPN 3030 (Redundant) to 3060 (Redundant) Upgrade Kit
CVPN6080-UPG-R/R	Cisco VPN 3060 (Redundant) to 3080 (Redundant) Upgrade Kit

Cisco VPN 3000 Series Accessories

CVPN3000-PWR=	Cisco VPN 3000 Concentrator Power Supply

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 VPN Security Router Bundles with Enhanced Integrated Network Security

The Cisco VPN Security Router Bundles are based on the Cisco 1700, 2600XM, 2691, 3600, 3700, and 7200 modular multiservice router platforms. A benefit to purchasing the bundles is a single part number when ordering a Cisco router with all the necessary VPN and Security components at a reduced price compared to ordering each component separately. Each VPN bundle can have optional modules added as needed. All bundles include the selected router platform, a VPN hardware card, additional memory, and the Cisco IOS® to run IPSec 3DES or AES encryption and IOS Firewall with IDS (Intrusion Detection System). In addition the 2600XM and 3700 Series now have Advanced Security Network Modules available for ULR Filtering and hardware-based IDS. Cisco 1700, 2600XM, 2691, 3600, and 3700 Series based Security bundles come pre-installed with Security Device Manager (SDM) for fast and easy deployment based on Cisco TAC and ICSA Labs recommended router security configurations.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco VPN Security Router Bundles	• Deploying VPN or 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 • Reduction of network equipment to manage • Needs to integrate Voice and VPN Services (V3PN)

Specifications

Feature	Cisco VPN Security Router Bundles
All Bundles Include	Firewall with IDS; GRE and IPSec; High Availability/Failover; VPN QoS; AES in Hardware (excluding C1700 Bundles)
IPPCP Compression	Software: C1700 Bundles Hardware: C2600XM, C2691-VPN, C3725-VPN, C3745-VPN, 7200 Bundles
Max Tunnel	C1700: 100; C2600XM, C2691-VPN: 800; C3725-VPN, C3745-VPN: 2000; 7200 Bundles: 5000

For More Information

See individual product pages for more detail (page 1-1).

Cisco Intrusion Detection System (IDS) Network Sensors

Cisco integrated network security solutions enable organizations to protect productivity gains and reduce operating costs. The Cisco Intrusion Protection is designed to efficiently protect your data and information infrastructure. Cisco delivers four critical elements for efficient intrusion protection system which are:

- Accurate threat detection—Cisco Intrusion Detection System Version 4.0 (Cisco IDS 4.0) delivers the first step in providing a secure environment by comprehensively detecting all potential threats
- Intelligent threat investigation—Cisco Threat Response technology virtually eliminates false alarms, and automatically determines which threats need immediate attention to avoid costly intrusions.
- Ease of management—Browser-based tools simplify the user interaction, while providing powerful analytical tools that allow for a rapid and efficient response to threats.

- Flexible deployment options—A range of high-availability devices provide the flexible backbone for creating the secure and efficient intrusion protection system.

The current Cisco IDS sensing portfolio includes the following sensor appliances: IDS 4215, IDS 4235, IDS 4250, and IDS 4250-XL. Additionally, Cisco IDS delivers solutions that are integrated into the Catalyst 6500 switch with the Intrusion Detection System Module (IDSM-2) and into the Cisco Access Routers with the IDS Network Module (NM-CIDS).

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco IDS Network Sensors	• A distributed intrusion detection system capable of directing and forwarding alarms between local, regional, and headquarters-based monitoring consoles • A scalable architecture to allow the deployment of large numbers of sensors in order to provide comprehensive security coverage in large network environments • Cisco network IDS appliances (Cisco IDS 4200 Series Appliances) that can be deployed throughout the network with the ability to monitor multiple subnets using a single appliance through the support of multiple interfaces • The Cisco IDS Switch Module (IDSM2) enables customers to perform both security monitoring and switching functions within the same chassis • The Cisco IDS Network Module enables full features intrusion protection integrated into the Cisco Access Routers • Broad performance range from 10 Mbps to 1 Gbps • Automated false alarm reduction capabilities through CTR (Cisco Threat Response) • Flexible IDS signature customization options • Broad range of management and monitoring options to fit any environment. • A robust, 24 hour x 7 day-a-week monitoring and response system with the latest attack detection capabilities

Key Features

- High-Speed Performance including support for full line rate gigabit environments
- Integrated solutions for the Cisco Catalyst Switch and Cisco Access Routers
- Easy Installation and Setup; Remote Configuration Capability
- Comprehensive Attack Database
- Notification actions; Automated response actions
- Comprehensive IDS Anti-Evasion Techniques
- Cisco IOS-like CLI for full featured IDS management capabilities

Competitive Products

- Internet Security Systems (ISS): RealSecure
- Symantec: Recourse Manhunt & ManTrap/NetProwler
- Enterasys: Dragon IDS
- Intrusion.com: SecureNet
- Netscreen: OneSecure IDP
- Snort: IDS
- Tipping Point
- NAI: Intrushield
- Network Flight Recorder, Inc.: NFR

Specifications

Feature	IDS-4215	IDS-4235	IDS-4250	IDS-4250-XL	IDS Module (IDSM-2)	IDS Network Module (NM-CIDS)
Performance	80 Mbps	250 Mbps	500 Mbps	1000 Mbps	600 Mbps	45Mbps
Processor	850 MHz	1.26 GHz	Dual 1.26 GHz	Dual 1.26 GHz. Includes customized HW acceleration	Custom Hardware	10-45 Mbps
RAM	512 MB	1 GB	2 GB	2 GB	2 GB	512 MB

Monitoring Interface	Autosensing 10/100 Base-T Ethernet, (upgradable to support up to 5 monitoring interfaces)	Autosensing 10/100/1000 Base-T Ethernet (upgradable to support up to 5 monitoring interfaces)	Autosensing 10/100/1000BASE-TX (upgradable to support up to 5 monitoring interfaces) Optional 1000-Base SX (fiber) supported with the SX model	Dual 1000BASE-SX interface with MTRJ	PCI	Internal 10-/100-Mbps Ethernet and external 10-100-Mbps Ethernet
Command & Control Interface	Autosensing 10/100 Base-T Ethernet	Autosensing 10/100/1000Base-TX	Autosensing 10/100/1000Base-TX	Autosensing 10/100/1000Base-TX	PCI	10/1010/100Base T

Selected Part Numbers and Ordering Information[1]

Cisco IDS Network Appliance Sensor

IDS-4215-K9	4215 Cisco IDS 4215 Sensor (chassis, software, SSH, 2 onboard 10/100 Base-T interfaces with RJ-45 connector) 80-Mbps
IDS-4215-4FE-K9	Cisco IDS 4215 Sensor (chassis, software, SSH, 2 onboard 10/100BASE-Tx interfaces with RJ-45 connector plus 4FE interface card), 80-Mbps
IDS-4235-K9	Cisco IDS 4235 Sensor (chassis, software, SSH, 10/100/1000BASE-T with RJ-45 connector, up to 200 Mbps)
IDS-4250-TX-K9	Cisco IDS 4250 Sensor (chassis, software, SSH, 10/100/1000BASE-T with RJ-45 connector)
IDS-4250-SX-K9	Cisco IDS 4250 Sensor (chassis, software, SSH, 1000BASE-SX with SC connector)
IDS-4250-XL-K9	Cisco IDS 4250-XL Sensor (chassis, software, SSH, hardware accelerator with dual 1000BASE-SX and MTRJ connectors)

Cisco IDS Network Module for Cisco Access Routers

IDS NM-CIDS	Cisco IDS Network Module, 20-GB IDE hard disk

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).

Note **Export Considerations:** The Cisco IDS 4215, Cisco IDS 4235, Cisco IDS 4250, Cisco IDS 4250-XL, Cisco IDSM-2 & Cisco IDS Network Module are 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 IDS web site: **http://www.cisco.com/go/ids**

See the Cisco IDS Management solutions web site: **http://www.cisco.com/go/vms**

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 before it can occur, thereby removing potential known and unknown ("Day Zero") security risks that threaten enterprise networks and applications. The Cisco Security Agent 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. Customers require robust endpoint security that prevents security attacks from affecting the network and critical applications.

As a key component of the SAFE blueprint for secure e-business, the Cisco Security Agent provides unprecedented endpoint protection that enables businesses to participate in e-commerce securely and take advantage of the Internet economy.

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

Key Features

- Provides industry-leading protection for Unix and Windows servers
- Open, extensible architecture offers the capability to define and enforce security according to corporate policy

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-B1000-DTOP-K9	Cisco Security Desktop Agent (Win + Sol), 1000 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/securityagent**

Cisco Secure Access Control Server (ACS) for Windows and Cisco Secure Access Control Solution Engine

Cisco Secure Access Control Server (ACS) version 3.2 for Windows, a key component of Cisco's Identity Based Networking Services (IBNS) architecture, extends access security by combining authentication, user/admin access and policy control from a centralized identity networking framework allowing for greater flexibility and mobility, increased security, and user productivity gains. Cisco Secure ACS also provides identity networking support for Cisco Structured Wireless Aware Networks (SWAN), as an extension of the local authentication provided on Cisco Aironet Access Points. ACS allows a network administrator to manage and administer user access for Cisco IOS® routers, virtual private networks (VPNs), firewalls, dial and broadband DSL, cable access solutions, storage, content, voice over IP (VoIP), Cisco wireless solutions, and Cisco Catalyst® switches via IEEE 802.1x access control.

Version 3.2 introduces a new, secure, hardware-based offering for Cisco Secure ACS. The Cisco Secure ACS Solution Engine, a 1-rack-unit (1-RU) security-hardened solution engine with a preinstalled Cisco Secure ACS license, provides essentially the same features and functions as the Cisco Secure ACS for Windows, in a dedicated, application-specific solution engine package. Cisco Secure ACS Solution Engine provides a z define access control lists of any length, per user or group of users. It extends per-user access control ero-touch installation and highly reliable AAA solution with increased total-cost-of-ownership protection through high availability and simplified day-to-day operation the Cisco Secure ACS service.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Secure Access Control Server (ACS) for Windows and Cisco Secure Access Control Solution Engine	• 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

- Protected Extensible Authentication Protocol (PEAP) support for Microsoft® Windows and Cisco clients—Provides support for Microsoft® PEAP on Windows 98, NT, 2000 and XP by supporting client authentication with MS-CHAPv2, and support for Cisco PEAP with one-time token authentication and support of non-MSCHAP end-user databases such as, NDS, and ODBC.
- EAP mixed configurations—Allows flexible EAP settings to be set concurrently and processed per the 802.1X protocol presented by the end user. ACS supports PEAP-EAP-GTC (Cisco PEAP), PEAP-EAP-MSCHAPv2 (Microsoft® PEAP), EAP-TLS, EAP-MD5, and Cisco EAP Wireless (LEAP).
- Accounting Support for Aironet—Supports user-based accounting from the Wireless Access Points when they are configured as RADIUS (Cisco Aironet) AAA clients.
- EAP-TLS enhancements—Extends ACS PKI capabilities with the addition of EAP-TLS authentication against ODBC user databases, and EAP-TLS silent session resume support which prevents users from re-authenticating during a RADIUS session timeout.

- Machine authentication support—Supports machine authentication by maintaining communication to a back end Windows Active Directory during boot time. ACS supports machine authentication using PEAP with MSCHAPv2 or EAP-TLS 802.1X authentication types.
- LDAP Multithreading—Increases performance by processing multiple LDAP authentication requests in parallel rather than in sequential order.
- Downloadable access control lists for VPN users—Allows administrators to define access control lists of any length, per user or group of users. It extends per-user access control list support to Cisco VPN solutions and PIX Firewall solutions.
- Integration with Cisco's security management software application—Provides a consolidated administrative TACACS+ control framework for many Cisco security management tools such as CiscoWorks VPN/Security Management Solution (VMS)

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[1]	• 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

1. Cisco Secure Access Control Server Solution Engine system specifications are available in the Product Literature

Selected Part Numbers and Ordering Information[1]

Cisco Secure Access Control Server (ACS) for Windows	
CSACS-3.1-WIN-K9	Cisco Secure ACS 3.1 for Windows
CSACS-3.1-WINUP-K9	Upgrade to CSACS 3.1 for Windows from ACS versions 1.x, 2.x, 3.0 and Cisco Secure ACS for Unix version 2.x
CSACSE-1111-K9	Cisco Secure ACS Solution Engine version 3.2; includes Cisco 1111 hardware platform and Cisco Secure Access Control Server software, version 3.2
CSACSE-1111-UP-K9	Upgrade for customers using Cisco Secure ACS 3.X for Windows or Cisco Secure ACS for Unix customers to the Cisco Secure ACS Solution Engine version 3.2; includes Cisco 1111 hardware platform and Cisco Secure Access Control Server software, version 3.2
CSACS-3.2-WIN-K9	Cisco Secure ACS 3.2 for Windows
CSACS-3.2-WINUP-K9	Upgrade to CSACS 3.1 for Windows from ACS versions 1.x, 2.x, 3.x and Cisco Secure ACS for Unix version 2.x

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**

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)

URT-2.5-K9	Starter Kit: includes one (1) User Registration Tool 2.5 Software license, and one (1) Cisco 1101 VLAN Policy Server (VPS) appliance
URT-2.5-UP	Software only; upgrades customers from URT 2.X to 2.5; includes upgrade for both URT Admin Server and Cisco 1100 VPS appliance
URT-1101-HW-K9	Hardware Only; Cisco 1101 VPS appliance; additional appliance needed for backup, use in distributed deployments, or deployments requiring Web logon capabilities

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 where high performance is not a requirement • 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 intrusion detection system (IDS) to complement firewall or existing IDS (Cisco Secure IDS) • 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
- Intrusion detection for real-time inline monitoring, interception, and response to network misuse for 100 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 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, 2600/2600XM, 3600, 7100, and 7200 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 and authentication proxy
Simultaneous Sessions	No maximum; dependent on platform, network connection, and traffic

Part Numbers and Ordering Information

For Cisco IOS Images containing firewall (FW) and intrusion detection (IDS) 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/csis**

Cisco 7100 Series

The Cisco 7100 series VPN router is a high-end, integrated VPN solution that melds high-speed, industry-leading routing with a comprehensive suite of advanced site-to-site VPN services. The Cisco 7100 series VPN router integrates key features of VPNs—tunneling, data encryption, security, firewall, advanced bandwidth management, and service-level validation—to deliver self-healing, self-defending, VPN platforms that cost-effectively accommodate remote-office and extranet connectivity using public data networks. The Cisco 7100 series VPN router offers specific hardware configurations optimized for VPN applications and network topologies. Optional WAN and embedded Fast Ethernet interfaces combined with high-performance routing and rich VPN services provide turnkey VPN routing solutions.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 7120	• Entry-level Cisco 7100 Series Router designed for large branch or central site VPN with VPN services throughput of up to 50 Mbps • Designed primarily for site-to-site VPN deployments with incidental remote access requirements
Cisco 7140	• High-end site-to-site VPN platform for central site VPN applications with VPN services throughput up to 140 Mbps • Provides superior routing and VPN services performance for central site environments, as well as dual power supplies for increased solution reliability

Key Features

- Comprehensive suite of VPN services—tunneling, data encryption, security, firewall, quality of service, and service level validation—integrated with industry leading routing
- High performance RISC processor delivering high-speed, scalable VPN services and routing throughput and extensive memory for reliable, high-speed VPN services delivery
- Dual autosensing 10/100BASE-T Fast Ethernet ports for connectivity to the corporate LAN; the Cisco 7120 Series also has an integrated 4-port T1/E1 serial WAN interface
- Integrated Services Module (ISM) is included for support up to 2000 simultaneous tunneling sessions with 90 Mbps encryption performance and Windows 95/98/NT4.0 and Windows 2000 compatibility for remote access; an optional

Integrated Services Adapter (ISA) may be installed in the Cisco 7140 to provide dual encryption acceleration performance up to 3000 tunnels and 140 Mbps 3DES encryption throughput

Competitive Products

- Check Point: VPN-1 Appliance
- Nortel: Contivity 4500
- Nokia: IP440

Specifications

Feature	Cisco 7120	Cisco 7140
Embedded Dual 10/100BASE-T Fast Ethernet Interfaces	Autosensing, RJ-45	Autosensing, RJ-45
WAN Physical Interfaces	EIA/TIA-232, EIA/TIA-449, X.21, V.35, EIA-530	None
WAN/LAN Interface Expansion Slot	1 slot	1 slot
Supported Network and Services Port Adapters	Gigabit Ethernet 1000BASE-SX and 1000BASE-LX/LH Fast Ethernet 100BASE-TX and 100BASE-FX Fast Ethernet/ISL TX and ISL FX Ethernet 10BASE-T and 10BASE-FL Dedicated Token Ring Multichannel T1 and E1 ATM Synchronous Serial HSSI ISDN BRI Packet over SONET OS3/STM1 Integrated Services Adapter (ISA)	Same as Cisco 7120
Service Module Slot	1 slot	1 slot
Included Service Modules	Integrated Services Module (ISM)	Integrated Services Module (ISM)
Console and Auxiliary Ports	1 of each, RJ-45 interface	1 of each, RJ-45 interface
SDRAM	64 MB packet 128 MB system (expandable to 256 MB)	64 MB packet 128 MB system (expandable to 256 MB)
Flash Memory	48 MB	48 MB
PCMCIA Slots for Flash Memory	2	2
Power Supply	Single AC	Dual AC
Dimensions (HxWxD)	3.5 in. x 17.5 in. x 18.25 in.	3.5 in. x 17.5 in. x 18.25 in.

Cisco IOS Software and Memory Requirements[1]

To run the Cisco IOS Software Feature Packs, you need, at a minimum, the amount of memory shown in the following table. Some configurations will require more than the recommended minimum.

Distribution Part Number	Feature Pack Description	IOS Image Release	Flash Memory Required	DRAM Memory Required
CD71-CL-12.1.6E=	IP IPSEC 56	12.1(6)E	16MB	64MB
CD71-CK2-12.1.6E=	IP IPSEC 3DES	12.1(6)E	16MB	64MB
CD71-CHK2-12.1.6E=	IP/FW/IDS IPSEC 3DES	12.1(6)E	16MB	64MB
CD71-AL-12.1.6E=	Enterprise IPSEC 56	12.1(6)E	16MB	64MB
CD71-AK2-12.1.6E=	Enterprise IPSEC 3DES	12.1(6)E	16MB	64MB
CD71-AHK2-12.1.6E=	Enterprise/FW/IDS IPSEC 3DES	12.1(6)E	16MB	64MB

1. For the complete list of IOS Feature Sets, refer to the parts list, via the URL listed under "For More Information". For users with CCO access, search by IOS feature or release via the *Feature Navigator* at http://www.cisco.com/go/fn

Selected Part Numbers and Ordering Information[1]

Cisco 7100 Series Bundles—7120	
CISCO7120-4T1/VPN	7120-4T1 VPN Bundle, ISM, 2xFE, AC PS, IPSEC DES
C7120-4T1/VPN/K9	7120-4T1 VPN Bundle, ISM, 2xFE, AC PS, IPSEC 3DES
Cisco 7100 Series Bundles—7140	
CISCO7140-2FE/VPN	7140-2FE VPN Bundle, ISM, 2xFE, 2xAC PS, IPSEC DES
C7140-2FE/2VPN/K8	7140-2FE VPN Bundle, ISM & ISA, 2xFE, 2xAC PS, IPSEC DES
C7140-2FE/2VPN/K9	7140-2FE VPN Bundle, ISM & ISA, 2xFE, 2xAC PS, IPSEC 3DES
C7140-2FE/VPN/K9	7140-2FE VPN Bundle, ISM, 2xFE, 2xAC PS, IPSEC 3DES
Cisco 7100 Port Adapters	
PA-FE-TX	1-port Fast Ethernet 100BaseTx Port Adapter
PA-FE-FX	1-port Fast Ethernet 100BaseFx Port Adapter
PA-2FE-TX	2-port Fast Ethernet 100BaseTx Port Adapter
PA-2FE-FX	2-port Fast Ethernet 100BaseFx Port Adapter
PA-2FEISL-TX	2-port Token Ring ISL 100BaseTx Port Adapter
PA-2FEISL-FX	2-port Token Ring ISL 100BaseFx Port Adapter
PA-4E	4-port Ethernet 10BaseT Port Adapter
PA-8E	8-port Ethernet 10BaseT Port Adapter
PA-5EFL	5-port Ethernet 10BaseFL Port Adapter
PA-4T+	4-port Serial Port Adapter, Enhanced
PA-8T-V35	8-port Serial, V.35 Port Adapter
PA-8T-232	8-port Serial, 232 Port Adapter
PA-8T-X21	8-port Serial, X.21 Port Adapter
PA-4R-DTR	4-port Dedicated Token Ring, 4/16Mbps, HDX/FDX Port Adapter
PA-GE	Gigabit Ethernet Port Adapter
PA-H	1-port HSSI Port Adapter
PA-2H	2-port HSSI Port Adapter
PA-A3-T3	1-port ATM Enhanced DS3 Port Adapter
PA-A3-E3	1-port ATM Enhanced E3 Port Adapter
PA-A3-OC3MM	1-port ATM Enhanced OC3c/STM1 Multimode Port Adapter
PA-A3-OC3SMI	1-port ATM Enhanced OC3c/STM1 Single mode (IR) Port Adapter
PA-A3-OC3SML	1-port ATM Enhanced OC3c/STM1 Single mode (LR) Port Adapter
PA-4E1G/75	4-port E1 G.703 Serial Port Adapter (75ohm/Unbalanced)
PA-4E1G/120	4-port E1 G.703 Serial Port Adapter (120ohm/Balanced)
PA-E3	1-port E3 Serial Port Adapter with E3 DSU
PA-2E3	2-port E3 Serial Port Adapter with E3 DSUs
PA-T3	1-port T3 Serial Port Adapter with T3 DSUs
PA-2T3	2-port T3 Serial Port Adapter with T3 DSUs
PA-MC-2T1	2-port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-2E1/120	2-port multichannel E1 port adapter with G.703 120ohm interf
PA-MC-4T1	4-port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-8T1	8-port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-8E1/120	8-port multichannel E1 port adapter with G.703 120ohm interf
PA-POS-OC3MM	1-port Packet/SONET OC3c/STM1 Multimode Port Adapter
PA-POS-OC3SMI	1-port Packet/SONET OC3c/STM1 Single mode (IR) Port Adapter
PA-POS-OC3SML	1-port Packet/SONET OC3c/STM1 Single mode (LR) Port Adapter
SM-ISM	Integrated Services Module for IPSec & MPPE encryption
SA-ISA	Integrated Services Adapter for IPSec or MPPE encryption
PA-4B-U	4-port BRI Port Adapter, U Interface
PA-8B-S/T	8-port BRI Port Adapter, S/T Interface

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 7100 series Web site: **http://www.cisco.com/go/7100**