Chapter 5: Security

This chapter provides only a subset of Cisco products and part numbers.

Security At-a-Glance

Product	Features	Page
NETWORK SECURITY		
Cisco IOS Security	· Delivers a sophisticated set of security capabilities for a comprehensive, layered security approach throughout the network infrastructure · Technologies help to defend critical business processes against attack and disruption, protect privacy, and support policy and regulatory compliance controls	5–3
Cisco ASA 5500 Series Adaptive Security Appliances	· Easy-to-deploy solutions that integrate world-class firewall, unified communications (voice and video) security SSL and IPSec VPN, intrusion prevention systems (IPSs), content security services, and secure unified communications in a flexible, modular product family	5–4
Cisco Intrusion Prevention Systems (IPS)	· Accurately identify, classify, and stop malicious traffic, including worms, spyware, adware, network viruses, and application abuse, before they affect business resiliency	5–9
Cisco Catalyst 6500 Series Firewall Services Module	· High-speed, integrated firewall module for Cisco Catalyst 6500 Switches and Cisco 7600 Series Routers · Provides the fastest firewall data rates in the industry: 5-Gbps throughput, 100,000 cells per second (CPS), and 1 million concurrent connections · Up to four FWSMs can be installed in a single chassis, providing scalability to 20 Gbps per chassis · Based on Cisco PIX Firewall technology, the Cisco Catalyst 6500 FWSM offers large enterprises and service providers unmatched security, reliability, and performance	5–12
SECURE ACCESS CONTROL		
Cisco TrustSec Solution ***NEW SOLUTION***	· Builds security and intelligence into the network with policy-based access control, identity-aware networking, and data confidentiality and integrity · Helps you secure borderless networks with confidence, consistency, and efficiency	5–13
Cisco NAC Appliance (Clean Access) ***NEW UPDATES***	· Cisco NAC Appliance (formerly Cisco Clean Access) is an easily deployed Network Admission Control (NAC) product that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources · Network administrators can authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to network access	5–14
Cisco Secure Access Control System ***NEW UPDATES***	· Controls network access based on dynamic conditions and attributes · Next-generation platform for centralized network identity and access control · Simple yet powerful, rule-based policy model and a new, intuitive management interface designed for optimum control and visibility	5–15
E-MAIL AND WEB SECURITY		
Cisco IronPort E-mail Security Solutions	· Provides a multi-layer approach to stopping e-mail-based threats	5–18
Cisco IronPort Secure Web Gateway Security Appliances	· S-Series web security appliance combines traditional URL filtering, reputation filtering, malware filtering, and data security on a single platform to address the growing challenges of both securing and controlling web traffic	5–19
Cisco IronPort M-Series Security Management Appliance	· M-Series security management appliance complements all of the Cisco IronPort e-mail and web security appliances · Provides one location for you to monitor all corporate policy settings and audit information	5–21
Cisco ACE Web Application Firewall	· Combines deep Web application analysis with high-performance Extensible Markup Language (XML) inspection and management to address the full range of these threats · Secures and protects Web applications from common attacks such as identity theft, data theft, application disruption, fraud, and targeted attacks	5–23
Cisco IOS Content Filtering	· Web security solution that helps organizations protect against known and new Internet threats, improve employee productivity, and enforce business policies for regulatory compliance	5–24
Cisco Spam and Virus Blocker ***NEW PRODUCT***	· Dedicated antispam, antivirus, and antiphishing security appliance designed specifically for small businesses which virtually eliminates e-mail threats right out of the box · Helps blocks spam, requires minimal administration, and connects to one of the largest databases of e-mail security threats to bolster its accuracy	5–25
Cisco ScanSafe Web Security ***NEW PRODUCT***	· Enhances security while enabling cost savings of up to 40% by eliminating the need to purchase, deploy and maintain hardware required for on-premise solutions	5–26

Cisco ScanSafe Web Filtering ***NEW PRODUCT***	· Offers granular control over all Web content, including SSL encrypted communications, using multiple techniques including real-time dynamic Web content classification, an industry-leading URL filtering database, file type filters and early warning filtering and real-time scanning of search results with SearchAhead	5–27
Cisco ScanSafe Anywhere+ ***NEW PRODUCT***	· Extends the real-time protection and policy enforcement of ScanSafe Web Security to roaming employees · Protects roaming employees wherever they are working and however they access the Internet.	5–27
SECURE MOBILITY		
Cisco AnyConnect Secure Mobility Solution ***NEW SOLUTION***	· Combines Cisco's web security and next-generation remote access technology to deliver a robust and secure enterprise mobility solution · Helps your organization easily manage the security risks of borderless networks	5–27
Cisco 3350 Mobility Services Engine	· Provides a new approach for the delivery of mobility services to enable mobile business applications · A combination of hardware and software, the Mobility Services Engine is an appliance-based solution that supports a suite of software services to provide centralized and scalable service delivery	5–29
Cisco Catalyst 6500 Series/ 7600 Series WebVPN Services Module	· High-speed, integrated Secure Sockets Layer (SSL) VPN services module for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers that addresses the scalability, performance, application support, and security required for large-scale, remote-access SSL VPN deployments	5–30
Cisco Security Agent	· Protects endpoints from all types of malware and confidential data loss with a lower total cost of ownership	5–31
Cisco Virtual Office Solutions	· Boost flexibility and productivity and extend the enterprise by delivering secure, rich, and manageable network services to teleworkers and employees working outside the traditional office environment	5–32
SECURITY MANAGEMENT		
Cisco Security Manager	· Enterprise-class management application that provides insight into and control of Cisco security and network devices	5–33
Cisco Security Monitoring, Analysis, and Response System (MARS)	· Centralized monitoring, event-correlation, and attack-mitigation system	5–33
PHYSICAL SECURITY		
Cisco Physical Access Gateway	· Primary means for the Cisco Physical Access Control solution to connect door hardware, such as locks and readers, to your IP network · One gateway can control up to two doors and can scale to thousands of doors at a fixed cost per door	5–35
Cisco Physical Access Manager	· Management application for the Cisco Physical Access Control solution · Easy-to-use interface lets you configure Cisco Physical Access gateways and modules, monitor activity, enroll users, and integrate with IT applications and data stores	5–36
Cisco Video Surveillance 2500 Series IP Cameras—Standard Definition	· Feature-rich, professional digital cameras designed for superior performance in a wide variety of environments · Enhanced, progressive scan imager for excellent video and color, even in the most demanding lighting conditions · MPEG-4 compression produces DVD-quality video · Automatic day/night mode, dual streams, bidirectional audio, motion detection, alarm inputs and outputs, and an analog BNC for ease of installation	5–37
Cisco Video Surveillance 4000 Series IP Cameras—High Definition ***NEW UPDATES***	· True high-definition (HD) video surveillance IP digital cameras designed for superior performance in a wide variety of video surveillance applications · Provide efficient network usage with the highest-quality video · Contact closures and two-way audio allow integration with microphones, speakers, and access control systems · Open, standards-based design provides an ideal platform for integration and operation as independent devices or as part of a Cisco Video Surveillance network	5–38
Cisco Video Surveillance 2000 Series IP Domes ***NEW UPDATES***	· High-resolution, feature-rich digital IP camera that delivers superior performance in a wide variety of environments · MPEG-4 compression of up to 30 frames per second (fps) at D1 NTSC resolution (720 x 480) or 25 fps at D1 PAL resolution (720 x 576) offers efficient network usage while providing high-quality video · Supports MJPEG compression	5–40
Cisco Video Surveillance Stream Manager Software	· Switching and recording software used in Cisco Video Surveillance IP Gateways, Convergence Chassis, Service Nodes, and Integrated Gateways · Provides virtual matrix switching to connect cameras, keyboards, and monitors, plus video storage and recall for display on analog monitors or PCs · Provides powerful features for the operation and management of a video surveillance solution	5–40
Cisco Video Surveillance Media Server Software	· Manages, replicates, distributes, and archives video streams · Core component of the Cisco network-centric video surveillance software portfolio offers the power and flexibility to meet a diverse range of video surveillance requirements	5–41

Cisco Video Surveillance Operations Manager Software	· In conjunction with the Cisco Video Surveillance Media Server, authenticates and manages access to video feeds · Centralized administration tool for management of media servers, cameras, encoders, and viewers · Meets the diverse needs of administrators, systems integrators, and operators	5–42
Cisco Physical Security Multiservices Platform ***NEW PRODUCT***	· Offers innovative choices for deploying and managing physical security services, including video surveillance, access control, and flexible incident response communications · Compact, 1-rack-unit (RU) appliance includes a wide array of features in a single, easy-to-use, and easy-to-deploy component	5–43
Cisco IPICS Server Software	· Security-enhanced, Linux-based platform installed on select Cisco 7800 Series Media Convergence Servers · Other Cisco IPICS system components include the Cisco IPICS Push-to-Talk Management Center (PMC), Cisco IPICS Phone Client, Cisco IPICS Operational Views (Ops Views), Cisco Land Mobile Radio (LMR) gateways, Router Media Service (RMS), and Session Initiation Protocol (SIP) telephony gateways	5–44
Cisco IPICS Dispatch Console ***NEW PRODUCT***	· End-to-end radio dispatching solution designed for mission-critical radio communications. It is the vital link between dispatchers and field personnel, helping to coordinate field response and ensure personnel safety · Designed and built to take advantage of the newest IP communications technologies, making it easier to dispatch responders and provide them with information that improves their situational awareness · Running on a standard PC platform, it extends existing push-to-talk (PTT) radio channels so that users with a variety of communication devices can participate	5–45
Cisco IPICS Mobile Client ***NEW PRODUCT***	· Smartphone application that allows responders to interact with other incident participants · In conjunction with the Cisco IPICS Dispatch Console, provides an on-demand solution for physical security and emergency first responders who are mobile, enabling them to begin reviewing incident information and addressing an incident even while on the way to the scene	5–46
SERVICES		
Cisco Security Services Enable the innovative, secure, network edge using intelligent, personalized services from Cisco and our partners. Through a discovery process that begins with understanding your business objectives, we help you integrate end-to-end solutions into your architecture and incorporate network services onto that platform. Sharing knowledge and leading practices, we support your success every step of the way as you deploy, absorb, manage, and scale new technology. Choose from a flexible suite of support services designed to meet your business needs and help you maintain high-quality network performance while controlling operational costs.		5–47
FOR MORE INFORMATION		
Product Ordering To place an order, visit: http://www.cisco.com/en/US/ordering/index.shtml. **End-of-Life and End-of-Sale** Please visit the end-of-life and end-of-sale website for a complete and up-to-date listing of products that are no longer being sold or supported, what replacement products are available, and information about product support. http://www.cisco.com/en/US/products/prod_end_of_life.html NOTE: This chapter provides only a subset of Cisco products and part numbers. For the most up-to-date and comprehensive information, refer to the Cisco website at http://www.cisco.com, the Cisco ordering website at http://www.cisco.com/en/US/ordering/index.shtml, or reference the URL listed in the "For More Information" section of each product.		

Cisco IOS Security

Cisco IOS Software routers ship with the industry's most comprehensive security services, intelligently embedding data, security, voice, and wireless in the platform portfolio for fast, scalable delivery of mission-critical business applications. The Cisco 800 Series Routers and Cisco 1800, 2800, and 3800 Series Integrated Services Routers are ideal for small businesses and enterprise branch offices, delivering a rich, integrated solution for connecting remote offices, mobile users, and partner extranets or service provider-managed customer premises equipment (CPE). The Cisco 7200 Series and 7301 Routers and the Cisco ASR 1000 Series Aggregation Services Routers are ideal for aggregation of WAN security services in campus and enterprise environments.

Cisco IOS Software routers include security services that address customer concerns regarding threat management, VPN and secure communications, integrated network solutions, and security management. With the convergence of features such as advanced firewall, VPN services, intrusion prevention system (IPS), Cisco Network Access Control (NAC), and content filtering, the Cisco IOS Security routers give customers flexibility to choose a solution that meets their bandwidth, LAN and WAN density, and multiservice requirements while benefiting from advanced security.

Ideal for Companies That Need These Features

Cisco IOS Software	• An integrated security solution that includes firewall, VPN, remote access, IPS, and content-filtering technologies • Low total cost of ownership by taking advantage of the existing infrastructure for modular and flexible deployment options • An integrated stateful inspection firewall with powerful security and multiprotocol routing all on the same routing platform • Scalability options from the Cisco 800 Series up to the Cisco 7200 Series, the Cisco 7301, and the Cisco ASR 1000 Series Aggregation Services Routers • Integrated, secure network solutions including secure unified communications and secure mobility • Secure extranet and intranet perimeters and Internet connectivity for secure branch and remote offices • Ability to meet compliance regulations such Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), or Sarbanes-Oxley Act of 2002 (SOX) that require firewall or data-encryption services

Key Features and Benefits

- Cisco IOS Security offers an advanced firewall that includes zone-based firewall, which provides secure, stateful, application-based packet inspection to support the latest protocols and advanced applications.
- Cisco IOS Firewall offers a threat--management foundation to deploy secure access policies at all network interfaces.
- Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection feature that effectively mitigates a wide range of network attacks. Supporting thousands of attack signatures, it provides the network intelligence to accurately identify, classify, and stop or block malicious traffic in real time.
- Cisco IOS Content Filtering helps your organization protect itself from known and new Internet threats, improve employee productivity, and enforce business policies for regulatory compliance.
- Cisco IOS IP Security (IPsec) and Secure Sockets Layer (SSL) VPN offer services for site-to-site VPN and unified remote-access security. These services include standards-based IPsec VPN, Cisco Group Encrypted Transport VPN, Dynamic Multipoint VPN (DMVPN), Easy VPN, and SSL VPN.
- Dynamic, per-user authentication and authorization for LAN, WAN, and VPN clients.
- Cisco Network Admission Control (NAC) support extends the ability of the network to enforce organizational security policies on devices seeking network access by delivering NAC services on an integrated services module.

Selected Part Numbers and Ordering Information

The Cisco IOS Security router bundles are based on the Cisco 800 Series Routers, Cisco 1800, 2800, and 3800 Series Integrated Services Routers, and Cisco 7200 Series and 7301 routers providing a full range of security features. These bundles include entry security bundles, enhanced security bundles for added performance and scale, and entry voice (Voice Security [VSEC]) and premier voice (H-VSEC) bundles for combined security and unified communications. These bundles are orderable through a single part number at a reduced price compared to ordering each component separately.

Cisco 7600 Series security bundles are based on the Cisco 7600 Series E chassis and the IP Security (IPsec) VPN SPA.

Cisco ASR 1000 Series Aggregation Services Router security bundles are available for the Cisco ASR 1002, ASR 1004, and ASR 1006 chassis and include the respective Cisco IOS XE feature licenses without the need for additional hardware support in the form of security blades or modules.

For More Information

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

Cisco ASA 5500 Series Adaptive Security Appliances

Cisco ASA 5500 Series Adaptive Security Appliances are purpose-built solutions that combine best-in-class security and VPN services with an innovative, extensible services architecture. Designed as a core component of the Cisco Secure Borderless Network, the Cisco ASA 5500 Series provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity. The result is a powerful multifunction network security appliance family that provides the security breadth and depth for protecting home-office, branch-office, small and medium-sized business, enterprise, and data center networks while reducing the overall deployment and operations costs and complexities associated with providing this new level of security.

Ideal for Companies That Need These Features

Cisco ASA 5500 Series Firewall Edition	• Ability to deploy new applications securely while protecting valuable assets from unauthorized access • Transparent firewall, virtualization, and intelligent network integration; • Comprehensive management solutions to lower operational costs: • Flexible centralized management solutions
Cisco ASA 5500 Series IPS Edition	• Customers that need to meet compliance mandates, existing Cisco ASA customers looking to enhance their security with intrusion prevention, growing customers that require their security solution to scale as they grow • Accurate inline prevention technologies • Multivector threat identification • Efficient traffic capture techniques, load-balancing capabilities, and visibility into encrypted traffic • Powerful management, event correlation, and support services

Cisco ASA 5500 Content Security Edition	• Market-leading content security capabilities, including antivirus and antispyware, URL and content filtering, antiphishing, and antispam. • Threat-protected VPN • Easy deployment and management
Cisco ASA 5500 Series SSL/IPsec VPN Edition	• SSL and IPsec VPN for any deployment environment • Clientless and full network VPN access • Flexible/shared licensing for different deployment needs • Cost-effective option for organizations needing only basic remote access capabilities

Key Features and Benefits

- Market-proven security and VPN capabilities—Full-featured, high-performance firewall, intrusion prevention system (IPS), content security, and SSL/IPsec VPN technologies deliver robust application security, user- and application-based access control, worm and virus mitigation, malware protection, content filtering, and remote user-site connectivity.
- Extensible services architecture—Taking advantage of a modular services processing and policy framework offered by the Cisco ASA 5500 Series Adaptive Security Appliances, businesses can apply specific security and network services on a per-traffic flow basis, delivering highly granular policy controls and a wide range of protective services with streamlined traffic processing. The efficiencies of this policy framework, as well as software and hardware extensibility through user-installable security services modules (SSMs) and security services cards (SSCs), advance the evolution of existing services and the deployment of new services without requiring a platform replacement or performance compromise. With these capabilities, the Cisco ASA 5500 Series provides the foundation for highly customizable security policies and exceptional services extensibility to help protect against the fast-evolving threat environment.
- Reduced deployment and operations costs—The multifunction Cisco ASA 5500 Series allows for platform configuration and management standardization, helping to decrease the costs of deployment and ongoing operations.

Specifications

Feature	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580-20	Cisco ASA 5580-40
Network location	Small Business, Branch Office, Enterprise Teleworker	Internet Edge	Internet Edge	Internet Edge	Internet Edge, Campus	Data Center, Campus	Data Center, Campus
Performance Summary							
Maximum firewall (Mbps)	150 Mbps	300 Mbps	450 Mbps	650 Mbps	1.2 Gbps	5 Gbps (real-world HTTP), 10 Gbps (jumbo frames)	10 Gbps (real-world HTTP), 20 Gbps (jumbo frames)
Maximum firewall connections	10000 / 25,000	50,000 / 130,000	280,000	400,000	650,000	1,000,000	2,000,000
Maximum firewall connections/second	4000	9000	12,000	25,000	36,000	90,000	150,000
Packets per second (64 byte)	85,000	190,000	320,000	500,000	600,000	2,500,000	4,000,000
Maximum 3DES/AES VPN throughput	100 Mbps	170 Mbps	225 Mbps	325 Mbps	425 Mbps	1 Gbps	1 Gbps
Maximum site-to-site and remote access VPN sessions	10 / 25	250	750	5000	5000	10,000	10,000
Maximum SSL VPN user sessions[1]	25	250	750	2500	5000	10,000	10,000
Bundled SSL VPN user session[1]	2	2	2	2	2	2	2
Technical Summary							
Memory	256 MB	256 MB	512 MB	1 GB	4 GB	8 GB	12 GB
Minimum system flash	64 MB	64 MB	64 MB	64 MB	64 MB	1 GB	1 GB
Maximum virtual interfaces (VLANs)	3 (trunking disabled) / 20 (trunking enabled)	50 / 100	150	200	250	100 (250[2])	100 (250[5])
Expansion Capabilities							

SSC/SSM/ICs supported	AIP SSC	CSC SSM, AIP SSM, 4GE SSM	CSC SSM, AIP SSM, 4GE SSM	CSC SSM, AIP SSM, 4GE SSM	Not Available	4-10/100/1000, 4-GE SR LC, 2-10GE SR LC	4-10/100/1000, 4-GE SR LC, 2-10GE SR LC
	Cisco ASA 5505	**Cisco ASA 5510**	**Cisco ASA 5520**	**Cisco ASA 5540**	**Cisco ASA 5550**	**Cisco ASA 5580-20**	**Cisco ASA 5580-40**
SSC/SSM/IC Expansion	1-SSC	1-SSM	1-SSM	1-SSM	Not Available	6-IC	6-IC
Intrusion Prevention	Yes (with AIP SSC)	Yes (with AIP SSM)	Yes (with AIP SSM)	Yes (with AIP SSM)	Not Available	Not Available	Not Available
Concurrent threat mitigation throughput (Mbps) (firewall + IPS services)	75 (with AIP SSC)	150 (with AIP SSM-10) 300 (with AIP SSM-20)	225 (with AIP SSM-10) 375 (with AIP SSM-20) 450 (with AIP SSM-40)	500 (with AIP SSM-20) 650 (with AIP SSM-40)	Not available	Not available	Not available
Content Security (anti-virus, anti-spyware, file blocking)	Not available	Yes (with CSC SSM)	Yes (with CSC SSM)	Yes (with CSC SSM)	Not available	Not available	Not available
Maximum number of users for anti-virus, anti-spyware, file blocking (CSC SSM only)	Not available	500 (CSC-SSM-10) 1000 (CSC-SSM-20)	500 (CSC-SSM-10) 1000 (CSC-SSM-20)	500 (CSC-SSM-10) 1000 (CSC-SSM-20)	Not available	Not available	Not available
Content Security Plus License features	Not available	Anti-spam, anti-phishing, URL filtering	Anti-spam, anti-phishing, URL filtering	Anti-spam, anti-phishing, URL filtering	Not available	Not available	Not available
Cisco Adaptive Security Appliance Software Version (latest)	8.3	8.3	8.3	8.3	8.3	8.3	8.3
Application-layer firewall services	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2 transparent firewalling	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security contexts (included/maximum)[3]	0/0	0/0 / 2/5	2/20	2/50	2/50	2/50	2/50
GTP/GPRS inspection[4]	Not available	Not available	Yes	Yes	Yes	Yes	Yes
High availability support[4]	Not supported Stateless A/S	Not supported A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S
SSL and IPsec VPN services	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPN clustering and load balancing	Not available	Not available / Yes	Yes	Yes	Yes	Yes	Yes
Advanced endpoint assessment[4]	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1. Beginning with Cisco ASA Software v7.1, SSL VPN (Web VPN) capability requires a license. Systems include 2 SSL VPN users by default for evaluation and remote management purposes.
2. Supported in a future ASA software release
3. Licensed feature
4. A/S = Active/Standby; A/A = Active/Active

Selected Part Numbers and Ordering Information

Cisco ASA 5500 Series Firewall Edition Bundles	
ASA5505-BUN-K9	Cisco ASA 5505 10-User Bundle includes 8-port Fast Ethernet switch, 10 IPsec VPN peers, 2 SSL VPN peers, Triple Data Encryption Standard/Advanced Encryption Standard (3DES/AES) license
ASA5505-K8	Cisco ASA 5505 10-User Bundle includes 8-port Fast Ethernet switch, 10 IPsec VPN peers, 2 SSL VPN peers, Data Encryption Standard (DES) license

ASA5505-50-BUN-K9	Cisco ASA 5505 50-User Bundle includes 8-port Fast Ethernet switch, 10 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license
ASA5505-UL-BUN-K9	Cisco ASA 5505 Unlimited-User Bundle includes 8-port Fast Ethernet switch, 10 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license
ASA5505-SEC-BUN-K9	Cisco ASA 5505 Unlimited-User Security Plus Bundle includes 8-port Fast Ethernet switch, 25 IPsec VPN peers, 2 SSL VPN peers, DMZ, stateless Active/Standby high availability, 3DES/AES license
ASA5510-BUN-K9	Cisco ASA 5510 Firewall Edition includes 3 Fast Ethernet interfaces, 250 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license
ASA5510-K8	Cisco ASA 5510 Firewall Edition includes 3 Fast Ethernet interfaces, 250 IPsec VPN peers, 2 SSL VPN peers, DES license
ASA5510-SEC-BUN-K9	Cisco ASA 5510 Security Plus Firewall Edition includes 2 Gigabit Ethernet + 3 Fast Ethernet interfaces, 250 IPsec VPN peers, 2 SSL VPN peers, Active/Standby high availability, 3DES/AES license
ASA5520-BUN-K9	Cisco ASA 5520 Firewall Edition includes 4 Gigabit Ethernet interfaces + 1 Fast Ethernet interface, 750 IPsec VPN peers, 2 SSL VPN peers, Active/Active and Active/Standby high availability, 3DES/AES license
ASA5520-K8	Cisco ASA 5520 Firewall Edition includes 4 Gigabit Ethernet interfaces + 1 Fast Ethernet interface, 750 IPsec VPN peers, 2 SSL VPN peers, Active/Active and Active/Standby high availability, DES license
ASA5540-BUN-K9	Cisco ASA 5540 Firewall Edition includes 4 Gigabit Ethernet interfaces + 1 Fast Ethernet interface, 5000 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license
ASA5540-K8	Cisco ASA 5540 Firewall Edition includes 4 Gigabit Ethernet interfaces + 1 Fast Ethernet interface, 5000 IPsec VPN peers, 2 SSL VPN peers, DES license
ASA5550-BUN-K9	Cisco ASA 5550 Firewall Edition includes 8 Gigabit Ethernet interfaces + 1 Fast Ethernet interface, 4 Gigabit SFP interfaces, 5000 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license
ASA5550-K8	Cisco ASA 5550 Firewall Edition includes 8 Gigabit Ethernet interfaces + 1 Fast Ethernet interface, 4 Gigabit SFP interfaces, 5000 IPsec VPN peers, 2 SSL VPN peers, DES license
ASA5580-20-BUN-K8	Cisco ASA 5580-20 Firewall Edition includes 2 management interfaces, 5000 IPsec VPN peers, 2 SSL VPN peers, DES license
ASA5580-20-BUN-K9	Cisco ASA 5580-20 Firewall Edition includes 2 management interfaces, 5000 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license
ASA5580-20-4GE-K9	Cisco ASA 5580-20 Firewall Edition 4 Gigabit Ethernet Bundle includes 4 Gigabit Ethernet interfaces, 2 management interfaces, 5000 IPsec VPN peers, 2 SSL VPN peers, Dual AC power, 3DES/AES license
ASA5580-20-8GE-K9	Cisco ASA 5580-20 Firewall Edition 8 Gigabit Ethernet Bundle includes 8 Gigabit Ethernet interfaces, 2 management interfaces, 5000 IPsec VPN peers, 2 SSL VPN peers, Dual AC power, 3DES/AES license
ASA5580-40-BUN-K8	Cisco ASA 5580-40 Firewall Edition includes 2 management interfaces, 5000 IPsec VPN peers, 2 SSL VPN peers, DES license
ASA5580-40-BUN-K9	Cisco ASA 5580-40 Firewall Edition includes 2 management interfaces, 5000 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license
ASA5580-40-8GE-K9	Cisco ASA 5580-40 Firewall Edition 8 Gigabit Ethernet Bundle includes 8 Gigabit Ethernet interfaces, 2 management interfaces, 5000 IPsec VPN peers, 2 SSL VPN peers, Dual AC power, 3DES/AES license
ASA5580-40-10GE-K9	Cisco ASA 5580-40 Firewall Edition 4 10Gigabit Ethernet Bundle includes 4 10Gigabit Ethernet interfaces; 2 management interfaces; 5000 IPsec VPN peers; 2 SSL VPN peers, Dual AC power, 3DES/AES license
Cisco ASA 5500 Series IPS Edition Bundles	
ASA5505-50-AIP5-K9	Cisco ASA 5505 50-User IPS Edition includes AIP-SSC-5, 8-port Fast Ethernet switch, 10 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license
ASA5505-U-AIP5P-K9	Cisco ASA 5505 Unlimited-User IPS Edition includes AIP-SSC-5, DMZ support, high availability, 8-port Fast Ethernet switch, 10 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license
ASA5510-AIP10-K9	Cisco ASA 5510 IPS Edition includes AIP-SSM-10, firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 5 Fast Ethernet interfaces
ASA5510-AIP10SP-K9	Cisco ASA 5510 IPS Edition includes AIP-SSM-10, firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 2 Gigabit Ethernet interfaces, 3 Fast Ethernet interfaces, and high availability

ASA5510-AIP20SP-K9	Cisco ASA 5510 IPS Edition includes AIP-SSM-20, firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 2 Gigabit Ethernet interfaces, 3 Fast Ethernet interfaces, and high availability
ASA5520-AIP10-K9	Cisco ASA 5520 IPS Edition includes AIP-SSM-10, firewall services, 750 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
ASA5520-AIP20-K9	Cisco ASA 5520 IPS Edition includes AIP-SSM-20, firewall services, 750 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
ASA5520-AIP40-K9	Cisco ASA 5520 IPS Edition includes AIP-SSM-40, firewall services, 750 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
ASA5540-AIP20-K9	Cisco ASA 5540 IPS Edition includes AIP-SSM-20, firewall services, 5000 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
ASA5540-AIP40-K9	Cisco ASA 5540 IPS Edition includes AIP-SSM-40, firewall services, 5000 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
Cisco ASA 5500 Series Content Security Edition Bundles	
ASA5510-CSC10-K9	Cisco ASA 5510 Content Security Edition includes CSC-SSM-10, 50-user antivirus/anti-spyware with 1-year subscription, firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 3 Fast Ethernet interfaces
ASA5510-CSC20-K9	Cisco ASA 5510 Content Security Edition includes CSC-SSM-20, 500-user antivirus/anti-spyware with 1-year subscription, firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 3 Fast Ethernet interfaces
ASA5520-CSC10-K9	Cisco ASA 5520 Content Security Edition includes CSC-SSM-10, 50-user antivirus/anti-spyware with 1-year subscription, firewall services, 750 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
ASA5520-CSC20-K9	Cisco ASA 5520 Content Security Edition includes CSC-SSM-20, 500-user antivirus/anti-spyware with 1-year subscription, firewall services, 750 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
Cisco ASA 5500 Series SSL/IPsec VPN Edition Bundles	
ASA5505-SSL10-K9	Cisco ASA 5505 SSL/IPsec VPN Edition includes 10 IPsec VPN peers, 10 SSL VPN peers, 50 firewall users, 8-port Fast Ethernet switch
ASA5505-SSL25-K9	Cisco ASA 5505 SSL/IPsec VPN Edition includes 25 IPsec VPN peers, 25 SSL VPN peers, 50 firewall users, 8-port Fast Ethernet switch
ASA5510-SSL50-K9	Cisco ASA 5510 SSL/IPsec VPN Edition includes 250 IPsec VPN peers, 50 SSL VPN peers, firewall services, 3 Fast Ethernet interfaces
ASA5510-SSL100-K9	Cisco ASA 5510 SSL/IPsec VPN Edition includes 250 IPsec VPN peers, 100 SSL VPN 100 peers, firewall services, 3 Fast Ethernet interfaces
ASA5510-SSL250-K9	Cisco ASA 5510 SSL/IPsec VPN Edition includes 250 IPsec VPN peers, 250 SSL VPN peers, firewall services, 3 Fast Ethernet interfaces
ASA5520-SSL500-K9	Cisco ASA 5520 SSL/IPsec VPN Edition includes 750 IPsec VPN peers, 500 SSL VPN peers, firewall services, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
ASA5540-SSL1000-K9	Cisco ASA 5540 SSL/IPsec VPN Edition includes 5000 IPsec VPN peers, 1000 SSL VPN peers, firewall services, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
ASA5540-SSL2500-K9	Cisco ASA 5540 SSL/IPsec VPN Edition includes 5000 IPsec VPN peers, 2500 SSL VPN peers, firewall services, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
ASA5550-SSL2500-K9	Cisco ASA 5550 SSL/IPsec VPN Edition includes 5000 IPsec VPN peers, 2500 SSL VPN peers, firewall services, 8 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
ASA5550-SSL5000-K9	Cisco ASA 5550 SSL/IPsec VPN Edition includes 5000 IPsec VPN peers, 5000 SSL VPN peers, firewall services, 8 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
ASA5580-20-10K-K9	Cisco ASA 5580 SSL/IPsec VPN Edition includes 10,000 IPsec VPN peers, 10,000 SSL VPN peers, firewall services, 4 Gigabit Ethernet interfaces, 2 management interfaces, Dual AC power, 3DES/AES license
Security Services Modules	
ASA-SSM-AIP-5-K9=	Cisco ASA Advanced Inspection and Prevention Security Services Module 5
ASA-SSM-AIP-10-K9=	Cisco ASA Advanced Inspection and Prevention Security Services Module 10
ASA-SSM-AIP-20-K9=	Cisco ASA Advanced Inspection and Prevention Security Services Module 20
ASA-AIP-40-INC-K9=	Cisco ASA Advanced Inspection and Prevention Security Services Module 40
ASA-SSM-CSC-10-K9=	Cisco ASA Content Security and Control Security Services Module 10 with 50-user antivirus/anti-spyware, 1-year subscription
ASA-SSM-CSC-20-K9=	Cisco ASA Content Security and Control Security Services Module 20 with 500-user antivirus/anti-spyware, 1-year subscription

SSM-4GE=	Cisco ASA 4-Port Gigabit Ethernet Security Services Module
Cisco ASA 5520 Adaptive Security Appliance for Unified Communications Security	
ASA5520-UC-BUN-K9	Cisco ASA 5520 Adaptive Security Appliance UC Security Edition; includes 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 1000 UC proxy sessions, 750 IPsec VPN peers, 2 SSL VPN peers, Active/Active and Active/Standby high availability, Triple Data Encryption Standard/ Advanced Encryption Standard (3DES/AES) license
ASA5520-UC-BUN-K8	Cisco ASA 5520 Adaptive Security Appliance UC Security Edition; includes 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 1000 UC proxy license, 750 IPsec VPN peers, 2 SSL VPN peers, Active/Active and Active/Standby high availability, DES license
Cisco ASA 5540 Adaptive Security Appliance for Unified Communications Security	
ASA5540-UC-BUN-K9	Cisco ASA 5540 Adaptive Security Appliance UC Security Edition; includes 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 2000 UC proxy sessions, 5000 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license
ASA5540-UC-BUN-K8	Cisco ASA 5540 Adaptive Security Appliance UC Security Edition includes 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 2000 UC proxy sessions, 5000 IPsec VPN peers, 2 SSL VPN peers, DES license
Cisco ASA 5550 Adaptive Security Appliance for Unified Communications Security	
ASA5580-20-UC-K9	Cisco ASA 5580 Adaptive Security Appliance UC Security Edition; includes 4 Gigabit Ethernet interfaces, 5000 UC proxy sessions, 10,000 IPSec VPN peers, 2 SSL VPN peers, 3DES/AES license,
ASA5580-20-UC-K8	Cisco ASA 5580 Adaptive Security Appliance UC Security Edition; includes 4 Gigabit Ethernet interfaces, 5000 UC proxy sessions, 10,000 IPSec VPN peers, 2 SSL VPN peers, DES license
Cisco ASA 5580 Series Interface Expansion Cards	
ASA5580-4GE-CU=	Cisco ASA 5580 4-port 10/100/1000 Ethernet interface card, RJ45
ASA5580-4GE-FI=	Cisco ASA 5580 4-port Gigabit Ethernet fiber interface card, SR, LC
ASA5580-2X10GE-SR=	Cisco ASA 5580 2-port 10 Gigabit Ethernet fiber interface card, SR, LC
Cisco ASA 5500 Series Software	
ASA-SW-UPGRADE=	Cisco ASA Software one-time upgrade for nonsupport customers

For More Information

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

Cisco Intrusion Prevention System

Business networks of all sizes now face increasingly sophisticated attacks that can impede productivity, obstruct access to applications and resources, and cause significant communications disruption. In addition, because of compliance regulations and consumer privacy laws, business priorities now include minimizing legal liability, protecting brand reputation, and safeguarding intellectual property.

A core component of Cisco Secure Borderless Network, Cisco IPS collaborates with other key network components for end-to-end network-wide protection. Threat information is shared between Cisco IPS and host-based IPS Cisco Security Agent and Cisco wireless controller. Available as a dedicated appliance, Cisco IPS is also integrated into Cisco firewall, switch, and router platforms for maximum protection and deployment flexibility.

This inline, network-based defense can identify, classify, and stop known and unknown threats, including worms, network viruses, application threats, system intrusion attempts, and application misuse.

Cisco IPS Sensors and Cisco IPS Sensor Software deliver high-performance, intelligent threat detection and protection. Cisco IPS with Global Correlation uses global threat information that has been turned into actionable intelligence, such as reputation scores, and pushed out to all enabled technologies. Reputation filtering and global inspection give Cisco IPS 7.0 several advantages:

- Twice the effectiveness of signature-only intrusion prevention systems
- More accurate with fewer false-positives using reputation
- 100 times faster than traditional signature-only methods

This technology provides metrics in both multimedia and transactional environments, so organizations can anticipate true IPS performance tailored to their business. The sensors can be deployed widely and incrementally on servers and endpoints, as dedicated appliances and as service modules on routers, switches, and firewalls. They collaborate and adapt in real time to emerging threats.

In addition, with Cisco Services for IPS, organizations easily manage their IPS deployment with near-real time updates to the most recent threats.

Ideal for Companies That Need These Features

Cisco IPS 4200 Series Sensors	• Dedicated hardware appliance platform with performance levels from 300 Mbps to 4 Gbps
Cisco Advanced Inspection and Prevention Security Services Module (AIP-SSM)	• IPS security module or card for the Cisco ASA 5500 Series for companies that want to manage IPS with their firewall in one appliance
Cisco IPS Advanced Integration Module (AIM)	• IPS AIM for the Cisco 1841, 2800, and 3800 Series Integrated Services Routers with performance level of up to 45 Mbps
Cisco IDS Services Module (NME)	• IPS NME for the Cisco 2800 and 3800 Series Integrated Services Routers with performance level of up to 75 Mbps
Cisco IDS Services Module 2 (ISDM-2)	• IPS security module for Cisco Catalyst 6500 Series Switches with up to 500 Mbps performance
Cisco IOS IPS	• Focused set of IPS capabilities using Cisco IOS Software on the router with varying performance levels

Key Features and Benefits

- Pervasive network integration—Cisco Intrusion Prevention System (IPS) solutions defeat threats from multiple vectors, including network, server, and desktop endpoints. The solutions extend across Cisco platforms, from purpose-built appliances to services modules integrated into firewall and routers and switches. A Cisco IPS solution protects the network from policy violations, vulnerability exploitations, and anomalous activity through detailed inspection of traffic at Layers 2 through 7, across the entire network.
- Collaborative threat prevention—A Cisco IPS solution employs a unique, system-wide security ecosystem that assesses and reacts to threats, delivering exceptional network scalability and resiliency. This ubiquitous alliance includes cross-solution feedback linkages, common policy management, multivendor event correlation, attack-path identification, passive-active fingerprinting, and host-based (Cisco Security Agent) IPS collaboration.
- Proactive posture adaptation—As an organization's network threat posture changes, a Cisco IPS solution evolves and adapts to stay ahead of the security landscape, mitigating threats by both known and unknown attacks. Extensive behavioral analysis, anomaly detection, policy adjustments, and rapid threat-response techniques save time, resources, and most importantly, the organization's assets and productivity.

NOTE: IPS technology strategically deployed throughout the network provides excellent end-to-end, zero-day protection. A Cisco IPS solution protects an organization's infrastructure and business.

Specifications

Feature	Cisco IPS-4240	Cisco IPS-4255	Cisco IPS-4260	Cisco IPS-4270	Cisco IPS Module (IDSM-2)	Cisco IPS Network Module (AIM)	Cisco IPS Network Module (NM-CIDS)
Performance	250 Mbps	500 Mbps	1 Gbps	2 Gbps	500 Mbps	45 Mbps	45 Mbps
Monitoring Interface	Four 10/100/1000 Base-TX	Four 10/100/1000 Base-TX	Autosensing 10/100/1000 Base-TX	Four 10/100/1000 Base-TX or Four 10-00Base-SX	PCI	Internal 10/100 Mbps Ethernet	Internal 10-100-Mbps Ethernet and external 10-100-Mbps Ethernet
Optional Interface			4x 10/100/1000 Base-TX 2x1000SX	• Four 10/100/1000 Base-TX • Two 1000Base-SX (fiber) (up to 16 total monitoring interfaces)			
Command and Control Interface	10/100 Base-TX	10/100 Base-TX	10/100 Base-TX	Two onboard 10/100/1000 Base-TX	PCI	10/100 Base-TX (on host ISR)	10/1010/100 Base-TX

Selected Part Numbers and Ordering Information

Cisco IPS 4200 Appliances	
IPS-4240-K9	Cisco IPS 4240 Sensor (chassis, software, SSH, four 10/100/1000BASE-TX interfaces with RJ-45 connector)

IPS4240-DC-K9	Cisco IPS 4240 NEBS-Compliant Sensor with DC power (chassis, software, SSH, four 10/100/1000BASE-TX interfaces with RJ-45 connector)
IPS-4255-K9	Cisco IPS 4255 Sensor (chassis, software, SSH, four 10/100/1000BASE-TX interfaces with RJ-45 connector)
IPS-4260-K9	Cisco IPS 4260 Sensor (chassis, software, SSH, two onboard 10/100/1000BASE-TX interfaces with RJ-45 connector)
IPS-4260-4GE-BP-K9	Cisco IPS 4260 Sensor with an included 4-GE copper NIC with hardware bypass (chassis, software, SSH, two onboard 10/100/1000BASE-TX interfaces with RJ-45 connector, and four 10/100/1000BASE-TX interfaces with built-in bypass)
IPS-4260-2SX-K9	Cisco IPS 4260 Sensor with an included NIC card (chassis, software, SSH, two onboard 10/100/1000BASE-TX interfaces with RJ-45 connector, and two fiber interfaces)
IPS4270-20-K9	Cisco IPS 4270 Sensor (chassis, redundant power, software, SSH, two onboard 10/100/1000BASE-TX interfaces with RJ-45 connector)
IPS4270-20-4GE-K9	Cisco IPS 4270 Sensor (chassis, redundant power, software, SSH, two onboard 10/100/1000BASE-TX interfaces with RJ-45 connector, and four 10/100/1000BASE-TX interfaces)
IPS4270-20-4SX-K9	Cisco IPS 4270 Sensor (chassis, redundant power, software, SSH, two onboard 10/100/1000BASE-TX interfaces with RJ-45 connector, and four fiber interfaces)
IPS-4GE-BP-INT=	Spare 4-port copper interface card with built-in hardware bypass for the Cisco IPS 4260 and 4270
IPS-2SX-INT=	Spare 2-port fiber interface card for the Cisco IPS 4260 and 4270
IPS Modules on ISR	
AIM-IPS-K9	Cisco Intrusion Prevention System Advanced Integrated Module for Cisco 1841, 2800, 3800
NME-IPS-K9	Cisco Intrusion Prevention System Advanced Integrated Module for Cisco 2800, 3800
Security Services Modules	
ASA-SSC-AIP-5-K9=	Cisco ASA Advanced Inspection and Prevention Security Services Card 5
ASA-SSM-AIP-10-K9=	Cisco ASA Advanced Inspection and Prevention Security Services Module 10
ASA-SSM-AIP-20-K9=	Cisco ASA Advanced Inspection and Prevention Security Services Module 20
ASA-AIP-40-INC-K9 =	Cisco ASA Advanced Inspection and Prevention Security Services Module 40
Select Bundles	
ASA5510-AIP10-K9	Cisco ASA 5510 IPS Edition includes AIP-SSM-10, firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 5 Fast Ethernet interfaces
ASA5520-AIP10-K9	Cisco ASA 5520 IPS Edition includes AIP-SSM-10, firewall services, 750 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
ASA5520-AIP20-K9	Cisco ASA 5520 IPS Edition includes AIP-SSM-20, firewall services, 750 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
ASA5520-AIP40-K9	Cisco ASA 5520 IPS Edition includes AIP-SSM-40, firewall services, 750 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
ASA5540-AIP20-K9	Cisco ASA 5540 IPS Edition includes AIP-SSM-20, firewall services, 5000 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
ASA5540-AIP40-K9	Cisco ASA 5540 IPS Edition includes AIP-SSM-40, firewall services, 5000 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface
WS-C6506E-IPSC-K9	Cisco Catalyst 6506-E Switch, Supervisor Engine 32 with 8 x 1 Gigabit Ethernet Small Form-Factor Pluggable (SFP) plus 1 x 10/100/1000 uplink port, 8 copper SFP interfaces, 4 IDSM-2s, and 1 Power-Supply 3000W
WS-C6506E-IPSF-K9	Cisco Catalyst 6506-E Switch, Supervisor Engine 32 with 8 x 1 Gigabit Ethernet SFP plus 1 x 10/100/1000 uplink port, 8 multimode fiber SFP interfaces, 4 IDSM-2s, and 1 Power-Supply 3000W
WS-C6506E-IPS10GK9	Cisco Catalyst 6506-E Switch, Supervisor Engine 32 with 2 x 10 Gigabit Ethernet XENPAK plus 1 x 10/100/1000 uplink port, 2 short-range 10 Gigabit XENPAK interfaces, 4 IDSM-2s, and 1 Power-Supply 3000W

For More Information

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

Cisco Catalyst 6500 Series Firewall Services Module

The Cisco Catalyst 6500 Series Firewall Services Module (FWSM) is a high-speed, integrated firewall module for Cisco Catalyst 6500 Switches and Cisco 7600 Series Routers. It provides the fastest firewall data rates in the industry: 5-Gbps throughput, 100,000 cells per second (CPS), and 1 million concurrent connections. Up to four FWSMs can be installed in a single chassis, providing scalability to 20 Gbps per chassis. Based on Cisco PIX Firewall technology, the Cisco FWSM offers large enterprises and service providers unmatched security, reliability, and performance.

The Cisco FWSM includes a number of advanced features that help reduce costs and operational complexity while allowing organizations to manage multiple firewalls from the same management platform. Features such as resource manager helps organizations limit the resources allocated to any security context at any time, thus helping ensure that one security context does not interfere with another. The transparent firewall feature configures the FWSM to act as a Layer 2 bridging firewall, resulting in minimal changes to network topology.

Ideal for Companies That Need These Features

Cisco Catalyst 6500 Series Firewall Services Module	· Ability to add an integrated firewall module for Cisco Catalyst 6500 Switches and Cisco 7600 Series routers

Key Features and Benefits

- An integrated module—Installed inside a Cisco Catalyst 6500 Series Switch or Cisco 7600 Internet Router, the Cisco Catalyst 6500 Series Firewall Services Module (FWSM) allows any port on the device to operate as a firewall port and integrates firewall security inside the network infrastructure.
- Compatibility with future versions—The FWSM can handle up to 5 Gbps of traffic, providing exceptional performance to meet future requirements without requiring a system overhaul. Up to three additional FWSMs can be added to the Cisco Catalyst 6500 to achieve better than 10-Gigabit Ethernet scalability.
- Enhanced reliability—The FWSM is based on Cisco PIX technology and uses the same time-tested Cisco PIX Operating System, a secure, real-time operating system.
- Lower cost of ownership—The FWSM offers among the best price-to-performance ratios of any firewall. Because FWSM is based on the Cisco PIX Firewall, the cost of training and management is lower, and because it is integrated in the chassis, there are fewer boxes to manage.
- Ease of use—The intuitive GUI of the Cisco PIX Device Manager can be used to manage and configure the features within the FWSM. The FWSM can now be managed using the Cisco ASA 5500 Series Adaptive Security Device Manager (ASDM) v5.2 as well.
- Efficiency and productivity gains—Virtualized FWSM delivers multiple firewalls on one physical hardware platform. Network administrators can configure, deploy, and manage these functions as if they were separate devices. Using virtualization to reduce the number of physical devices in a network significantly reduces the cost and complexity of managing network infrastructure.

Specifications

Feature	Cisco Catalyst 6500 Series Firewall Services Module
Leading scalability and performance	5.5 Gbps throughput per service module; Up to four FWSMs (20 Gbps) per Catalyst 6500 chassis with static VLAN or IOS Policy-based Routing; 2.8 Mpps; 1 million concurrent connections; 100,000 connection setups and teardowns per second; 256,000 concurrent NAT or PAT translations; Jumbo Ethernet packets (8500 bytes) supported
VLAN Interfaces	1000 total per service module; 256 VLANs per security context in routed mode; 8 VLAN pairs per security context in transparent mode
Access Lists	Up to 80,000 access control entries in single context mode NOTE: The FWSM implements Layer 3 and 4 access control security checks in hardware with virtually no performance impact using non-upgradeable high-speed memory
Virtual Firewalls (Security Contexts)	20, 50, 100, 250 Virtual Firewall licenses; Virtual Firewalls and 1 administrative context are provided for testing purposes.
Every port within the chassis becomes a security port	Every FWSM works in tandem with other modules in the chassis to deliver robust security throughout the entire chassis
New services can be deployed with minimal operational complexity	The integrated approach of the Cisco FWSM integrates virtualization and high availability. Solutions are enhanced through complementary functions. This integrated approach maximizes return on network investment by: · Building on the existing network: All FWSMs take advantage of the infrastructure to deliver new services · Simplifying maintenance and management: Integration of services modules into one chassis allows for ease of use and support for network administrators · Reducing environmental costs: Lower overall power and cabling costs

Selected Part Numbers and Ordering Information

Hardware	
WS-SVC-FWM-1-K9	Cisco Firewall Services Module for Cisco Catalyst 6500 and 7600 Series

WS-SVC-FWM-1-K9=	Cisco Firewall Services Module for Cisco Catalyst 6500 and 7600 Series (spare)
Security Bundles	
WS-C6506-E-FWM-K9	Cisco Catalyst 6506 Firewall Security System with Enhanced Chassis and Supervisor 720 3B
WS-C6509-E-FWM-K9	Cisco Catalyst 6509 Firewall Security System with Enhanced Chassis and Supervisor 720 3B
WS-C6513-FWM-K9	Cisco Catalyst 6513 Firewall Security System with Supervisor 720 3B
WS-6509EXL-2FWM-K9	Cisco Catalyst 6509 Firewall Security System with Enhanced Chassis, Supervisor 720 3BXL and two Firewall Service Modules
WS-6513XL-2FWM-K9	Cisco Catalyst 6513 Firewall Security System with Supervisor 720 3BXL and two Firewall Service Modules
WS-6506-EXL-FWM-K9	Cisco Catalyst 6506 Firewall Security System with Enhanced Chassis, Supervisor 720 3BXL and one Firewall Service Module
WS-6509-EXL-FWM-K9	Cisco Catalyst 6506 Firewall Security System with Enhanced Chassis, Supervisor 720 3BXL and one Firewall Service Module
WS-C6513-XL-FWM-K9	Cisco Catalyst 6513 Firewall Security System with Enhanced Chassis, Supervisor 720 3BXL and one Firewall Service Module
Software	
SC-SVC-FWM-1.1-K9	Firewall Services Module Software Release 1.1 for Cisco Catalyst 6500 and 7600 Series
SC-SVC-FWM-2.2-K9	Firewall Services Module Software Release 2.2 for Cisco Catalyst 6500 and 7600 Series
SC-SVC-FWM-2.3-K9	Firewall Services Module Software Release 2.3 for Cisco Catalyst 6500 and 7600 Series
SC-SVC-FWM-3.1-K9	Firewall Services Module Software Release 3.1 for Cisco Catalyst 6500 and 7600 Series
SC-SVC-FWM-3.2-K9	Firewall Services Module Software Release 3.2 for Cisco Catalyst 6500 and 7600 Series

NOTE: Cisco Firewall Services Module Software 1.1 has reached end-of-sale status. Customers are encouraged to upgrade or purchase FWSM Software 2.3 or 3.1, 3.2.

For More Information

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html

Cisco TrustSec

Cisco TrustSec Solution helps customers secure their networks, data, and resources using their organization's security policy, user and device identity information, pervasive access control mechanisms, and data protection for network traffic. Cisco TrustSec is a foundational component of Cisco Secure Borderless Networks. The three key Cisco TrustSec functional areas are:

- Policy-based access control
- Identity-aware networking
- Data integrity and confidentiality

Policy-Based Access Control

Cisco TrustSec provides network access controls based on a consistent policy for users, endpoint devices, and networking devices (such as routers and switches). Cisco TrustSec has the ability to control how a user or a device can be granted access, what security policies endpoint devices must meet, such as posture compliance, and what network resources a user is authorized to use in the network.

Identity-Aware Networking

Cisco TrustSec uses end-user and device identity and other information (such as time and location) to provide precise security policy controls. These policy controls can be implemented not only at the network edge where users first connect to the network, but also throughout the entire network. Cisco TrustSec also delivers further role-based networking services, including support for Cisco Medianet and quality of service for business-critical applications.

Data Integrity and Confidentiality

Cisco TrustSec secures data paths in the switching environment with IEEE 802.1AE standard encryption. Cisco switching infrastructure maintains controls so that critical security applications such as firewalls, intrusion prevention, and content inspection can retain visibility into data streams.

Key Features and Benefits

- Enables highly secure collaboration—TrustSec dynamically assigns access and services for users and devices to support a mobile workforce. Having a consistent set of security policies in place helps support a more secure and collaborative business environment and offers a smooth, reliable user experience as well.
- Strengthens security—TrustSec helps secure access to your network and resources whether your connection is wired, wireless, or over VPN. It also helps ensures that endpoint devices are authorized and healthy with consistent, network-wide security policy enforcement.
- Addresses compliance—TrustSec helps address compliance requirements by providing access control to sensitive and valuable information and assets, collecting user activity and history data, as well as providing

end-to-end monitoring and reporting capabilities. You can use these capabilities for controls, auditing, and reporting as part your effort to meet compliance requirements.

For More Information

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

Cisco NAC Appliance (Clean Access)

Cisco NAC Appliance (formerly Cisco Clean Access) is an easily deployed Network Admission Control (NAC) product that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. With NAC Appliance, network administrators can authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to network access. It identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with your network's security policies and repairs any vulnerabilities before permitting access to the network.

Cisco NAC has several core components, with additional optional components for enhanced capabilities.

- Cisco NAC Server—This device initiates assessment and enforces access privileges based on endpoint compliance. Users are blocked at the port layer and restricted from accessing the trusted network until they successfully pass inspection. The Cisco NAC Server is available in seven sizes based on the number of online, concurrent users: 100, 250, 500, 1500, 2500, 3500, and 5000 users. A single company can have several servers of differing sizes; for example, a headquarters building would require a 1500-user Cisco NAC Server, while a branch office for the same company might only require a 100-user server.
- Cisco NAC Manager—A centralized, web-based console for establishing roles, checks, rules, and policies. The Cisco NAC Manager is available in three sizes: the Cisco NAC Lite Manager manages up to three Cisco NAC Servers; the Cisco NAC Standard Manager manages up to 20 Cisco NAC Servers; and the Cisco NAC Super Manager manages up to 40 Cisco NAC Servers or 80 Cisco NAC Network Modules.
- Cisco NAC Agent—A thin, read-only agent that enhances posture assessment functions and streamlines remediation. Cisco NAC Agents are optional and are distributed free of charge.

Ideal for Companies That Need These Features

Cisco NAC Appliance (Clean Access)	• Minimized network outages • Enforcement of security policies • Significant cost savings with automated device repairs and updates

Key Features and Benefits

- Authentication integration with single sign-on—Cisco NAC serves as an authentication proxy for most forms of authentication, natively integrating with Kerberos, Lightweight Directory Access Protocol (LDAP), RADIUS, Active Directory, S/Ident, and others. Cisco NAC supports single sign-on for VPN clients, wireless clients, and Windows Active Directory domains.
- Vulnerability assessment—Cisco NAC supports scanning of all Windows, Mac OS, and Linux-based operating systems and machines, as well as non-PC networked devices such as game consoles, PDAs, printers, and IP phones. It conducts network-based scans or can use custom-built scans as required. Cisco NAC can check for any application as identified by registry key settings, services running, or system files.
- Device quarantine—Cisco NAC can place noncompliant machines into quarantine. Quarantine can be accomplished by using subnets as small as /30, or by using a quarantine VLAN.
- Automatic security policy updates—Automatic security policy updates that are part of Cisco's standard software maintenance package provide predefined policies for the most common network access criteria, including policies that check for critical operating system updates, common antivirus software virus definition updates, and common antispyware definition updates.
- Centralized Management—The Cisco NAC web-based management console allows administrators to define the types of scans required for each role, as well as the related remediation packages necessary for recovery. One management console can manage multiple servers.
- Remediation and Repair—Quarantining gives devices access to remediation servers that can provide operating system patches and updates, virus definition files, or endpoint security solutions such as Cisco Security Agent. Administrators can enable automated remediation through the optional agent, or specify a series of remediation instructions. In addition, Cisco NAC delivers user-friendly features, such as the monitoring mode and silent remediation, to minimize user impact.
- Flexible Deployment Modes—Cisco NAC offers the broadest array of deployment modes to fit into any customer network. Customers can deploy the product as a virtual or real IP gateway, at the edge or centrally, with Layer 2 or Layer 3 client access, and in-band or out-of-band with network traffic.

Specifications

	Cisco NAC Appliance 3315	Cisco NAC Appliance 3355	Cisco NAC Appliance 3395
Products	• Cisco NAC Server for 100, 250, and 500 users • Cisco NAC Lite Manager	• Cisco NAC Server for 1500, 2500, 3500, and 5000 users • Cisco NAC Standard Manager	• Cisco NAC Super Manager
Processor	Quad-core Intel Xeon (Core 2 Quad)	Quad-core Intel Xeon (Nehalem)	2 x Quad-core Intel Xeon (Nehalem)
Memory	4 GB	6 GB	8 GB
Hard disk	250-GB SATA drive	2 x 300-GB SAS RAID drives	4 x 300-GB SFF SAS RAID drives
Removable media	CD/DVD-ROM drive	CD/DVD-ROM drive	CD/DVD-ROM drive

Network Connectivity			
Ethernet network interface cards (NICs)	• 2 x Integrated NICs • 2 x Gigabit NICs (PCI-X)	• 2 x Integrated NICs • 2 x Gigabit NICs (PCI-X)	• 2 x Integrated NICs • 2 x Gigabit NICs (PCI-X)
10BASE-T cable support	Category (Cat) 3, 4, or 5 unshielded twisted pair (UTP) up to 328 ft (100 m)	Cat 3, 4, or 5 UTP up to 328 ft (100 m)	Cat 3, 4, or 5 UTP up to 328 ft (100 m)
10/100/1000BASE-TX cable support	Cat 5 UTP up to 328 ft (100 m)	Cat 5 UTP up to 328 ft (100 m)	Cat 5 UTP up to 328 ft (100 m)
Secure Sockets Layer (SSL) accelerator card	None	Cavium CN1120-NHB-E	Cavium CN1120-NHB-E
Interfaces			
Serial ports	1	1	1
USB 2.0 ports	4 (two front, two rear)	4 (one front, one internal, two rear)	4 (one front, one internal, two rear)
Keyboard ports	1	1	1
Video ports	1	1	1
Mouse ports	1	1	1
External SCSI ports	None	None	None
System Unit			
Form factor	Rack-mount 1 RU	Rack-mount 1 RU	Rack-mount 1 RU
Weight	35 lb (15.87 kg) fully configured	35 lb (15.87 kg) fully configured	35 lb (15.87 kg) fully configured
Dimensions	1.70 x 16.78 x 27.75 in. (4.32 x 42.62 x 70.49 cm)	1.70 x 16.78 x 27.75 in. (4.32 x 42.62 x 70.49 cm)	1.70 x 16.78 x 27.75 in. (4.32 x 42.62 x 70.49 cm)
Power supply	350W	Dual 675W (redundant)	Dual 675W (redundant)
Cooling fans	6; non-hot plug, nonredundant	9; redundant	9; redundant
BTU rating	2661 BTU/Hr (at 120V)	2661 BTU/Hr (at 120V)	2661 BTU/Hr (at 120V)
Regulatory and Standards Compliance			
Industry certifications	FIPS 140-2 Level 2 Common Criteria EAL2	FIPS 140-2 Level 2 Common Criteria EAL2	FIPS 140-2 Level 2 Common Criteria EAL2

Selected Part Numbers and Ordering Information

NACMGR-3-K9	Cisco NAC Appliance 3310 Manager—Max 3 servers
NACMGR-3FB-K9	Cisco NAC Appliance 3310 Manager Failover Bundle—Max 3 servers
NACMGR-20-K9	Cisco NAC Appliance 3350 Manager—Max 20 servers
NACMGR-20FB-K9	Cisco NAC Appliance 3350 Manager Failover Bundle—Max 20 servers
NACMGR-40-K9	Cisco NAC Appliance 3390 Manager—Max 40 servers
NACMGR-40FB-K9	Cisco NAC Appliance 3390 Manager Failover Bundle—Max 40 servers

For More Information

http://www.cisco.com/en/US/products/ps6128/index.html

Cisco Secure Access Control System (ACS)

Cisco Secure Access Control System (ACS) is a highly scalable, high-performance access policy system that centralizes device administration, authentication, and user access policy and reduces the management and support burden for these functions.

Cisco Secure ACS 5.1 is the second release of this next-generation network identity and access solution. This release establishes Cisco Secure ACS as a Policy Administration Point (PAP) and Policy Decision Point (PDP) for policy-based access control. Release 5.1 offers additional capabilities, including:

- A powerful, attribute-driven rules-based policy model that addresses complex policy needs in a flexible manner
- A lightweight, web-based graphical user interface (GUI) with intuitive navigation and workflow
- Integrated advanced monitoring, reporting, and troubleshooting capabilities for maximum control and visibility

- Improved integration with external identity and policy databases, including Windows Active Directory and Lightweight Directory Access Protocol (LDAP)-accessible databases, simplifying policy configuration and maintenance
- A distributed deployment model that enables large-scale deployments and provides a highly available solution

The Cisco Secure ACS 5.1 rules-based policy model supports the application of different authorization rules under different conditions, and thus policy is contextual and not limited to authorization determined by a single group membership. New integration capabilities allow information in external databases to be directly referenced in access policy rules, and attributes can be used both in policy conditions and authorization rules.

Cisco Secure ACS 5.1 features centralized collection and reporting for activity and system health information for full manageability of distributed deployments. It supports proactive operations such as monitoring and diagnostics, and reactive operations such as reporting and troubleshooting. Advanced features include a deployment-wide session monitor, threshold-based notifications, entitlement reports, and diagnostic tools.

Key Features and Benefits

- Complete access control and confidentiality solution—Can be deployed with other Cisco TrustSec components-including policy components, infrastructure enforcement components, endpoint components, and professional services-for a comprehensive access control and confidentiality solution.
- AAA protocols—Cisco Secure ACS 5.1 supports two distinct protocols for authentication, authorization, and accounting (AAA). Cisco Secure ACS 5.1 supports RADIUS for network access control and TACACS+ for network device access control. Cisco Secure ACS is a single system for enforcing access policy across the network.
- Database options—Cisco Secure ACS 5.1 supports an integrated user repository in addition to supporting integration with existing external identity repositories such as Windows Active Directory and LDAP. Multiple databases can be used concurrently for maximum flexibility in enforcing access policy.
- Authentication protocols—Cisco Secure ACS 5.1 supports a wide range of authentication protocols including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST), and EAP-Transport Layer Security (TLS) to support your authentication requirements.
- Access policies—Cisco Secure ACS 5.1 supports a rules-based, attribute-driven policy model that provides greatly increased power and flexibility for access control policies that may include authentication protocol requirements, device restrictions, time of day restrictions, posture validation, and other access requirements. Cisco Secure ACS may apply downloadable access control lists (dACLs), VLAN assignments, and other authorization parameters.
- Centralized management—Cisco Secure ACS 5.1 supports a completely redesigned lightweight, web-based GUI that is easy to use. An efficient, incremental replication scheme quickly propagates changes from primary to secondary systems providing centralized control over distributed deployments. Software upgrades are also managed through the GUI and can be distributed by the primary system to secondary instances.
- Monitoring and troubleshooting—Cisco Secure ACS 5.1 includes an integrated monitoring, reporting, and troubleshooting component that is accessible through the web-based GUI. This tool provides maximum visibility into configured policies and authentication and authorization activities across the network. Logs are viewable and exportable for use in other systems as well.
- Platform options—Cisco Secure ACS 5.1 is available as a closed and hardened Linux-based appliance or as a software operating system image for VMware ESX.

Cisco Secure Access Control Server (ACS) Express

Cisco Secure Access Control Server (ACS) Express is an entry-level RADIUS and TACACS+ authentication, authorization, and accounting (AAA) server for retail branch locations, enterprise branch offices, and small and medium-sized businesses (SMBs) that have fewer than 350 users and 50 devices.

Cisco Secure ACS Express provides a centralized identity networking solution that:

- Offers a simple user and access policy management interface
- Gives administrators greater access to and control of users and machines in various networks including wireless, wired, and virtual private networks
- Controls administrative access to network devices using RADIUS and TACACS+

This product is intended to serve small to medium-sized businesses, retail sites and enterprise branch offices where customers need an easy-to-use GUI yet require a comprehensive but simple feature set and a lower price point to address their specific deployment needs.

Cisco Policy Administration Point (PAP)

Cisco Policy Administration Point (PAP) provides centralized administration, management and monitoring of entitlement policies, and delegation and integration with enterprise information repositories such as Active Directory and Lightweight Directory Access Protocol (LDAP).

Cisco Secure Access Control Server (ACS) Solution Engine

The Cisco Secure Access Control Server (ACS) Solution Engine is a dedicated, rack-mountable appliance for network access policy control. It helps companies comply with growing regulatory and corporate requirements, improve productivity, and contain costs. It supports multiple scenarios simultaneously, including:

- Device administration: Authenticates administrators, authorizes commands, and provides an audit trail
- Remote Access: Works with VPN and other remote network access devices to enforce access policies
- Wireless: Authenticates and authorizes wireless users and hosts and enforces wireless-specific policies
- Network admission control: Communicates with posture and audit servers to enforce admission control policies

Cisco Secure Access Control System (ACS) View

Cisco Secure Access Control System (ACS) View provides the highest level of reporting, alerting, and troubleshooting functions for Cisco Secure ACS deployments. Providing maximum visibility into configured

policies and authentication and authorization activities across the network, Cisco Secure ACS View is the ideal solution for organizations that require the greatest levels of reporting and control.

Specifications

Component Specifications	Cisco ACS 5.1
CPU	Intel Xeon 2.66-GHz Q9400 (Quad Core)
System memory	4 GB DDR II ECC
Hard disk drive	2 x 250 GB 7.2K RPM 3.5" SATA
Optical storage	DVD-ROM
Network connectivity	4 10/100/1000, RJ-45 interfaces
I/O ports	1 serial port, 4 USB 2.0 (2 front, 2 rear), SVGA Video
Rack-mounting	4-post (kit included)
Physical dimensions (1RU)	17.3 (W) x 22.0 (D) x 1.75 (H) in.; 44.0 (W) x 55.9 (D) x 4.45 (H) cm
Weight	24.25 (minimum) to 28.0 lb (maximum); 11.0-12.7 kg
Power Specifications	
Number of Power Supplies	1
Power Supply Size	351W universal, autoswitching
Environmental Specifications	
Operating temperature range	50 to 95°F; 10 to 35°C (up to 3000 ft / 914.4m)
Heat emitted	341 (minimum) to 1024 (maximum) BTUs; 100-300W
Maximum altitude	7000 ft; 2133 m
Component Specifications	
VMware Version	ESX 3.5 or ESX 4.0
CPU	Intel Core 2 (2.13 GHz)
System memory	4 GB
Hard disk requirement	Minimum 512 GB
Cisco Secure Access Control Server (ACS) Express	
Processor	Intel 352 Celeron D
Memory	1 GB RAM
Hard drive	250 GB
Optical Drive	DVD-ROM
Interfaces	Two onboard 10/100/1000 Ethernet NIC ports
Cisco Secure Access Control Server (ACS) 4.2	
Hardware Requirements	· IBM PC compatible with Pentium IV processor, 1.8 GHz or faster · 1GB RAM minimum · Color monitor with minimum graphics resolution of 256 colors at 800 x 600 resolution · CD-ROM drive · 100BaseT or faster network connection
OS Requirements	Windows Server 2003, R2, Service Pack 2
Cisco ACS Secure Solution Engine	
Processor	Pentium IV, 3.4 GHz
Memory	1 GB RAM
Hard drive	120 GB SATA
Optical Drive	CD/DVD combo
Interfaces	Two integrated 10/100/1000 Ethernet ports

Selected Part Numbers and Ordering Information

For the most up to date part numbers, please visit http://www.cisco.com/go/acs

For More Information

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

Cisco IronPort E-mail Security Solutions

The Cisco IronPort E-mail Security Solutions are easy-to-deploy solutions that defend your e-mail system against spam, viruses, phishing, and a wide variety of other threats. In use at eight of the ten largest Internet service providers (ISPs) and more than 40 percent of the world's largest enterprises, these systems have a demonstrated record of unparalleled security and reliability. Cisco IronPort e-mail security appliances protect enterprises of all sizes—the same code base that power our most sophisticated customers is used in the entire product family. By reducing the downtime associated with e-mail-borne malware, these products simplify the administration of corporate mail systems and reduce the burden on technical staff while offering insight into mail system operations.

Ideal for Companies That Need These Features

Cisco IronPort E-mail Security Services	• Anti-spam and anti-virus solution • Data loss prevention (DLP) • Regulatory compliance • E-mail encryption
Cisco IronPort Cloud E-mail Security	Delivers leadership with choice, providing superior protection and control with the cost-effective convenience of a cloud deployment model. It stops spam and viruses with a fully-supported infrastructure in Cisco data centers. Maximum data protection eliminates data contamination, reduces overhead, increases the speed of deployment and provides capacity assurance for future growth.
Cisco IronPort Hybrid E-mail Security	Offers that maximizes flexibility by dividing control between the customer site and Cisco cloud-based, software as a service (SaaS) infrastructure. With a divided control model, whereby appliances reside on the customer premises and in the Cisco data center, this model secures an organization's e-mail infrastructure by stopping spam and viruses. It also provides maximum flexibility and optimal design with additional outbound controls including DLP, encryption and onsite LDAP integration.
Cisco IronPort Managed E-mail Security	Secures an organization's e-mail infrastructure by stopping spam and viruses, allowing IT managers to focus on other strategic initiatives. This service eliminates the need to continuously train personnel and budget for more hardware due to increasing spam volumes. Customers benefit from the highest levels of data security provided by an on-site e-mail security appliance, while taking advantage of the flexibility to delegate some or all of the management and maintenance responsibilities.

NOTE: Please contact IronPort for sizing of specific appliances.

Key Features and Benefits

- IronPort AsyncOS—IronPort AsyncOS is a unique, high-performance software architecture engineered from the ground up to address concurrency-based communications bottlenecks and the limitations of file-based queuing.
- IronPort Reputation Filters—IronPort Reputation Filters perform a real-time e-mail threat assessment and then identify suspicious e-mail senders. Suspicious senders are rate-limited or blocked, preventing malicious traffic from entering the network. As the first line of defense on the IronPort e-mail security appliances, Reputation Filters dispose of up to 90 percent of incoming spam at the connection level -- saving bandwidth, conserving system resources, and yielding the very highest levels of security for critical messaging systems. A proven preventive solution, IronPort Reputation Filters defend the largest Internet service provider (ISP) and enterprise networks, as well as small and medium-sized businesses (SMBs), in production environments around the world.
- IronPort Anti-Spam—The catch rate of IronPort Anti-Spam is 97 to 99 percent. Its false positive rate is less than 1 in 1 million. To eliminate the broadest range of known and emerging e-mail threats, IronPort Anti-Spam combines best-of-class conventional techniques with breakthrough context-sensitive detection technology.
- IronPort Virus Outbreak Filters—IronPort Virus Outbreak Filters detect new virus outbreaks in real time, and then quarantine suspicious messages -- offering protection up to 42 hours before traditional anti-virus solutions.
- IronPort E-mail Encryption—IronPort E-mail Encryption technology revolutionizes e-mail encryption, meeting compliance requirements while delivering powerful new business-class e-mail features.
- IronPort Data Loss Prevention (DLP)—IronPort delivers high-performance, comprehensive data loss prevention for data in motion, helping organizations both large and small prevent leaks, enforce compliance, and protect their brand and reputation.
- The IronPort SenderBase Network—SenderBase collects data from more than ten times the networks of competing monitoring systems, with data on more than 30 percent of the world's e-mail and Web traffic. This volume provides a very statistically significant sample size, resulting in immediate and accurate detection of even low-volume mail senders. A highly diverse group of more than 100,000 organizations, including some of the largest networks in the world, contribute information to IronPort's SenderBase on a remarkable 5 billion messages per day. SenderBase gives mail administrators excellent real-time visibility into security threats from around the world.
- The Threat Operations Center—The 24-hour Threat Operations Center (TOC) provides a view into global traffic activity, enabling IronPort to analyze anomalies, uncover new threats, and track traffic trends.

For More Information

http://www.cisco.com/web/products/ironport

Cisco IronPort Secure Web Security Appliances

The Cisco IronPort S-Series Web Security Appliance provides multiple layers of defense against these risks, both horizontally (at the application layer) and vertically (up the protocol stack). Cisco IronPort Web Usage Controls enforce acceptable-use policy (AUP), while Cisco Security Intelligence Operations, Cisco IronPort Web Reputation Filters, and the Cisco IronPort Anti-Malware System—with simultaneous scanning by Sophos, Webroot, and McAfee for greater efficacy—provide protection against web-based malware.

The Cisco IronPort S-Series also offers comprehensive coverage for the three most common protocols carrying business information across the boundary and over the Internet: HTTP, HTTPS, and FTP. Finally, the Layer 4 Traffic Monitor detects and blocks phone-home malware activity that attempts to circumvent port 80 security features. With threats becoming more complex and sophisticated, Cisco IronPort S-Series appliances offer one of the industry's most comprehensive Web security protection and enterprise-class performance.

Ideal for Companies That Need These Features

Cisco IronPort S-Series Secure Web Security Appliance	• A secure web gateway, with multiple layers of defense against malware • High security and high performance • Consolidated security, Acceptable Use Policy (AUP), application control, and content caching features, all on a single, integrated appliance • HTTPS decryption and scanning • Data security and off-box DLP support

Key Features and Benefits

- Single appliance security and control—The Cisco IronPort S-Series offers a single appliance solution to secure and control the three greatest web traffic risks facing enterprise networks: security risks, resource risks, and compliance risks.
- Mitigation of malware risks and costs—With malware infecting approximately 75 percent of corporate desktops, overhead for managing infected desktops, ensuring minimal downtime to employees, and minimizing the risk of information leakage is considerable.
- Reduced administrative costs—By stopping these threats at the network perimeter with Cisco IronPort Web Security Appliances, enterprises can significantly reduce the administrative costs, prevent attacker phone-home activity on networks, reduce support calls, enhance worker productivity, and also eliminate the business exposure that accompanies these threats.
- Complete, accurate protection—Cisco IronPort S-Series appliances are designed from the beginning to address the broadest range of web-based malware threats, including those from the use of FTP and dynamic Web 2.0 sites. A multilayered defense that includes Cisco Security Intelligence Operations, Cisco IronPort Web Usage Controls, Cisco IronPort Web Reputation Filters, and Cisco IronPort DVS technology (with multiple antimalware scanning engines running simultaneously) helps ensure industry-leading accuracy.

This multilayered protection is based on a comprehensive content application layer inspection, as well as network layer pattern detection, checking both inbound and outbound activities. These innovations make the Cisco IronPort S-Series one of the industry's most secure web gateways.

- Enforcement of acceptable use policies—By implementing acceptable use web policies, enterprises can both conserve resources for work-related web usage and inform employees to help shape web access behavior over time. Enterprises can increase the amount of time that employees spend on business-oriented activities, reducing misuse of enterprise networks and bandwidth.
- Simplified data security—The data-loss problem extends well beyond malware. Employees can easily use webmail to send a message including proprietary information, post confidential data on social networks and blogs, or transfer financial documents over FTP to a server outside the corporate network. Making sure that sensitive data does not leave the corporate boundary-while allowing employees to take advantage of the full power of the Internet-is an important and challenging problem to solve.

Cisco IronPort Web Security Appliances enable organizations to take quick, easy steps to enforce common-sense data security policies for outbound traffic on HTTP, HTTPS, and FTP, as well as enabling simple interoperability with major dedicated DLP solutions.

- Mobile security across borderless networks—The Cisco AnyConnect Secure Mobility solution supports a wide range of desktops and mobile devices, helping ensure that web security continues to be enforced as employees change which devices they use. By using a standardized security solution for employees whether they are in the office or mobile, IT can also streamline security operations for a compelling TCO.
- SaaS access controls—The Cisco IronPort solution uses a standards-based authentication mechanism to bring sign-on under the control of your enterprise. Taking advantage of the employee credentials and access rights stored in the local directory, either Active Directory or LDAP, administrators retain control over access rights, and employees get a transparent experience using their corporate username and password for accessing all applications.
- Reporting visibility—The Cisco IronPort S-Series appliances deliver real-time and historical security information, allowing administrators to quickly understand web traffic activity. Real-time reports let administrators identify and track factors such as policy and security violations as they occur. Historical reports allow administrators to identify trends and report on efficacy and return on investment (ROI).
- Enterprise-scale performance—Cisco IronPort Web Security Appliances scale to meet the unique scanning needs of web traffic, thereby helping ensure that the employee's experience is maintained. Cisco offers industry-leading performance through its proprietary Cisco IronPort AsyncOS platform, an enterprise-grade web proxy and cache file system as well as an intelligent, multicore engine for rapid content scanning.

Consequently, the Cisco IronPort S-Series is a platform that can address the capacity requirements of even the largest of enterprises.

- Low TCO—Traditional solutions typically require multiple appliances or servers to protect against security, resource, and compliance risks. Unlike other solutions, the Cisco IronPort S-Series provides a single platform that contains a complete, in-depth defense-along with all the necessary management tools-significantly reducing initial and ongoing TCO.
- Reduced administrative overhead—Designed to minimize administrative overhead, Cisco IronPort Web Security Appliances offer easy setup and management with an intuitive GUI, support for automated updates, and comprehensive monitoring and alerting. The solution is also easy to deploy and configure to match corporate-specific policies.

Specifications

	S660	S360	S160
User Targets	10000+	1000-10000	< 1000
Chassis			
Form Factor	2RU	2RU	1RU
Dimensions	3.5" (h) x 17.5" (w) x 29.5" (d)	3.5" (h) x 17.5" (w) x 29.5" (d)	1.75" (h) x 17.5" (w) x 21.5" (d)
Power Supply	750 watts, 100/240 volts	750 watts, 100/240 volts	345 watts, 100/240 volts
Redundant Power Supply	Yes	Yes	No
Processor, Memory, and Disks			
CPUs	2x4 (2 Quad Cores) XEONs	1x4 (1 Quad Core) XEONs	2x2 (1 Dual Core) Pentium
Memory	8 GB	4 GB	4 GB
Disk Space	1.6 TB	1.2 TB	500 GB
Hot Swappable Hard Drives	Yes	Yes	No
RAID	RAID 10, battery-backed 256MB cache	RAID 10, battery-backed 256MB cache	RAID 1, battery-backed 256MB cache
Interfaces			
Ethernet	6xGigabit NICs, RJ-45	6xGigabit NICs, RJ-45	2xGigabit NICs, RJ-45
Serial	1xRS-232 (DB-9) Serial	1xRS-232 (DB-9) Serial	1xRS-232 (DB-9) Serial
Fiber	Optional	No	No
Configuration, Logging, and Monitoring			
Web Interface	GUI-based (HTTP or HTTPS)	GUI-based (HTTP or HTTPS)	GUI-based (HTTP or HTTPS)
Command Line Interface	SSH or Telnet (Configuration Wizard or command-based)	SSH or Telnet (Configuration Wizard or command-based)	SSH or Telnet (Configuration Wizard or command-based)
Logging	Squid, Apache, syslog	Squid, Apache, syslog	Squid, Apache, syslog
Centralized Reporting	Supported	Supported	Supported
File Transfer	SCP, FTP	SCP, FTP	SCP, FTP
Configuration Files	XML-based	XML-based	XML-based
Centralized Configuration	Supported	Supported	Supported
Monitoring	SNMPv1-3, e-mail alerts	SNMPv1-3, e-mail alerts	SNMPv1-3, e-mail alerts

Selected Part Numbers and Ordering Information

The following information pertains to Cisco IronPort bundle offerings. For a-la-carte, government, or educational pricing please contact a Cisco IronPort sales representative at sales@ironport.com.

Note: All bundles include Platinum Support, Rails (4-Post Square), and Sawmill Software for Cisco IronPort URL Filtering, Web Reputation Filters, and Anti-Malware System; the Cisco IronPort Anti-Malware System includes signatures from Webroot and McAfee.

Note the following abbreviations:

URL = URL Filtering; ASPY = Antispyware; WEBREP = Cisco IronPort Web Reputation Filters; AV = Antivirus and antimalware

Single Appliance Bundles (1 Year)		
URL	**URL+WREP**	**URL+WREP+ASPY+AV**
WBUN-1A-EN-A-1Y	WBUN-1A-EN-AB-1Y	WBUN-1A-EN-ABC-1Y
Single Appliance Bundles (3 Year)		
URL	**URL+WREP**	**URL+WREP+ASPY+AV**
WBUN-1A-EN-A-3Y	WBUN-1A-EN-AB-3Y	WBUN-1A-EN-ABC-3Y

Single Appliance Bundles (5 Year)		
URL	**URL+WREP**	**URL+WREP+ASPY+AV**
WBUN-1A-EN-A-5Y	WBUN-1A-EN-AB-5Y	WBUN-1A-EN-ABC-5Y
Dual Appliance Bundles (1 Year)		
URL	**URL+WREP**	**URL+WREP+ASPY+AV**
WBUN-2A-EN-A-1Y	WBUN-2A-EN-AB-1Y	WBUN-2A-EN-ABC-1Y
Dual Appliance Bundles (3 Year)		
URL	**URL+WREP**	**URL+WREP+ASPY+AV**
WBUN-2A-EN-A-3Y	WBUN-2A-EN-AB-3Y	WBUN-2A-EN-ABC-3Y
Dual Appliance Bundles (5 Year)		
URL	**URL+WREP**	**URL+WREP+ASPY+AV**
WBUN-2A-EN-A-5Y	WBUN-2A-EN-AB-5Y	WBUN-2A-EN-ABC-5Y

For More Information

http://www.cisco.com/web/products/ironport

Cisco IronPort M-Series Security Management Appliance

The Cisco IronPort M-Series Security Management Appliance complements all of the Cisco IronPort e-mail and web security appliances. By helping ensure top performance for all of your application security gateways, the Cisco IronPort M-Series provides one location for you to monitor all corporate policy settings and audit information. Designed and built as a flexible management tool to centralize and consolidate policy and runtime data, this product can provide a single management interface for all of your organization's Cisco IronPort security appliances. Optional features allow you to run all your security operations from a single appliance, or to spread the load across multiple appliances.

Ideal for Companies That Need These Features

Cisco IronPort M-Series Security Management Appliance

- Top performance from Cisco IronPort e-mail and web security appliances
- A central platform for managing all reporting and auditing information
- Comprehensive visibility into all e-mail traffic
- Flexible management and complete security control at the network gateway
- Deployment flexibility and management to protect corporate network integrity

Key Features and Benefits

- Each Cisco IronPort M-Series appliance can host one or more of the innovative security management features available from the Cisco IronPort appliance to ease administrator workload.
- The end-user quarantine is a self-service solution, with an easy-to-use web or e-mail-based interface and simple integration into existing directory and mail systems. All operations are automatic and self-managing, so there is no risk of a capacity overload. Most importantly, the Cisco IronPort Spam Quarantine requires no maintenance by the administrator or the end user.
- End users can be authenticated either through a corporate Lightweight Directory Access Protocol (LDAP) directory or with their regular e-mail password for any standards-based Internet Message Access Protocol (IMAP) or point-of-presence (POP) server. Message distribution lists can be managed through one-click authentication from the quarantine message digests.
- Centralized reporting allows for consolidation of traffic data from multiple e-mail security appliances to provide fully integrated security reporting.
- Cisco IronPort third-generation reporting technology provides comprehensive insight into even the highest-volume networks in the world. Detailed and accurate information is coalesced into clear and informative reports, suitable for all levels of your organization.
- Cross-application reporting provides insight into the threats being blocked from inside and outside your network, internal user behavior, and critical content security policy infractions [[is this what you mean? Otherwise, you're saying the reporting provides insight into ... policy]]. You can see which users are sending the most mail, and track policy infractions across any department, site, or communication medium.
- End-to-end communications auditing enables administrators to know where and when a communication took place. They can search message telemetry for multiple e-mail security appliances or request-response data from the web and report the full scanning and delivery details.
- The Cisco IronPort M-Series is a centralized policy and device management system that provides fine-grained role-based and hierarchical access to security and policy settings across hundreds of Cisco IronPort S-Series devices, improving security and reducing management overhead by allowing for delegation of critical policy decisions.
- You can use the Cisco IronPort M-Series appliance to manage quarantines, reporting data, and message tracking information—letting you dedicate your other appliances to mitigating e-mail and web security threats.
- All upgrades and new features are delivered directly from the Cisco IronPort appliance for your approval, and then automatically installed and managed.

Specifications

Chassis	IronPort M1060	IronPort M660	IronPort M160
Form Factor	19" rack-mountable 2RU rack height	19" rack-mountable 2RU rack height	19" rack-mountable 2RU rack height
Dimensions	3.5" (h) x 17.5" (w) x 29.5" (d)	3.5" (h) x 17.5" (w) x 29.5" (d)	1.75" (h) x 17.5" (w) x 21.5" (d)
Power Supply	750 watts, 100/240 volts	750 watts, 100/240 volts	345 watts, 100/240 volts
Processor, Memory, and Disks			
CPUs	2x4 (Quad Cores) Intel XEON	2x4 (Quad Core) Intel XEON	1x2 (Dual Core) Intel XEON
Disk Space	3 TB	1.8 TB	500 GB
RAID	RAID 10, battery-backed 256MB cache	RAID 10, battery-backed 256MB cache	RAID 1, battery-backed 256MB cache
Interfaces			
Ethernet	3xGigabit NICs, RJ-45	3xGigabit NICs, RJ-45	2xGigabit NICs, RJ-45
Fiber	Yes	No	No
Web Interface	GUI-based (HTTP or HTTPS)	GUI-based (HTTP or HTTPS)	GUI-based (HTTP or HTTPS)

Selected Part Numbers and Ordering Information

The following information pertains to Cisco IronPort bundle offerings. For a-la-carte, government, or educational pricing please contact a Cisco IronPort sales representative at sales@ironport.com.

Cisco IronPort Security Reporting Bundle

This bundle is for e-mail only.

- All new deals include a Cisco IronPort M160 Security Management Appliance
- All bundles include the following licenses for up to two E-mail Security Appliances
  - IronPort spam quarantine
  - Centralized e-mail reporting
  - Centralized message tracking
- All bundles include platinum support and rails (4-post square)
- For 5-year bundle contracts only—If IronPort, in its sole discretion, creates a new version or upgrade that is delivered to customer as part of the support and maintenance program and the software specifically licensed by the customer is incompatible with the IronPort hardware the customer uses to run the software, IronPort will upgrade the customer's incompatible hardware at no additional charge.

New Deals (1 Year)		
SKU	**ISQ + Reporting + Tracking**	**Users**
MBUN-1A-EN-ABC-1K-1Y	5000.00	100 to 999
MBUN-1A-EN-ABC-2K-1Y	11,675.00	1000 to 2000
New Deals (3 Years)		
SKU	**ISQ + Reporting + Tracking**	**Users**
MBUN-1A-EN-ABC-1K-3Y	9000.00	100 to 999
MBUN-1A-EN-ABC-2K-3Y	21,000.00	1000 to 2000
New Deals (3 Years)		
SKU	**ISQ + Reporting + Tracking**	**Users**
MBUN-1A-EN-ABC-1K-3Y	9000.00	100 to 999

Security Management Appliances	
M1050-BUN-R-NA	Cisco IronPort M1050, Standard Configuration
M650-BUN-R-NA	Cisco IronPort M650, Standard Configuration
M1060-BUN-R-NA	Cisco IronPort M1060, Standard Configuration
M660-BUN-R-NA	Cisco IronPort M660, Standard Configuration
M160-BUN-R-NA	Cisco IronPort M160, Standard Configuration
M1050-BUN-S-NA	Cisco IronPort M1050, Spare Unit (production unit required)
M650-BUN-S-NA	Cisco IronPort M650, Spare Unit (production unit required)
M1060-BUN-S-NA	Cisco IronPort M1060, Spare Unit (production unit required)
M660-BUN-S-NA	Cisco IronPort M660, Spare Unit (production unit required)

M160-BUN-S-NA	Cisco IronPort M160, Spare Unit (production unit required)
M1050-BUN-U-NA	Cisco IronPort M1050, Refurbished Unit
M650-BUN-U-NA	Cisco IronPort M650, Refurbished Unit

For More Information

http://www.cisco.com/en/US/products/ps10155/index.html

http://www.ironport.com/management

Cisco ACE Web Application Firewall

Many organizations are looking to increase efficiency and profitably with the implementation of new Web 2.0 applications and services. These new Web-based services provide greater flexibility and interactivity to customers, employees, and partners. At the same time, criminals have seized on exploiting these new, and often poorly secured services.

The Cisco ACE Web Application Firewall combines deep Web application analysis with high-performance Extensible Markup Language (XML) inspection and management to address the full range of threats. It secures and protects Web applications from common attacks such as identity theft, data theft, application disruption, fraud, and targeted attacks.

The Cisco ACE Web Application Firewall is especially designed to help organizations that store, process, and transmit credit card data comply with the current Payment Card Industry (PCI) Data Security Standard (DSS), requirements. Because of its unique blend of HTML and XML security, the Cisco ACE Web Application Firewall provides a full compliance solution for the PCI DSS sections 6.5 and 6.6, which mandate the implementation of a Web application firewall by June 30, 2008.

Key Features and Benefits

- PCI DSS regulation compliance
- Full-proxy security for both traditional HTML-based web applications and modern XML-enabled Web services applications
- Authentication and authorization enforcement to block unauthorized access
- Best-in-industry scalability and throughput for managing XML application traffic
- Positive and negative security enforcement to keep bad traffic patterns out and identify and allow only good traffic through
- Ability to deploy security policies and profiles in monitoring mode to prevent application downtime due to false positives typical in an automated learning environment
- Policy-based provisioning to increase developer productivity and improve deployment flexibility

Specifications

Feature	Cisco ACE Web Application Firewall
Transport Security	Full SSL v2/3 support with configurable cipher suites; FIPS 140-2 Level 3 platforms available
Cryptographic Support	Cryptographic algorithms including—Advanced Encryption Standard (AES); Data Encryption Standard (DES); Triple DES (3DES); Blowfish; RSA; Diffie-Helman; Digital Signature Algorithm (DSA); Secure Hash Algorithm 1 (SHA-1) and Message-Digest 5 (MD5)
Web Application Security	Full reverse proxy; Monitor mode deployment; Buffer overflow; HTTP parameter manipulation, Protocol compliance; Null byte blocking; Input encoding normalization; Response filtering and rewriting; Flexible firewall actions; Cookie and session tampering; Cross-site scripting (XSS); Command injection, SQL injection; Privacy enforcement by preventing information leak; Cryptography enforcement; Application and server error message cloaking; Referrer enforcement; Positive and negative security models; Custom rules and signatures; PCI compliance profiles
Administration	Web user interface; Command-line interface; SSH; Simple Network Management Protocol (SNMP); Roles-based access control (RBAC); Delegated administration; Central policy management and distributed enforcement; Import and export of configuration, statistics, and logs
Logging, Monitoring, and Auditing	Syslog and message and event logs; Traffic and service-level agreement (SLA) monitoring and reporting; Statistics for monitoring and various alerts and triggers; Audit trail of administrative operations

Selected Part Numbers and Ordering Information

Part Number	Product Name	Product Options	Support and Services
ACE-XML-K9 or ACE-XML-NF-K9	Cisco ACE Web Application Firewall Appliance	Chassis	CON-SNT-ACEXK9 or CON-SNT-ACEXNK9
ACE-XML-SW-6.0	Cisco ACE Web Application Firewall Software	Software	[Part: ACE-XML-SW-6.0]

ACE-XML-FIPS or ACE-XML-NONFIPS	FIPS-compliant SSL acceleration or Non-FIPS-compliant SSL acceleration	Cryptography	CON-SNT-ACEXFIPS or CON-SNT-ACEXNFIP
ACE-WAF-GAT-LICFX or ACE-WAF-MGT-LICFX	Cisco ACE Web Application Firewall license or Cisco ACE Web Application Firewall Manager license	Licensing	CON-SAU-ACEWGW or CON-SAU-ACEWMG

For More Information

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

Cisco IOS Content Filtering

Cisco IOS Content Filtering is a Web security solution that helps organizations protect against known and new Internet threats, improve employee productivity, and enforce business policies for regulatory compliance.

Cisco IOS Content Filtering is ideally suited for small medium businesses and enterprise branch offices that need a scalable, low-maintenance solution.

As employees surf the internet, they expose themselves to websites that are known to give out malware, adware, spyware, and phishing. This not only causes downtime, but also revenue losses. According to an Infonetics Research (2006), nearly 2 percent of revenue losses and 51 percent of downtime costs are due to security costs.

Deployed on Cisco integrated services routers, Cisco IOS Content Filtering offers category-based productivity and security ratings. Content-aware security ratings protect against malware, malicious code, phishing attacks, and spyware. URL and keyword blocking help to ensure that employees are productive when accessing the Internet. This is a subscription-based hosted solution that leverages Trend Micro's global TrendLabs threat database, and is closely integrated with Cisco IOS.

Ideal for Companies That Need These Features

Cisco IOS Content Filtering

- Improved employee productivity—Restrict Internet use that exposes your organization to Internet risks and prevent employees from surfing Websites that lead to productivity loss or legal liability
- Conserve network resources—Set security policies that limit Internet access to prevent download of bandwidth-intensive applications and malware that would consume network resources
- Ease of Use—Simplify registration, configuration, and category management

Key Features and Benefits

- Subscription-Based—Easy-to-renew 1-, 2-, or 3-year subscription-based service is associated to the router platform; no individual user licenses are required. Subscription provides access to Trend Micro's database, with content filtering policies set on the router.
- Reputation Security-Ratings—Protection against a variety of web-based threats, including zero-day attacks. Assesses the security risk posed by a Web site based on our risk analysis. Helps combat phishing and guards against spyware that may send confidential information to hackers and cybercriminals. The reputation security Rating for a given URL based on a combination of past behavior and current exposure to malware, adware, phishing, spyware, and hacking provides the utmost level of web security for your network.
- Category-Based URL Classification (Over 70+ Categories Available)—Content-based classification of URLs helps restrict access to objectionable or productivity-affecting Websites (sites focusing on gambling or weapons, for example). Categories for reputation-based blocking (spyware and keylogging, for example) are also available.
- Keyword Blocking—Cisco IOS Content Filtering allows blocking of Websites based on selected keywords that occur in the URL.
- Black and White List Support—Cisco IOS Content Filtering supports 100 black and 1000 white URLs. For example, trusted Websites can be added to a white list.
- Management Provisioning—Cisco IOS Content Filtering is easy to use and deploy. It is managed through Cisco Configuration Professional, a Web-based router management tool, and through CSM (Cisco Security Manager)
- Caching—The caching feature stores URL categories and their policy decisions (permit or deny) locally on the router, ensuring quick response time to access the Internet. Administrators can configure the cache duration on the router.

Selected Part Numbers and Ordering Information

SL-CNFIL-87x-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 871, 876, 878, 878 Routers (URL/Phishing)
SL-CNFIL-88x-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 881, 886, 887,888 Routers (URL/Phishing)
SL-CNFIL-89x-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 891, 892 Routers (URL/Phishing)
SL-CNFIL-8xx-TRI	30-day free trial license for Cisco 800 Series
SL-CNFIL-180X-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 1801,1802,1803 Routers (URL/Phishing)

SL-CNFIL-181X-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 1811,1812 Routers (URL/Phishing)
SL-CNFIL-184-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 1841 Routers (URL/Phishing)
SL-CNFIL-186-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 1861 Routers (URL/Phishing)
SL-CNFIL-1xxx-TRI	30-day free trial license for Cisco 1800/1900 Series
SL-CNFIL-280-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 2801 Routers (URL/Phishing)
SL-CNFIL-281-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 2811 Routers (URL/Phishing)
SL-CNFIL-282-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 2821 Routers (URL/Phishing)
SL-CNFIL-285-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 2851 Routers (URL/Phishing)
SL-CNFIL-2xxx-TRI	30-day free trial license for Cisco 2800/2900 Series
SL-CNFIL-382-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 3825 Routers (URL/Phishing)
SL-CNFIL-384-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 3845 Routers (URL/Phishing)
FL-19-CNFIL-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 1900 Routers (URL/Phishing)
FL-29-CNFIL-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 2900 Routers (URL/Phishing)
FL-39-CNFIL-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 3900 Routers (URL/Phishing)
SL-CNFIL-3xxx-TRI	30-day free trial license for Cisco 3800/3900 Series

For More Information

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

Cisco Spam and Virus Blocker

The Cisco Spam and Virus Blocker is a dedicated antispam, antivirus, and antiphishing security appliance designed specifically for small businesses which virtually eliminates e-mail threats right out of the box. It helps blocks spam, requires minimal administration, and connects to one of the largest databases of e-mail security threats to bolster its accuracy.

Ideal for Companies That Need These Features

Cisco Spam and Virus Blocker

- Protect your business against dangerous e-mail threats
- Improve the productivity of your employees by eliminating spam
- Reduce the time spent managing spam and e-mail threat security
- Increase the performance of your network, servers, and personal computers by getting rid of unwanted e-mail
- Reduce your liability for a spam or virus attack that is unintentionally propagated through your network

Key Features and Benefits

- Precision accuracy—Helps ensure that e-mail threats and spam are caught, and business e-mail is delivered.
- Continuous automatic updates—Constant communication with SenderBase services, a network database of e-mail security threats, ensures that your Cisco Spam and Virus Blocker installs the latest updates to protect your business e-mail.
- Easy installation and use—Simple browser-based setup wizards allow you to install Cisco Spam and Virus Blocker in nearly any network within 15 minutes, providing protection for your business right out of the box.
- Effortless management—From the moment the appliance is installed, you get spam protection with no additional effort from you or your staff.

Specifications

Feature	Cisco Spam and Virus Blocker
Hard drive	2x 80 GB 2.5-in. 7.2k Serial ATA (SATA)
CPU	Intel Celeron 440
Connectivity	Ethernet; dual embedded Gigabit network interface cards (NICs)
Memory	2 GB
Reliability and availability	Mean time between failures (MTBF): 74,000 hours
Network management	Accessible via HTTP and HTTPS; command-line interface accessible via SSH and Telnet
Network (or programming or other) interfaces	Accessible via HTTP and HTTPS; command-line interface accessible via SSH and Telnet

Protocols	· DNS · SSL/Transport Layer Security (TLS) · Network Address Translation (NAT) port mapping · Simple Mail Transfer Protocol (SMTP) · HTTP, HTTPS · FTP · Simple Network Management Protocol (SNMP) · Network Time Protocol (NTP) · Secure Shell (SSH) · Lightweight Directory Access Protocol (LDAP) · Remote Procedure Call (RPC) · Telnet · TCP/IP
Language support	GUI: English, French, Italian, German, Spanish, Chinese (Simplified and Mandarin), Japanese, Korean, Portuguese, Russian
(HxWxD)	1U rack: 16.1-in. depth
Weight: 14.6 lb (without rails)	Power
345W	Temperature range
Operating temperature: 50° to 95°F (10° to 35°C)	Storage temperature: -40° to 149°F (-40° to 65°C)
Mail server compatibility	Integrates with all mail servers (Exchange, Notes, Domino, etc.)

Selected Part Numbers and Ordering Information

BLKR-SVB-50U-1Y	Cisco Spam & Virus Blocker-50 users, 1 year
BLKR-SVB-50U-3Y	Cisco Spam & Virus Blocker-50 users, 3 years
BLKR-SVB-100U-1Y	Cisco Spam & Virus Blocker-100 users, 1 year
BLKR-SVB-100U-3Y	Cisco Spam & Virus Blocker-100 users, 3 years
BLKR-SVB-250U-1Y	Cisco Spam & Virus Blocker-250 users, 1 year
BLKR-SVB-250U-3Y	Cisco Spam & Virus Blocker-250 users, 3 years

For More Information

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

Cisco ScanSafe Web Security

ScanSafe Web Security is powered by Outbreak Intelligence™ which is comprised of numerous correlated detection technologies, automated machine-learning heuristics, and multiple "scanlets". Outbreak Intelligence builds a detailed view of each Web request and the associated security risk to ensure that ScanSafe customers use the Web safely.

Outbreak Intelligence scans over 1 billion Web requests a day, in real-time, stopping millions of malware instances and protecting thousands of the most demanding organizations around the world. Outbreak Intelligence scanlets analyze all elements of a Web request including HTML, JavaScript, Flash and active scripts, among others, which when coupled with numerous Context scanlets, offers multiple indicators as to the security posture of each Web request.

Ideal for Companies That Need These Features

Cisco ScanSafe Web Security	· Proactive, in-the-cloud protection against zero-day threats · Prevent malware that is attempting to steal confidential data · Protect against malware communication leaving the network · Easily identify infected machines on your network · Reduce time and resources used to remediate infected machines

Key Features and Benefits

- In-depth security analysis of all Web content as it is requested by end users
- High performance, secure Web access enabled by a global, multi-tenant infrastructure
- Powered by Outbreak Intelligence that is proven to block over 20% more malware than traditional security techniques
- Granular reporting to determine and resolve users that are infected by malware or are at risk

For More Information

http://www.scansafe.com/security

Cisco ScanSafe Web Filtering

ScanSafe Web Filtering offers granular control over all Web content, including SSL encrypted communications, utilizing multiple techniques including real-time dynamic Web content classification, an industry-leading URL filtering database, file type filters and early warning filtering and real-time scanning of search results with Search*Ahead*.

Enabled in-the-cloud, ScanSafe Web Filtering enables businesses to implement granular control for both inbound and outbound communications while realizing cost savings of up to 40% by eliminating the need to purchase, deploy and maintain hardware required for on-premise solutions. ScanSafe Web Filtering allows businesses to be in complete control of how end users access content on the Internet by providing intuitive tools to create, monitor, and enforce effective inbound and outbound Web policy.

ScanSafe Web Filtering is managed through an intuitive Web-based interface, ScanCenter, which integrates all management and reporting capabilities. Through ScanCenter, a global Web usage policy can be created and enforced across the organization, even down the group or user level. Any edits to the policy are rolled out in real time without having to wait for policy changes to propagate throughout the network.

Ideal for Companies That Need These Features

Cisco ScanSafe Web Filtering

- Limit legal liability by controlling access to inappropriate Web content
- Optimize network resources by reducing bandwidth consumption
- Enhance productivity by limiting non-business related Web activity
- Limit exposure to financial and other penalties related to the loss of confidential data
- Understand and control how your network resources are being used

Key Features and Benefits

- Control all Web-based traffic including SSL encrypted communications
- Prevent confidential data from leaving the network
- Ensure safe search engine results
- Granular reporting on all aspects of Web usage

For More Information

http://www.scansafe.com/webfiltering

Cisco ScanSafe Anywhere+

Anywhere+ extends the real-time protection and policy enforcement of ScanSafe Web Security to roaming employees. With Anywhere+ it is finally possible to protect roaming employees wherever they are working and however they access the Internet.

Anywhere+ is delivered as a service for complete security, reduced complexity and simplified user management. Anywhere+ removes the performance issues and bandwidth congestion associated with backhauling Web traffic over the corporate VPN, so the security perimeter is now anywhere you want it to be.

Anywhere+ is deployed through a lightweight, tamper-proof driver which forwards Web traffic to the ScanSafe security scanning infrastructure. ScanSafe data centers are located all over the world from San Francisco to Sydney ensuring that end-users always have optimized performance as well as award-winning security and filtering.

Ideal for Companies That Need These Features

Cisco ScanSafe Anywhere+

- Ensure consistent security policy for all end-users, including remote and roaming workers
- Eliminate cost and effort of backhauling traffic from small offices and remote workers
- Optimized, high performance service regardless of geographical location
- Avoid users circumventing control with a tamper-proof solution
- Enforce global policy changes in real time

Key Features and Benefits

- Complete integration into defined global security policy
- Automatically selects optimal ScanSafe data center
- “Last mile” encryption ensures security of data sent to ScanSafe data center
- Supports centralized, silent deployment

For More Information

http://www.scansafe.com/anywhereplus

Cisco AnyConnect Secure Mobility Solution

With Cisco AnyConnect Secure Mobility Solution, users can access the network with their mobile device of choice, including laptops and handhelds. At the same time, this solution helps your organization easily manage the security risks of borderless networks.

This mobile security solution provides:

- Security policy enforcement that is context-aware, comprehensive, and preemptive
- Connectivity that is intelligent, simple, and always on
- Highly secure mobility across the rapidly increasing number of managed and unmanaged mobile devices

The Cisco AnyConnect Secure Mobility solution consists of the following components:

- Cisco AnyConnect Secure Mobility Client for highly secure connectivity
- Cisco IronPort Web Security Appliance for security policy enforcement
- Cisco AnyConnect Secure Mobility Solution enables the connection to simply work and be persistently connected, without the user needing to juggle where and how to best connect and persist, even when roaming between networks.
- The Cisco IronPort S-Series Web Security Appliance applies context-aware policy, including enforcing acceptable use and protection from malware for all users. The Web Security Appliance also accepts user authentication information from the AnyConnect client, providing an automatic authentication step for the user to access their web content.
- Cisco ASA Series as the firewall and secure mobility headend Cisco AnyConnect Version 2.5, with Cisco ASA 5500 Series Adaptive Security Appliances at the headend, provides the remote-access connectivity portion of Cisco AnyConnect Secure Mobility.

Ideal for Companies That Need These Features

Cisco AnyConnect Secure Mobility Solution	For end users, Cisco AnyConnect Secure Mobility provides: • A connectivity experience that is intelligent, seamless and always-on • Secure mobility across today's proliferating managed and unmanaged mobile devices For security administrators, Cisco AnyConnect Secure Mobility provides: • Security policy enforcement that is context-aware, comprehensive and preemptive • Reduced operating costs with a simplified IT operations for all end users • Improved customer satisfaction by providing flexibility and choice for end users For company executives, Cisco AnyConnect Secure Mobility provides: • Ability to boost productivity by enabling mobile access from any device without compromising security • Provide the end users choice of how, when, and where to access their information

Key Features and Benefits

- Security policy enforcement that is context-aware, comprehensive and preemptive
- A connectivity experience that is intelligent, seamless and always-on
- Secure mobility across today's proliferating managed and unmanaged mobile devices

Specifications

Specifications for the AnyConnect Secure Mobility Client. For the ASA and IronPort S-Series please see other sections

Pre-connection Posture Assessment (Premium license required)	• In conjunction with Cisco Secure Desktop, Host Scan verification checking seeks to detect the presence of antivirus software, personal firewall software, and Windows service packs on the endpoint system prior to granting network access. • Administrators also have the option of defining custom posture checks based on the presence of running processes. • Cisco Secure Desktop can detect the presence of a watermark on a remote system. The watermark can be used to identify assets that are corporate-owned and provide differentiated access as a result. The watermark checking capability includes system registry values, file existence matching a required CRC32 checksum, IP address range matching, and certificate issued by/to matching. • An advanced endpoint assessment option is available to automate the process of repairing out-of-compliance applications.
Advanced IP Network Connectivity	• Access to internal IPv4 and IPv6 network resources • Centralized split tunneling control for optimized network access IP address assignment mechanisms: • Static • Internal pool • Dynamic Host Configuration Protocol (DHCP) • RADIUS/LDAP
Client Firewall Policy	• New in AnyConnect 2.5 • Added protection for Split Tunneling configurations. • Used in conjunction with Cisco Secure Mobility to allow for local access exceptions (i.e. printing, tethered device support, etc). • Supports port-based rules for IPv4 and network/IP Access Control Lists (ACLs) for IPv6. • Available for Windows XP SP2, Vista, Windows 7 & Mac OS X
AnyConnect Profile Editor	• New in AnyConnect 2.5 & Adaptive Security Appliance 8.3 • AnyConnect policies may be customized directly from Cisco ASDM (Adaptive Security Device Manager).

For More Information

http://www.cisco.com/en/US/netsol/ns1049/index.html

Cisco 3350 Mobility Services Engine

The Cisco 3300 Series Mobility Services Engine is an open platform that provides a new approach for the delivery of mobility services to enable mobile business applications. A combination of hardware and software, the Mobility Services Engine is an appliance-based solution that supports a suite of software services to provide centralized and scalable service delivery. The Mobility Services Engine transforms the wireless LAN into a mobility network by abstracting the application layer from the network layer, effectively allowing for the delivery of mobile applications across different types of networks, including Wi-Fi, Ethernet, cellular, and RFID.

The Cisco 3300 Series Mobility Services Engine provides an open API that allows a broader ecosystem of partners to access network intelligence in developing industry-relevant mobility solutions. The Mobility Services Engine is an extension of the Cisco Unified Wireless Network, and integrates with Cisco Unified Communications and Cisco compatible devices to deliver a comprehensive approach to business mobility-an approach that extends applications to the right device at the right time, no matter which network is being used.

Key Features and Benefits

- Simplifies provisioning and management of mobility services
- Offers scalable and reliable multidevice, multinetwork application delivery
- Facilitates a broad partner ecosystem for mobile applications development
- As a component of the Cisco Unified Wireless Network, supports lightweight access points
- Integrates with the Cisco Unified Wireless Network, including the Cisco Wireless Control System, for a single mobility management solution

The Cisco 3350 Mobility Services Engine transforms existing WLANs into comprehensive mobility networks through a uniform method of mobility services delivery.

The Cisco 3350 Mobility Services Engine software suite includes:

- Cisco Context-Aware Software to track up to 18,000 devices
- Cisco Mobile Intelligent Roaming for up to 2000 simultaneous devices
- Cisco Adaptive Wireless Intrusion Prevention System (IPS) Software

Specifications

Feature	Cisco 3310	Cisco 3350
Supported Services	• Context-aware software to track up to 2000 devices • Adaptive Wireless Intrusion Prevention System software to support up to 2000 monitor mode access points	• Context-aware software to track up to 18,000 devices • Adaptive Wireless Intrusion Prevention System software to support up to 3000 monitor mode access points.
Evaluation Support	• Customers who purchase a mobility service have the option to trial other mobility services on their MSE at the following scale: • Context-aware client tracking: 100 Clients • Context-aware tag tracking: 100 Tags • Adaptive Wireless Intrusion Prevention: 20 monitor mode access points	
Processor	(1) Dual-Core Intel Processor 1.8 GHz	(2) Quad-Core Intel Xeon Processors 2.33 GHz
Memory	4-GB PC2-5300 (4 x 1 GB)	8-GB PC2-5300 (4 x 2 GB)
Hard Disk	(2) Fixed 247-GB Serial ATA-150 / SATA-300 MBps	(2) Hot-swappable 137-GB SAS-300 MBps drives
Connectivity	Network: Two embedded Multifunction Gigabit Network Adapters	Network: Two embedded Multifunction Gigabit Network Adapters with TCP/IP Offload Engine
Management	SNMP v1, v2c, and v3	SNMP v1, v2c, and v3
Management Interface	Cisco WCS Mobility Services v.5.2 or greater running Internet Explorer 6.0/Service Pack 1 or later	Cisco WCS Mobility Services v.5.2 or greater running Internet Explorer 6.0/Service Pack 1 or later
Network Devices	Cisco 2100, 4400 & 5500 Series Wireless LAN Controllers; Cisco Catalyst 6500 Series Wireless Services Module, Cisco Catalyst 3750G Integrated Wireless LAN Controller, Cisco Wireless LAN Controller Module (WLCM and WLCM-E) for Integrated Services Routers; Cisco Aironet® lightweight access points	Cisco 2100, 4400 & 5500 Series Wireless LAN Controllers; Cisco Catalyst 6500 Series Wireless Services Module, Cisco Catalyst 3750G Integrated Wireless LAN Controller, Cisco Wireless LAN Controller Module (WLCM and WLCM-E) for Integrated Services Routers; Cisco Aironet lightweight access points
Programming Interfaces	SOAP/XML APIs	SOAP/XML APIs
Form Factor	• 1.70 in. x 16.78 in. x 20 in. (4.32 cm x 42.62 cm x 50.8 cm) • 15 lbs (6.8 kg) maximum	• 1.70 in. x 16.78 in. x 27.25 in. (4.32 cm x 42.62 cm x 69.22 cm) • 39.5 lbs (17.92 kg) maximum

Power	· AC power supply wattage: 540W · AC power supply voltage: 100-120V at 50-60 Hz; 200-240V at 50-60 Hz	· AC power supply wattage: 852W · AC power supply voltage: 100-120V at 50-60 Hz; 200-240V at 50-60 Hz · Redundant Power Supplies
Software Compatibility	· Available with Cisco Mobility Services Engine (MSE) Software Release 5.2 or later · Requires WLC software version 4.2.130 or later and Wireless Control System (WCS) Version 5.2 or later · Multiple mobility services can run concurrently on the same MSE using WLC and MSE Software Release 6.0 or later · Supported services may have different software requirements	· Available with Cisco Mobility Services Engine (MSE) Software Release 5.1 or later · Requires WLC software Version 4.2.130 or later and WCS Version 5.1 or later · Multiple mobility services can run concurrently on the same MSE using WLC and MSE Software Release 6.0 or later · Supported services may have different software requirements

Selected Part Numbers and Ordering Information

AIR-MSE-3350-K9	Cisco 3350 Series Mobility Services Engine
AIR-MSE-3310-K9	Cisco 3310 Series Mobility Services Engine

For More Information

http://www.cisco.com/en/US/products/ps9777/index.html

Cisco Catalyst 6500 Series/7600 Series WebVPN Services Module

The Cisco WebVPN Services Module is a high-speed, integrated Secure Sockets Layer (SSL) VPN services module for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers that addresses the scalability, performance, application support, and security required for large-scale, remote-access SSL VPN deployments. Supporting up to 32,000 SSL VPN users and 128,000 connections per chassis, the Cisco WebVPN Services Module can cost-effectively meet the capacity requirements of large enterprises. The unique virtualization capabilities integrated into the module simplify the policy creation and enforcement for diverse enterprise user communities and make it an ideal solution for managed service providers. Taking advantage of the broad, industry-proven application support and endpoint security provided by Cisco VPN 3000 Series concentrators, the Cisco WebVPN Services Module is ideally suited to meet the secure connectivity demands of any organization.

Ideal for Companies That Need These Features

Cisco Catalyst 6500 Series/ 7600 Series WebVPN Services Module	· Ability to add a high-speed, integrated SSL VPN services module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series routers

Key Features and Benefits

- Integration with network infrastructure—Incorporating VPN into the Cisco Catalyst 6500 Series switches and Cisco 7600 Series Internet routers helps secure the network without the need for extra overlay equipment or network alterations.
- Virtualization and VRF awareness—Virtualization technology is a way to pool resources while masking the physical attributes and boundaries of the resources from the resource users. Up to 128 virtual routing and forwarding (VRF)-aware virtual contexts are supported per module.
- Advanced endpoint security—A primary component of the Cisco WebVPN Services Module, Cisco Secure Desktop offers preconnection security posture assessment and a consistent and reliable means of eliminating all traces of sensitive data.
- Scalability—A single module is capable of supporting up to 8000 simultaneous users and up to 32,000 concurrent connections. Up to four modules can be supported in a single chassis to support up to 32,000 simultaneous SSL VPN users and 128,000 connections.
- Ease of deployment—The Cisco WebVPN Services Module comes with integrated device manager support. This helps configure and provision the module without the need for an external element management system, providing a ready-to-deploy solution.

Specifications

Feature	Cisco Catalyst 6500 Series/7600 Series WebVPN Services Module
Scalability	· Up to 8000 users · Up to 300 Mbps · Up to 64 SSL VPN virtual contexts and 64 gateways · Up to 4 modules in a chassis
Virtualization	Ability to divide into multiple contexts, with each context as a complete logical representation of the WebVPN Services Module, complete with separate policies and configuration

VRF-Aware	· VRF mapping · Single-IP model (URL-based or login-name-based) · Multiple-IP model · Per-VRF AAA server · Per-VRF DNS server · Per-VRF gateway · Per-VRF number of users
User Authentication	· RADIUS · Windows NT, Active Directory, UNIX NIS · Group-based access control using Cisco Secure Access Control Server (ACS)
End-System Integrity (Cisco Secure Desktop integration)	· Antivirus check · Personal firewall check · Seeks to minimize risk of temporary and downloaded files and cookies from remaining on system
Redundancy and Load Sharing	· Stateless failover · Cisco IOS® Software server-load balancing (SLB) and Content Switching Module integration within the chassis · Active/Active failover
Application Support	Web access, file services, e-mail, Telnet, file transfer, legacy applications, specialized applications
Browser Support	Netscape, Internet Explorer, Firefox
Protocols	SSL 3.0 and 3.1; TLS 1.0
Configuration and Management	Console CLI, HTTP, HTTPS, Telnet, Secure Shell (SSH)
Syslog Support	Console display, external server, internal buffer
Cipher Suites	· SSL_RSA_WITH_RC4_128_MD5 · SSL_RSA_WITH_RC4_128_SHA · SSL_RSA_WITH_DES_CSC_SHA · SSL_RSA_WITH_3DES_EDE_CBC_SHA
Network Access Control	IP address, Differentiated Services Code Point/Type of Service (DSCP/ToS), TCP/UDP port, per-user, per-group

Selected Part Numbers and Ordering Information

WS-SVC-WEBVPN-K9	WebVPN Services Module for Cisco Catalyst 6500 Series and Cisco 7600 Series
WS-SVC-WEBVPN-K9=	WebVPN Services Module (spare)
SC-SVC-WVPN-1.1-K9	WebVPN Services Module Software 1.1
SC-SVC-WVPN-1.1-K9=	WebVPN Services Module Software 1.1 (spare)
FR-SVC-WVPN-5000	Cisco Catalyst 6500 and Cisco 7600 WebVPN 5000 user license
FR-SVC-WVPN-8000	Cisco Catalyst 6500 and Cisco 7600 WebVPN 8000 user license

For More Information

http://www.cisco.com/en/US/products/ps6404/index.html

Cisco Security Agent

Businesses are under intense pressure to protect their IT assets from attacks that are increasing in frequency and sophistication. At the same time they need to address stringent compliance requirements and minimize expenses and complexity.

Cisco Security Agent 6.0.2 is the first endpoint security solution that combines zero update attack defense, policy driven data loss prevention, and signature based anti-virus detection into a single agent. This unique blend of capabilities defends servers and desktops against sophisticated zero-day attacks and enforces acceptable-use and compliance policies within a simplified management infrastructure.

Ideal for Companies That Need These Features

Cisco Security Agent	· Zero-update protection to prevent brand new exploits, targeted attacks · Continuously defends critical servers that cannot be taken offline to patch · Identification and control of sensitive data · Regulatory-compliance auditing and control · Enhanced visibility into threats in the network · Automatic, no-cost antivirus signature updates · Always-on protection, even when not connected to the corporate network · Lower total cost of ownership

Key Features and Benefits

- Provides industry-leading protection against day zero exploits for laptops, desktops, servers, and POS devices.
- Provides visibility and control of sensitive data across all endpoints; protecting against data loss from both end-user actions and targeted malware.
- Access to sensitive files is audited; policy controls can be implemented to stop malicious data transfers to removable media or through insecure network applications
- Imposes restrictions for wireless and remote users (i.e. cannot copy sensitive information to removable media while off the corporate network).
- Provides behavioral-based protection from known and unknown threats.
- Zero-update protection is critical when addressing brand new exploits or variants that take advantage of published/unpublished system and application vulnerabilities.
- Offers network collaboration that strengthens the security posture of the organization.
- Offers comprehensive management, visibility, and reporting.
- Critical endpoint component of the Cisco Secure Borderless Network architecture

For More Information

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

Cisco Virtual Office

Remote worker solutions from Cisco boost flexibility and productivity and extend the enterprise by delivering secure, rich, and manageable network services to teleworkers and employees working outside the traditional office environment. By providing full IP phone, wireless, data, and video services, Cisco Virtual Office provides a smooth, office-caliber experience to staff, wherever they may be located.

The Cisco Virtual Office solution consists of the following components:

- A remote-site presence with a Cisco 800 Series Integrated Services Router and a Cisco Unified IP Phone 7900 Series phone.
- Headend presence remote-site aggregation includes a VPN router and centralized management software for policy, configuration, and identity controls. Cisco and approved partners provide deployment and ongoing services for successful deployment and integration as well as consultative guidance for automating the deployment.

Deployment Options

Cisco Virtual Office includes provisioning and management through numerous management tools that provide the ability to define network-wide policy, use identity for authorization, and actively update configurations at remote sites.

Cisco Virtual Office Express refers to a simplified architecture to address initial installation steps. It extends the same network services available through the Cisco Virtual Office solution but is distinct in its ability to quickly set up the secured connections between sites. Cisco Virtual Office Express has a reduced number of management and headend components to provide rich functions while keeping operating costs low.

Solution Benefits

The Cisco Virtual Office solution addresses many of the requirements associated with remote working for both end users and organizations alike. In doing so, it also provides benefits across three distinct organizational groups:

- For end users—Cisco Virtual Office allows schedule flexibility and improves work/life balance by providing the ability to work at home or on the road. The solution also provides integrated family support with multiple Service Set Identifiers (SSIDs) for wireless and separate VLANs for a secure "split-tunneling."
- For IT groups—Cisco Virtual Office simplifies the process of extending real-time, high-performance network services to remote locations. These services are delivered without any compromise to the overall security policy. Traffic is protected through VPN technologies, and authorization to access corporate resources is managed through strict identity controls. This solution also provides architecture for centralized, simplified management and operations, and contributes to improved scalability security and low total cost of ownership. For example, Cisco IT effectively supports more than 15,000 Cisco Virtual Office deployments with just a handful of resources. This support is particularly important because users at these locations have heightened expectations for the delivery of virtual office services, and these locations typically do not have IT staff for onsite support. For an even simpler deployment model, Cisco Virtual Office Express comprises a single, integrated device that results in initial cost savings as well as investment protection in the form of the scalability and modularity of the routers as business needs expand. With only one management solution to learn, training needs are minimized and ongoing operations are simplified.
- For businesses and organizations—This solution improves productivity of the workforce while saving costs associated with energy, facilities, and real estate. It also enables better business resiliency, allowing the workforce to stay secure and connected if employees cannot get to the office or are traveling.

A Differentiated Solution

Teleworkers and technology that enables teleworking has existed for many years, but the solutions in the past have typically lacked a critical component, creating a barrier to adoption. Perhaps the solution is not robust enough to handle communication and collaboration applications. Perhaps it lacks the proper security controls to comply with corporate standards. Or perhaps it does not use unified communications or wireless technologies, making it less convenient. Cisco Virtual Office delivers a truly comprehensive solution that addresses each of these concerns, providing mutual benefits to the end user, the IT department—and ultimately—the business.

For More Information

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

Cisco Security Manager

Cisco Security Manager is an enterprise-class management application that provides insight into and control of Cisco security and network devices. Cisco Security Manager offers comprehensive security management (configuration and event management) across a wide range of Cisco security appliances, including Cisco ASA Adaptive Security Appliances, Intrusion Prevention System (IPS) Sensor Appliances, Integrated Services Routers, Firewall Services Modules, and Cisco Catalyst 6000 Series Switches. Cisco Security Manager allows you to efficiently manage networks of all sizes-from small networks to large networks consisting of hundreds of devices.

Cisco Threat Defense

Cisco threat defense helps organizations secure and manage their borderless network environment. Organizations are protected from today's dynamic threat environment using proactive intelligence from Cisco Security Intelligence Operations (SIO), market-leading network security devices, and a single, integrated management platform.

Simplified Security Management

- Next-generation Cisco Security Manager enables organizations to gain insight and control of the entire security topology through a single, integrated user interface, including:
  - Global policies for Cisco ASA and IPS Appliances
  - Single console for configuration and device changes
- Next-generation Cisco Security Manager increases visibility into security environment so that you can better understand and respond to threat patterns and risk. Features include:
  - Single view of Cisco IPS with Cisco Global Threat Correlation engine and ASA-thwarted events
  - Single view of traffic statistics
  - Drill-down capabilities
  - Integration of reputation data into IPS events
  - Dynamic policy tuning based on actionable events
- Cisco IPS with the Cisco Global Threat Correlation engine reduces the time needed to manage IPS by providing more accurate detection and automated rule sets
- Support for event-to-policy linkages and cross-launching
- Integrated troubleshooting tools such as Cisco Packet Tracer and the traceroute command
- Detection of out-of-band changes and selective ASA policy management for heterogeneous operational IT environments
- Simplified policy definition paradigms for ASA appliances (providing Network Address Translation [NAT] services) and Global Access Rules for improved management efficiency
- Enhanced support for Cisco's latest intrusion protection system (IPS) and firewall features, such as Botnet Traffic Filter and the Global Threat Correlation engine, for an improved threat response experience

For More Information

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

Cisco Security Monitoring, Analysis, and Response System (MARS)

Cisco Security Monitoring, Analysis and Response System (MARS) is a family of high-performance, scalable appliances for threat management, monitoring, and mitigation that enable customers to make more effective use of network and security devices by combining traditional security event monitoring with network intelligence, context correlation, vector analysis, anomaly detection, hotspot identification, and automated mitigation capabilities. By combining network intelligence, an understanding of network topology, and automated mitigation capabilities, Cisco Security MARS helps companies accurately identify and eliminate network attacks while maintaining network compliance.

Ideal for Companies That Need These Features

Cisco Security MARS 25; Cisco Security MARS 25R	• Low-end device to plot network topology and gain insight into network topology • Ideal for small offices, test labs, departments, small retail establishments, DMZs, and CPE
Cisco Security MARS 55	• Consolidation of firewall and intrusion detection system (IDS) with network events and network flows in a small network • Ideal for small to medium-sized offices, remote branch offices, retail establishments, small businesses, DMZs, and CPE
Cisco Security MARS 110	• Ideal for second-generation appliances for large offices and CPE
Cisco Security MARS 110R	• Ideal for large enterprises, central offices, and large firewalls
Cisco Security MARS 210	• Ideal for second-generation appliances for large enterprises, central offices, and large firewalls (FWSMs)
Cisco Security MARS GC; Cisco Security MARS GC2	• Ideal for large distributed environments and multiservice switching platforms (MSSPs). • Useful for autonomous business units that are rolling activities to global teams and for state and federal governments for consolidating activities from various agencies

Key Features and Benefits

- Centralized monitoring—Cisco Security MARS provides detailed information about the network infrastructure, including routers, switches, firewalls, VPN concentrators, and endpoint devices, through a variety of device logs, alerts, and NetFlow communication. It also provides process threat information down to the IP and MAC address, nearest attached switch port, as well as the attack path through the network.
- Central event repository—The central event repository serves as a central repository for all events generated by security devices, such as firewalls, authentication servers, network intrusion prevention systems (IPSs) and intrusion detection systems (IDSs) and proxy servers. All collected events are cross-correlated in real time.
- Data reduction—Cisco Security MARS can reduce millions of security events to a handful of actual reported network incidents.
- Timely attack mitigation—Built-in expertise recognizes and recommends mitigation for attacks before they can bring down an entire network.
- End-to-end network awareness—The application integrates Network Address Translation (NAT), Port Address Translation (PAT), and MAC address information to identify attackers, targets, and network hotspots in graphical form for quick action. It uses the full configurations of all types of network devices and end systems. Pre- and post-NAT addresses can be displayed.
- Integrated vulnerability assessment—This solution determines whether a possible network attack is genuine or a false positive, reducing the number of alarms and the time needed to take action.
- Reduced deployment and operation cost—Cisco Security MARS discovers and then maps the topology of a network and becomes operational in a very short period of time.
- Standard 802.1x support—The application facilitates authentication of a host connecting to the switch port before obtaining an IP address.
- Cisco Distributed Threat Mitigation (DTM) and CICS support—This collaborative solution proactively identifies the most active signatures from the IPS appliance deployed in the network and, based on the most active threats detected on the network, distributes the same IPS signatures to the user-defined Cisco IOS IPS devices.
- Case management—Administrators can escalate an incident by creating a case and forwarding the case with notes to other users and security administrators.
- NetFlow analysis—Cisco IOS NetFlow data is collected and analyzed by Cisco Security MARS, at speeds as high as 300,000 flows per second.

Specifications

Feature	CS-MARS-25R-K9	CS-MARS-25-K9	CS-MARS-55-K9	CS-MARS-110-K9
Storage	120 GB (non-RAID)	120 GB (non-RAID)	240 GB RAID 0	1500 GB RAID 10 Hot-swappable
Form Factor	1RU x 16	1RU x 16	1RU x 25.6	2RU x 27 3/4" (D); 3.44" (H); 19" (W)
Power Supply	300W, 120/240V autoswitch	300W, 120/240V autoswitch	300W, 120/240V autoswitch	2 x 750W dual-redundant 120/240V autoswitch
Performance				
Events/sec.	50	500	1000	7500
Netflows/ sec.	1500	15,000	30,000	150,000
Feature	**CS-MARS-210-K9**	**CS-MAR-GC-K9**	**CS-MARS-GC2-K9**	
Storage	2000 TB RAID 10 Hot-swappable	1 TB RAID 10 Hot-swappable	2 TB RAID 10 Hot-swappable	
Form Factor	2 RU x 27 3/4" (D); 3.44" (H); 19" (W)	4RU x 25.6	2 RU x 27 3/4" (D); 3.44" (H); 19" (W)	
Power Supply	2 x 750W dual-redundant 120/240V autoswitch	500W dual-redundant 120/240V autoswitch	2 x 750W dual-redundant 120/240V autoswitch	
Events/sec.	15,000			
Netflows/ sec.	300,000			
Maximum Connections		Not restricted	Not restricted	

Selected Part Numbers and Ordering Information

Cisco SMARTnet Service Part Number		
CS-MARS-25R-K9	CON-SNT-MARS25R	Cisco Security MARS 25R
CSMARS-25-K9	CON-SNT-MARS25	Cisco Security MARS 25
CSMARS-55-K9	CON-SNT-MARS55	Cisco Security MARS 55

CSMARS-110R-K9	CON-SNT-MARS110R	Cisco Security MARS 110R
CSMARS-110-K9	CON-SNT-MARS110	Cisco Security MARS 110
CSMARS-210-K9	CON-SNT-MARS210	Cisco Security MARS 210
CSMARS-GC2R-K9	CON-SNT-MARSGC2R	Cisco Security MARS GC2R
CSMARS-GC2-K9	CON-SNT-MARSGC2	Cisco Security MARS GC2

For More Information

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

Cisco Physical Access Gateway

An integral component of the Cisco Physical Access Control solution, the Cisco Physical Access Gateway is the primary module used to connect door hardware (readers, locks, etc.) to the IP network. The gateway can connect to a maximum of two doors and associated inputs and outputs.

The Cisco Physical Access Gateway is a mandatory component of any access-control deployment. The following optional modules may be connected to the Cisco Physical Access Gateway to control additional doors, inputs, and outputs:

- Cisco Physical Access Gateway Reader Module
- Cisco Physical Access Gateway Input Module
- Cisco Physical Access Gateway Output Module

Key Features and Benefits

- Manage up to two doors
- Additional module support
- Reader and lock power
- Credential cache
- Event cache
- Encryption

Specifications

Feature	Cisco Physical Access Gateway			
Housing	Aluminum			
Dimensions (LxWxH)	5 x 7 x 2.14 in. 127 x 178 x 54.6 mm			
Weight	Without Plugs and Brackets	With Plugs	With Brackets	With Plugs and Brackets
	1.65 lb (749 g)	1.8 lb (817 g)	1.81 lb (823 g)	1.97 lb (891 g)
Certifications	FCC UL CE			
Operating Temperature	Indoors only 32 to 122ûF (0 to 50ûC)			
Humidity	5 to 95% relative, non-condensing			
Power	There are two options to power the device: 12 to 24 VDC (+/- 10%) through an external power supply 802.3AF-compliant Power over Ethernet (PoE) connected to the Ethernet 0 connector			

Selected Part Numbers and Ordering Information

The Cisco Physical Access Gateway is available through Cisco Authorized Technology Provider (ATP)

CIAC-GW-K9	Cisco Physical Access Gateway

For More Information

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

Cisco Physical Access Manager

Cisco Physical Access Manager (Version 1.2) is the management application for the Cisco Physical Access Control solution. It comes installed on hardware, and is sold as an appliance. This application is used to configure Cisco Physical Access Gateways and Modules, monitor activity, enroll users, and integrate with IT applications and data stores.

Key Features and Benefits

- Thin clients—Cisco Physical Access Manager supports a thin-client model. Clients from computers running the Windows operating system can contact Cisco Physical Access Manager and download and install an application that allows interaction with the Cisco Physical Access Manager for administrative purposes.
- Microsoft Active Directory integration—You can configure administrative users of Cisco Physical Access Manager to use Microsoft Active Directory for authentication.
- Badging and enrollment—An optional licensable module enables the creation of badge templates, badge printing, taking user photographs, and enrolling users into the Cisco Physical Access Manager user database.
- Device configuration—You can configure Cisco Physical Access Gateway hardware using Cisco Physical Access Manager. The access gateway contacts Cisco Physical Access Manager, to download pre-provisioned configuration information.
- Access policies—You can assign areas (comprising a group of doors) and users entry permission based on schedules.
- User rights —You can assign permissions to administrative users of the Cisco Physical Access Manager and you can tailor user profiles very specifically.
- Credential management—You can edit cardholder credentials, including system wide card formats.
- Alarm and event management—Cisco Physical Access Manager provides a view of events and alarms in the system. You can filter alarm and event views based on several criteria.
- Global I/O—You can associate events (contact closure inputs or card access denied, for example) to actions (activate output contact closures, send an e-mail message, etc.).
- Reporting—You can create standard and custom reports with Cisco Physical Access Manager.
- Audit trails—Cisco Physical Access Manager provides a log of all administrative uses of the system, arranged by user.
- Enterprise application integration—An optional licensable component allows Cisco Physical Access Manager to be synchronized with data from either external SQL databases or Microsoft Active Directory.
- Cisco Video Surveillance Manager integration—Cisco Physical Access Manager dynamically acquires camera inventory from Cisco Video Surveillance Manager and associates cameras to doors; you can view recorded or live video for every event from the door.
- License management—You can add license files (capacity upgrades or feature additions) to the application.
- Server administration—You can administer the Cisco Physical Access Manager appliance by performing tasks such as IP address assignment.
- Access gateway image management—You can upgrade Cisco Physical Access Gateway images using the Cisco Physical Access Manager.
- Configuration backup—You can back up the entire configuration to an external server.
- System restore—You can restore previously backed up configuration from an external server.
- High availability—You can configure two Cisco Physical Access Manager appliances as a pair to provide warm standby redundancy; you must install the secondary appliance with a high-availability license.
- URL Invocation—HPPT/S URLs can be invoked as a result of any event or alarm. Event data can be inserted in the URL to integrate with any external application that accepts URL invocations.
- Web Services API—A licensable option allows for external systems to use a Web Services API to integrate with CPAM. Both HTTP and SOAP/XML bindings are supported.

Specifications

The following table lists the hardware specifications of the Appliance on which Cisco Physical Access Manager Version 1.1 is installed.

CPU	Intel Core2 Duo 2.13-GHz processor with a 1066-MHz front side bus (FSB) and 2 MB of Level 2 cache
Memory	4 GB PC2-5300 DDR2 SDRAM ECC
Hard Drive	250 GB SATA 7200 RPM
Ethernet	2 X 10/100/1000 RJ-45, 10BASE-T, 100BASE-TX, 1000BASE-T
Weight	15.0 lb (6.8 kg), base chassis
Maximum Power Consumption	350W (maximum output, power supply rating) 540W (maximum input, power supply rating)

Selected Part Numbers and Ordering Information

The Cisco Physical Access Manager is available through Cisco Authorized Technology Provider (ATP) Partners.

CIAC-PAME-1125-K9	Appliance, bundled with Cisco Physical Access Manager Version 1.0 Software
CIAC-PAME-BD=	Cisco Physical Access Manager Badge Designer and Enroller
CIAC-PAME-HA=	Cisco Physical Access Manager High-Availability License
CIAC-PAME-M64=	Cisco Physical Access Manager 64-module capacity upgrade license
CIAC-PAME-M128=	Cisco Physical Access Manager 128-module capacity upgrade license
CIAC-PAME-M512=	Cisco Physical Access Manager 512-module capacity upgrade license
CIAC-PAME-M1024=	Cisco Physical Access Manager 1024-module capacity upgrade license
CIAC-PAME-EDI=	Cisco Physical Access Manager Enterprise Data Integration License
CIAC-PAME-WSAPI=	Cisco Physical Access Manager Web Services API License

For More Information

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

Cisco Video Surveillance 2500 Series IP Cameras

The Cisco Video Surveillance 2500 Series IP Cameras are high-resolution, feature-rich digital cameras designed for superior performance in a wide variety of video surveillance applications. The cameras employ MPEG-4 and MPEG compression to stream 30 frames per second (fps) at D1 NTSC resolution (720 x 480) or 25 fps at D1 PAL resolution (720 x 576), offering efficient network usage while providing high-quality video. Contact closures and two-way audio allow integration with microphones, speakers, and access control systems. (Note: Not all features are supported when using the camera with Cisco Video Surveillance Manager.) With their open, standards-based design, the cameras provide an ideal platform for integration and operation as independent devices or as part of a Cisco Video Surveillance network.

Key Features and Benefits

- Wide dynamic range—The cameras employ powerful digital imaging technology, allowing them to capture high-quality images in a wide variety lighting conditions. They use a progressive scan image sensor with global electronic shuttering to ensure natural color rendition, zero blooming and smear, and minimal motion blurring.
- Dual streaming—The camera can stream MPEG-4 and MJPEG video simultaneously. Each video stream can be configured with individual resolution, quality, and frame rate settings.
- Day/night operation—The camera provides true day/night functionality that includes an IR filter that automatically switches to night mode in low light scenes. This function can be set to manual or automatic control.
- Flexible power options—The cameras support Power over Ethernet (PoE) 802.3af or DC power through an optional external power supply.
- Wireless capabilities—The wireless IP camera model supports 1 x 2 multiple input multiple output (MIMO) communication, which provides better data throughput and higher link range than single-antenna designs. The wireless IP camera offers strong wireless security using Wi-Fi Protected Access (WPA)/WPA2 and supports various network protocols for 802.1x authentication.
- Embedded security and networking—The camera provides 802.1X authentication and hardware-based Advanced Encryption Standard (AES). For enhanced bandwidth management, the camera supports IP Multicast.
- Event notification—The camera can examine designated areas in the video for motion activity and then notify users or other applications when it detects activity that exceeds a predefined threshold. The camera also provides two digital inputs and two digital outputs that can be used to initiate specific actions when an alarm is detected.
- Mounting options—The camera can be installed with a fixed mount or with an optional external pan/tilt mount and motorized zoom lens.

Specifications

Feature	Cisco Video Surveillance 2500 Series IP Cameras
Imaging Device	1/3-in. progressive-scan CMOS with wide dynamic range
Image Control	Automatic white balance (AWB), automatic back lighting, automatic gain control (AGC), automatic exposure (AE), auto-manual iris
Dynamic Range	102 dB typical/120 dB maximum
Minimum Illumination	Color mode: F1.4 @ 0.65 lux Black and white mode: F1.4 @ 0.08 lux
Signal-to-Noise Ratio (SNR)	>48 dB
Lens Selection	Accepts manual or DC auto iris lens
Video Compression	MPEG-4 SP level 0 to 4, ASP level 0 to 5

Audio Compression*	G.711 A-Law, G.711 U-Law, G.726
Resolution and Frame Rate	NTSC/PAL 720 x 480/576 @ 30/25 fps (D1) 704 x 480/576 @ 30/25 fps (4CIF) 352 x 240/288 @ 30/25 fps (CIF)
Video Streaming	· Single-stream MPEG-4 up to D1 720 x 480/576 @ 30/25 fps · Single-stream MJPEG up to D1 720 x 480/576 @ 15 fps · Dual-stream: MPEG-4 and MJPEG · Primary stream MPEG-4 programmable up to 704 x 480/576 @ 25/20 fps · Secondary stream MPEG-4/MJPEG (selectable) programmable up to 352 x 240/288 @ up to 15 fps
Protocols	Dynamic Host Control Protocol (DHCP), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Secure HTTP (HTTPS), Network Time Protocol (NTP), Real-Time Transport Protocol (RTP), Real-Time Streaming Protocol (RTSP), Simple Mail Transfer Protocol (SMTP), Secure Sockets Layer/ Transport Layer Security (SSL/TLS), Transmission Control Protocol/Internet Protocol (TCP/IP)
Housing	Aluminum
LEDs	Power, Ethernet link, and activity
Dimensions	4.8 x 3.1 x 2 in. (122 x 80 x 50 mm)
Weight	1.15 lb (0.52 kg)
Certifications	· FCC, CE, and UL · Emission: 47 CFR Part 15: 2007, CISPR22: Edition 5, EN55022: Edition 5, EN61000-3-2: 2006, · EN61000-3-3: 1995 [Incamd 1 & 2], ICES-003 Issue 4: 2004, KN 22: 2008, VCCI: V-3/2007.04, Immunity: CISPR24: 1997 [Incamd 1 & 2], EN55024: 1998 [Incamd 1 & 2], EN61000-6-1: 2007
Operating Temperature	Indoors: 32 to 122°F (0 to 50°C) Outdoors (when installed in an appropriate outdoor enclosure with heating and cooling): –40 to 158°F (–40 to 70°C)

Selected Part Numbers and Ordering Information

The Cisco Video Surveillance 2500 Series IP Camera is available through Cisco Authorized Technology Provider (ATP) Partners.

CIVS-IPC-2500	Cisco 2500 IP Camera, full resolution, day/night
CIVS-IPC-2500W	Cisco 2500 IP Camera, full resolution, day/night, wireless
CIVS-PWRPAC-12V	Cisco VS external dual voltage power supply for encode/decode

For More Information

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

Cisco Video Surveillance 4000 Series High-Definition IP Cameras

Cisco Video Surveillance 4000 Series IP Cameras are feature-rich digital cameras designed for superior performance in a wide variety of video surveillance applications. The cameras employ true high-definition (HD) video and H.264 compression, streaming up to 30 frames per second (fps) at 1080p (1920 x 1080) resolution, and 60 fps at 720p (1280 x 720) resolution, offering efficient network usage with the highest-quality video. Contact closures and two-way audio allow integration with microphones, speakers, and access control systems. With their open, standards-based design, the cameras provide an ideal platform for integration and operation as independent devices or as part of a Cisco Video Surveillance network.

The Cisco Video Surveillance 4300 Series and 4500 Series IP Cameras (CIVS-IPC-4300 and CIVS-IPC-4500) have identical feature sets, with the exception of the additional digital signal processor (DSP) capabilities specifically designed to support real-time video analytics at the edge on the Cisco Video Surveillance 4500 Series IP Cameras. On these cameras, applications and end users have the option to run multiple analytics packages without compromising video streaming performance on the cameras. This highly flexible computing platform that will be compatible with future versions is ideal for next-generation video analytics applications.

Key Features and Benefits

- True high-definition (HD) video—The cameras stream crisp and clear 1080p (1920 x 1080) video at 30 frames per second while maintaining surprisingly low network bandwidth. For fast-motion applications, you can set the cameras to stream 720p (1280 x 720) video at 60 frames per second.
- Progressive scan video—The cameras capture each frame at its entire resolution using progressive scan rather than interfaced video capture, which captures each field of video. This feature allows for better detail for video of moving objects such as faces and license plates on automobiles.
- Dual streaming—The camera can stream H.264 and MJPEG video simultaneously. Each video stream can be configured with individual resolution, quality, and frame rate settings.
- Day and night operation—The cameras provide true day and night functions including an automatic infrared (IR) filter in low-light scenes. With the appropriate IR-corrected lenses and IR illumination, the cameras can provide HD video in low-light environments.

- Flexible power options—The cameras support Power over Ethernet (PoE) 802.3af, 12-VDC, or 24-VAC power through an optional external power supply.
- Mounting options—You can install the cameras with a fixed mount or with an optional external pan or tilt mount and motorized zoom lens.*
- Embedded security and networking*—The camera provides hardware-based Advanced Encryption Standard (AES). For enhanced bandwidth management, the camera supports IP Multicast.
- Event notification*—The camera can examine designated areas for activity and notify users or other applications when it detects activity that exceeds a predefined sensitivity and threshold. The camera also provides two digital inputs and two digital outputs that can be used to initiate specific actions when an alarm is detected.
- Optional USB memory card*—The camera supports an optional USB memory card for onboard storage of video and other data.

  Note: Features with an asterisk are not available when the camera is used with Cisco Video Surveillance Manager

Specifications

Feature	Cisco Video Surveillance 4000 Series IP Cameras
Imaging Device	1/3-in. progressive-scan RGB CMOS
Image Control	Automatic white balance (AWB), automatic gain control (AGC), automatic exposure (AE), and auto/manual iris
Dynamic Range	65 dB
Minimum Illumination	Color mode: F1.4 @ 0.4 lux Black and white mode: F1.4 @ 0.02 lux
Signal-to-Noise Ratio (SNR)	53 dB
Lens Selection	Accepts manual or DC auto iris lens
Video Compression	H.264, MJPEG
Audio Compression*	G.711 A-Law, G.711 U-Law, AAC
Resolution and Frame Rate H.264	1920 x 1080 @ 30 fps (1080p) 1280 x 720 @ 60 fps (720p) 720 x 480/576 @ 30/25 fps (D1) 704 x 480/576 @ 30/25 fps (4CIF) 352 x 240/288 @ 30/25 fps (CIF)
Resolution and Frame Rate MJPEG	720 x 480/576 @ 30/25 fps (D1) 704 x 480/576 @ 30/25 fps (4CIF) 352 x 240/288 @ 30/25 fps (CIF)
Protocols	Dynamic Host Control Protocol (DHCP), Hypertext Transfer Protocol (HTTP), Secure HTTP (HTTPS), Network Time Protocol (NTP), Real-Time Transport Protocol (RTP), Real-Time Streaming Protocol (RTSP), Simple Mail Transfer Protocol (SMTP), Secure Sockets Layer/ Transport Layer Security (SSL/TLS), Transmission Control Protocol/Internet Protocol (TCP/IP), Secure Real-time Transport Protocol (SRTP), Cisco Discovery Protocol, Bonjour, Simple Network Management Protocol (SNMP), and Secure Shell (SSH)
Housing	Aluminum
LEDs	Power, Ethernet link, and activity
Dimensions	5.2 x 3.1 x 2.5 in. 135 x 79.5 x 65 mm
Weight	1.2 lb 0.54 kg
Certifications	FCC, CE, and UL
Operating Temperature	Indoors: 32 to 122°F (0 to 50°C) Outdoors (when installed in an appropriate outdoor enclosure with heating and cooling): –40 to 158°F (–40 to 70°C)

Selected Part Numbers and Ordering Information

The Cisco 4000 Series Video Surveillance IP Camera is available through Cisco Authorized Technology Provider (ATP) Partners.

CIVS-IPC-4300	Cisco Video Surveillance 4300 IP Camera, HD, Day/Night
CIVS-IPC-4500	Cisco Video Surveillance 4500 IP Camera, HD, DSP, Day/Night
CIVS-PWRPAC-12V	12 VDC @ 1.6A Power Supply

For More Information

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

Cisco Video Surveillance 2000 Series IP Domes

The Cisco Video Surveillance 2000 Series IP Domes are high-resolution, feature-rich digital IP cameras that you can deploy in a wide variety of environments. The cameras use MPEG-4 compression of up to 30 frames per second (fps) at D1 NTSC resolution (720 x 480) or 25 fps at D1 PAL resolution (720 x 576), for efficient network usage and high-quality video. They also support MJPEG compression.

The Cisco Video Surveillance 2500 and 2400 IP Dome models include the same core technology as the 2500 Series IP Cameras. IP Dome 2530V is a vandal-resistant, ruggedized, outdoor camera for difficult environments with high or low temperatures, moisture, or dust. IP Dome 2520V is a vandal-resistant indoor camera for schools, railway platforms, or other public areas. IP Dome 2421 is an indoor-only, ceiling tile mount camera for retail and common office deployment.

Key Features and Benefits

- Wide dynamic range—The camera employs powerful digital imaging technology, allowing it to capture high-quality images in a wide variety of lighting conditions. It uses a progressive scan image sensor with global electronic shuttering to ensure natural color rendition, zero blooming and smear, and minimal motion blurring.
- Dual streaming—The camera can stream MPEG-4 and MJPEG video simultaneously. You can configure each video stream with individual resolution, quality, and frame-rate settings.
- Flexible power options—The camera supports Power over Ethernet (PoE) 802.3af and 12-VDC or 24-VAC power through an optional external power supply.
- Day or night operation—The camera provides true day or night operation and includes an infrared (IR) filter that automatically switches to night mode in low-light scenes. You can set this function to manual or automatic control.
- Cisco Media Application Programming Interface (API)—The camera supports the Cisco Media API, an open, standards-based interface that allows integration with compatible video surveillance management systems
- Embedded security and networking—The camera provides 802.1X authentication and hardware-based Advanced Encryption Standard (AES). For enhanced bandwidth management, the camera supports IP Multicast.

Specifications

Feature	Cisco 2421 Series IP Domes	Cisco 2520 Series IP Domes	Cisco Video Surveillance 2530 Series
Housing	Metal base and polycarbonate transparent cover	Metal base and polycarbonate transparent cover with tamper-resistant mounting	Metal base and polycarbonate transparent cover with tamper-resistant mounting IP-66 rated
LEDs	Power and Ethernet	Power and Ethernet	Power and Ethernet
Dimensions (WxH)	6.64 x 4.36 in. /169 x 111 mm	6.1 x 4.64 in. /155 x 118 mm	6.1 x 4.64 in. /155 x 118 mm
Weight	1.0 kg	1.4 kg	1.4 kg
Operating temperature	32 to 122° F 0 to 50° C	32 to 122° F 0 to 50° C	–30 to 55° C / –22 to 131° F

Selected Part Numbers and Ordering Information

CIVS-IPC-2530V	Indoor/outdoor Cisco standard-definition IP clear dome, D/N, 2.8-10 mm, vandal resistant
CIVS-IPC-2531V	Indoor/outdoor Cisco standard-definition IP smoked dome, D/N, 2.8-10 mm, vandal resistant
CIVS-IPC-2520V	Cisco standard-definition IP clear dome, D/N, 2.8–10 mm, vandal resistant
CIVS-IPC-2521V	Cisco standard-definition IP clear dome, D/N, 2.8–10 mm, vandal resistant
CIVS-IPC-2421	Indoor dome, smoked, lens 2.8–10 mm

For More Information

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

Cisco Video Surveillance Stream Manager Software

The Cisco Video Surveillance Stream Manager application is a collection of discrete software modules that provide advanced and flexible configuration, management, and operation of video surveillance networks and solutions. With intuitive GUIs and comprehensive features, Cisco Video Surveillance Stream Manager Software modules function as an integrated platform for security systems and enable true convergence of closed circuit television (CCTV) and the enterprise LAN. Stream manager applications provide digital video, audio, and serial data management across any IP network.

Cisco Video Surveillance Stream Manager Software modules combine the capabilities of many standalone hardware and software systems into one product, including features provided by digital video recorders, matrix

switching systems, video multiplexers, and transmission systems. These system functions are available wherever and whenever there is network connectivity. Whether used in an enterprise network or a small or medium-sized business, the stream manager provides a managed distributed digital video system.

- The Cisco Video Surveillance Stream Manager Configuration Module identifies and programs Cisco Video Surveillance IP Gateway encoders, decoders, and storage devices.
- The Cisco Video Surveillance Stream Manager Administration and Monitoring Module enables monitoring of network, server use, and dynamic system health, and provides status reporting.
- The Cisco Video Surveillance Stream Manager Administration and Monitoring with Failover Module provides all the features of the Administration and Monitoring Module, with the addition of failover management.
- The Cisco Video Surveillance Stream Manager Client Viewing Module provides access to all system operations, including camera control, stored video review, and alarm notifications. This application is the primary PC application for viewing live or stored video from the network.
- The Cisco Video Surveillance Stream Manager Upgrade Module (included in the Cisco Video Surveillance Stream Manager Configuration Module) upgrades firmware in video surveillance hardware.

Key Features and Benefits

- All-in-one video management solution
- User-friendly setup and operation
- IP virtual matrix switch functions
- Complete and secure video storage management
- Distributed processing on Cisco Video Surveillance devices, eliminating the need for a centralized server
- Activity detection and search
- Export video with authentication capabilities
- Advanced network visibility
- Sophisticated playback features, including trick replay functions

Specifications

Feature	Client Viewing Module	All Other Modules
CPU	Pentium dual-core, 2.8 GHz	Pentium IV, 2.8 GHz
RAM	1 GB	512 MB
Hard Drive	40 GB	40 GB
Audio Card	Optional, for listening to audio provided by an encoder	Optional, for listening to system alerts
Video Card	ATI X1600XT 512MB PCI-e or NVIDIA E-GEFORCE 7600GT CO 256MB DDR PCI-e	Standard PC video card
Network Card	10BASE-T, 100BASE-T, 1000BASE-T	10BASE-T, 100BASE-T, 1000BASE-T
Operating System	Microsoft Windows XP Pro with Service Pack 2 or Microsoft Windows Vista Business with Service Pack 1 (supported in Stream Manager 5.3	Microsoft Windows XP Pro with Service Pack 2 or Microsoft Windows Vista Business with Service Pack 1 (supported in Stream Manager 5.3
Web Services	Microsoft Net 2.0	Microsoft Net 2.0

Selected Part Numbers and Ordering Information

CIVS-SM-CFG50=	Cisco Video Surveillance Stream Manager Configuration Module
CIVS-SM-CL50=	Cisco Video Surveillance Stream Manager Client Viewing Module
CIVS-SM-AS50=	Cisco Video Surveillance Stream Manager Administration and Monitoring Module
CIVS-SM-ASF50=	Cisco Video Surveillance Stream Manager Administration and Monitoring with Failover Module

For More Information

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

Cisco Video Surveillance Media Server Software

Cisco offers network-centric video surveillance software and hardware that supports video transmission, monitoring, recording, and management. Cisco Video Surveillance solutions work with the advanced features and functions of the IP network infrastructure—switches, routers, and other network security devices—to enable secure, policy-based access to live or recorded video. With support for many surveillance cameras, encoders, and applications, Cisco Video Surveillance solutions allow you to build high-quality video surveillance systems that optimize cost, performance, and capability.

The core component of the Cisco Video Surveillance Manager, Cisco Video Surveillance Media Server 6.0 performs the following networked video surveillance system functions:

- Collection and routing of video from a wide range of cameras and encoders over an IP network
- Secure local, remote, and redundant video archiving
- Event tagging for review and archival purposes
- Bandwidth management for both live distribution and historical recording

Cisco Video Surveillance Media Server is fully compatible with other Cisco Video Surveillance Manager applications that provide video display control and distribution (virtual matrix switching), a customizable web-based user interface for roles-based operation and management, system configuration, and options to support storage area networks (SANs) and network- and direct-attached storage (NAS and DAS). The media server and other Cisco Video Surveillance software applications run on Linux-based servers. As a result, you can upgrade your investment to include new features, address your evolving requirements, and support a diverse range of deployment scenarios.

Key Features and Benefits

By using the power and advanced capabilities of IP networks, Cisco Video Surveillance Media Server Software allows you to add applications, users, cameras, and storage over time. As a result, the software provides exceptional video surveillance system flexibility and scalability to support:

- Deployments that range from small systems to those with thousands of cameras
- Hundreds of simultaneous users accessing live and recorded video
- Standard video codecs such as Motion JPEG, MPEG-2, MPEG-4, and H.264 simultaneously in a single Cisco Video Surveillance Media Server
- Conservation of storage using events, clipping, record-on-motion, and loop-based archival options
- Integration with other security and IT applications using open, standards-based API and Real-Time Transport Protocol (RTP) and Real-Time Streaming Protocol (RTSP) streaming
- IT-caliber, fault-tolerant storage for greater efficiency and easier maintenance

Specifications

The following table lists the minimum system requirements for server and client hardware for Media Server.

Feature	Server System	Client System
CPU	3-GHz Intel Pentium 4	3-GHz Intel Pentium 4
RAM	1 GB	1 GB
Hard Drive	200-GB hard drive	-
Video Card	-	nVidia or ATI AGP graphics adapter with 128 MB RAM
Network Connection	10/100 Ethernet Interface	10/100 Ethernet adapter
Operating System	SUSE Linux Enterprise Server (SLES) version 9 SP 3 or version 10 SP 1 (recommended)	Windows XP and Internet Explorer 6 or 7
Rack Space	1 to 5 RU	-

Selected Part Numbers and Ordering Information

CIVS-MS-SW6.0=	Cisco Video Surveillance Media Server 6.0

For More Information

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

Cisco Video Surveillance Operations Manager Software

Cisco offers network-centric video surveillance software and hardware that supports video transmission, monitoring, recording, and management. Cisco Video Surveillance solutions work with the advanced features and functions of the IP network infrastructure—switches, routers, and other network security devices—to enable secure, policy-based access to live or recorded video. With support for many third-party video surveillance cameras, encoders, and applications, Cisco Video Surveillance solutions allow you to build high-quality video surveillance systems that optimize cost, performance, and capability.

Cisco Video Surveillance Operations Manager is a component of the Cisco Video Surveillance Manager suite of products. It enables the efficient and effective configuration and management of video throughout an enterprise. It provides a secure web portal to configure, manage, display, and control video in an IP network, and provides the ability to easily manage a large number of security assets and users, including Cisco Video Surveillance Media Server instances, cameras, encoders, DVRs, and event sources, as well as digital monitors that are powered by Cisco Video Surveillance Virtual Matrix.

Key Features and Benefits

- Offers superior price and performance for managing video surveillance deployments of any size
- Runs on commercial off-the-shelf (COTS) Linux-based servers, making it easier to upgrade to include new features, address your evolving requirements, and support a diverse range of deployment scenarios
- Offers customizable interface for operators and administrators
- Provides multitiered hierarchy of user roles and privileges

- Provides open license with no built-in limits on numbers of users or resources managed and no per-seat costs
- Is compatible with most popular web browsers
- Is compatible with the Cisco Video Surveillance Manager Platform, allowing many choices for cameras, encoders, and related devices, and allowing systems to expand over time

Specifications

The table below lists the minimum system requirements for Operations manager and client hardware.

Feature	Server System	Client System
CPU	3-GHz Intel Pentium 4	3-GHz Intel Pentium 4
RAM	1 GB	1 GB
Hard Drive	200-GB hard drive	-
Video Card	-	nVidia or ATI AGP graphics adapter with 128 MB RAM
Network Connection	10/100 Ethernet Interface	10/100 Ethernet adapter
Operating System	SUSE Linux Enterprise Server (SLES) version 9 SP 3 or version 10 SP 1 (recommended)	Windows XP and Internet Explorer 6 or 7
Rack Space	1 to 5 RU	-

Selected Part Numbers and Ordering Information

CIVS-OM-SW4.0=	Cisco Video Surveillance Operations Manager 4.0

For More Information

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

Cisco Physical Security Multiservices Platform

The Cisco Physical Security Multiservices Platform offers you innovative choices for deploying and managing physical security services, including video surveillance, access control, and flexible incident response communications. It includes a wide array of features in an easy-to-use, and easy-to-deploy server suite.

Cisco physical security multiservices platform software application options are as follows (this platform supports only one software application option at a time):

- Video Surveillance Manager (1-RU)
  - Video Surveillance Manager version 4.2.1/6.2.1
  - 1 × CIVS-HDD-1000-1 TB SATA hard-disk drives in JBOD-like configuration with ~874 GB storage or 4 × CIVS-HDD-1000-1 TB SATA hard-disk drives in RAID-5 configuration with ~2.6 TB storage

  Supports one of the following option cards at a time:
  - 1 × CIVS-FC-1P-Fibre Channel card
  - 1 × CIVS-ES-16EC-16-channel encoder card for MPEG-4/JPEG (at CIF resolution)
- Physical access control (1-RU)
  - Cisco Physical Access Manager version 1.2
  - 1 × CIVS-HDD-1000-1 TB SATA hard-disk drive
- IPICS (1-RU) and 2-RU)
  - Cisco IPICS version 4.0 ready (download required)
  - 2 × CIVS-HDD-1000-1 TB SATA hard-disk drives in RAID-1 mirroring configuration with ~437 GB storage available

Key Features and Benefits

- Built-in 300W high-efficiency power supply in 1-RU
- 900 W high-efficiency power supply with hot-swappable, redundancy option in 2-RU
- High-performance fans with built-in redundancy for optimized cooling
- System health and management features, including redundant cooling fans, a convenient power switch, reset button, and LED indicators
- Optional hot-swappable hard-disk drives that can be removed without powering down the server (must have Redundant Array of Independent Disks [RAID] configuration to be hot-swappable)
- High storage density
- System resiliency
- Hardware diagnostics
- High-performing motherboard

Specifications

1 RU Mechanical Specifications	
Housing	1RU x 19 in., 4 x SATA front-loading drive bays
Motherboard	Intel E5502 1.86 GHz Xeon Dual-Core CPU, 4 GB DDR3 RAM
LEDs	Power, hard-drive activity, network activity, system overheat/fan fail
Weight	• 24.5 lbs. (11.1 kg), 4 x 1 TB hard-disk drives and 1 x power supply • 18.5 lbs. (8.4 kg), with power supply, no HDDs, and no cards
Dimension	1.7 in. (43 mm) x 17.2 in. (437mm) x 19.8 in. (503 mm)
Power Supply	300 W
Power Requirements (no option cards)	110V/60Hz: Spinup Surge: 175 W, Steady-State: 128 W 220V/60Hz: Spinup Surge: 222 W, Steady-State: 143 W
Operating Temperature	50° to 95° F (10° to 35° C)
2 RU Mechanical Specifications	
Housing	2RU x 19 in., 12 x SATA front-loading drive bays
Motherboard	Intel E5502 2.26 GHz Xeon Dual-Core CPU, 4 GB DDR3 RAM
LEDs	Power, hard-drive activity, network activity, system overheat/fan fail
Weight	• 42.5 lbs. (19.3 kg), 6 x 1 TB hard-disk drives and 2 x power supply • 27.5 lbs. (12.5 kg), no power supply, no HDDs, and no cards
Dimension	3.5 in. (89 mm) x 17.2 in. (437 mm) x 25.5 in. (648 mm)
Power Supply	1 x 900 W internal power supply
Power Requirements (no option cards)	110 V/60 Hz: Spin-up surge: 395 W, Steady-state: 274 W 220 V/60 Hz: Spin-up surge: 480 W, Steady-state: 284 W
Operating Temperature	50° to 95° F (10° to 35° C)

Selected Part Numbers and Ordering Information

The Multiservices Platform is available through Cisco Authorized Technology Provider (ATP) Partners.

CPS-MSP-1RU-K9	1-RU chassis with motherboard, one CPU, and one built-in 300W power supply (no drives, no power cables, and no option cards)
CIVS-HDD-1000	1 TB SATA drive for CIVS-MSP and CPS-MSP platforms (1-RU)
CPS-MSP-2RU-K9	2-RU chassis with motherboard, one CPU, and one 900W power supply (no drives and no power cables)
CPS-HDD-6TB-BNDL	6 x 1 TB SATA hard-disk drive bundle for CPS-MSP platforms (2-RU)

For More Information

http://www.cisco.com/en/US/products/ps10823/index.html

Cisco IPICS Server Software

The Cisco IPICS Server supports the management of the Cisco IPICS system. First responders and safety and security personnel use the Cisco IPICS system to enable rapid incident response, collaborative crisis communications, notification, and comprehensive interoperable communications. The Cisco IPICS Server is used to create virtual talk groups (VTGs) to facilitate push-to-talk (PTT) communications between users of multiple types and technologies of Land Mobile Radios with users of PCs, landline phones, cellular and Nextel phones, and Cisco Unified IP Phones.

The Cisco IPICS Server is a security-enhanced, Linux-based platform installed on select Cisco 7800 Series Media Convergence Servers, a family of proven and reliable hardware platforms that you can deploy in mobile command units or in headquarters, branch offices, or operations centers. Other Cisco IPICS system components include the Cisco IPICS Push-to-Talk Management Center (PMC), Cisco IPICS Phone Client, Cisco IPICS Operational Views (Ops Views), Cisco Land Mobile Radio (LMR) gateways, Router Media Service (RMS), and Session Initiation Protocol (SIP) telephony gateways.

Cisco IPICS is a systems-level, network-based solution for voice interoperability. It takes full advantage of open IP standards and IP network infrastructure for greater resiliency, scaling, and security, and is part of a complete communications solution for organizations of all sizes.

Key Features and Benefits

- All-in-one safety and security incident response, communications, and collaboration solution
- User-friendly setup and operation
- Centralized, remote, or distributed administration across locations, agencies, networks, and jurisdictions
- Complete and secure Virtual Push to Talk communications and management

- Support for secure incident management, response, notification, and messaging
- Customizable secure voice dial-in and dial-out access to radio channels and incident virtual talk groups
- Role-based user, dispatch console, operator, and system administrator management
- Support for radio resources, desktop PC clients, and Cisco Unified Communications IP Phone PTT clients
- Integrated support and management of Cisco integrated services routers and Land Mobile Radio gateways
- Proven IP network protocols for critical communications over IP Unicast, IP Multicast, Session Initiation Protocol (SIP), VPN, satellite, IP, and wireless networks

Selected Part Numbers and Ordering Information

CIS-IPICS2.0-K9(=)	Cisco IPICS 2.1 Server software and licenses, including licenses for: · 50 Cisco IPICS Virtual Talk Groups · 4 Cisco IPICS Channel/radio ports · 4 Cisco IPICS PMC clients · 10 Cisco IPICS IP Phone clients · 2 Cisco IPICS Operational Views
CIS-IPICS-PM1-K9(=)	Cisco IPICS Policy Engine for Cisco IPICS 2.1 or Higher Cisco IPICS Policy Engine Dial Port for Cisco IPICS 2.1 or Higher
CIS-VIP-DIAL(=)	Cisco IPICS Policy Engine Dial Port for Cisco IPICS 2.1 or Higher
CIS-VIP-VTG(=)	Cisco IPICS Virtual Talk Group (VTG) for Cisco IPICS 2.1 or Higher
CIS-VIP-CHNL(=)	Cisco IPICS Channel/Radio Port for Cisco IPICS 2.1 or Higher
CIS-PHN(=)	Cisco IPICS IP Phone Client License for Cisco IPICS 2.1 or Higher
CIS-PMC-K9(=)	Cisco IPICS PMC Client for Cisco IPICS 2.1 or Higher
CIS-OPSVIEW2(=)	Cisco IPICS Operational Views for IPICS 2.1 or Higher

For More Information

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

Cisco IPICS Dispatch Console

The Cisco IPICS Dispatch Console is an end-to-end radio dispatching solution designed for mission-critical radio communications. It is the vital link between dispatchers and field personnel, helping to coordinate field response and ensure personnel safety. Running on a standard PC platform, it extends existing push-to-talk (PTT) radio channels so that users with a variety of communication devices can participate.

The Cisco IPICS Dispatch Console introduces rich-media incident management support, giving dispatchers the power to consolidate information relating to an incident and instantly share it among participants. Incident dispatch enables the sharing of multimedia data such as the following:

- Live video sent from surveillance cameras, access control gateways, and mobile clients
- Archived videos such as Flip or YouTube
- Photos
- Alarm monitoring
- Journal and live statuses
- Website links

Key Features and Benefits

- Push to talk (PTT) and monitoring for up to 50 radio channels and talk groups
- Selecting, unselecting, and deselecting of channels
- Selecting and unselecting of audio speakers
- Receiving and transmitting of on-screen indicators for channel activity
- Instant recall recording per channel
- Last-call transmit
- Alert tones
- Channel multiselect
- Confirmation tones for trunked systems
- Unit ID and talker ID
- Emergency alert and acknowledge
- Coded and clear channels
- Loop prevention
- Integrated telephone
- Frequency select

Selected Part Numbers and Ordering Information

The Cisco IPICS Dispatch Console comes in two versions, Silver and Platinum. The Silver version provides a simple user interface and supports basic radio and incident dispatch functions. The Platinum version includes patch capabilities, integrated telephone, incident management, and policy management support.

IPICS Dispatch Console is available through Cisco Authorized Technology Provider (ATP) Partners.

CIS-CON4.0-SIL	Cisco Dispatch Console Silver License
CIS-CON4.0-PLA	Cisco Dispatch Console Platinum License
CIS-CON4.0-SIL-UG	Cisco Dispatch Console Silver Upgrade License

For More Information

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

Cisco IPICS Mobile Client

The Cisco IPICS Mobile Client is a new component of the Cisco IPICS solution that helps smartphones join an IPICS-enabled incident response network. This smartphone application allows responders to interact with other incident participants. Incidents can be within a single agency or among multiple agencies. With this application, responders can perform a variety of incident-related activities, including:

- Access incident-related push-to-talk (PTT) channels to communicate between responders and radio users
- Obtain up-to-date incident status information from each responder
- Access incident-related video clips, photographs, and status either pushed to them from the dispatcher or added by other responders
- Dynamically add their own video clips, photographs, and status updates

Key Features and Benefits

- Mobility—The Cisco IPICS Mobile Client, based on smartphone technology, moves with the user anywhere there is a wireless network, for example, Wi-Fi or third-generation (3G) cellular network.
- Radio interoperability and beyond—The Cisco IPICS Mobile Client allows PTT interoperability with radio channels and talk groups.
- Rich media—The Cisco IPICS Mobile Client moves beyond audio to support rich media and a new generation of mobile endpoints.
- Open standards compatible—Built as a smartphone application, the Cisco IPICS Mobile Client transfers to new devices as replacement technology is introduced.

Specifications

Platforms	**Apple iPhone 3G/3GS**
Connectivity	WiFi or 3G with active service (dependent upon Smartphone)
Assigned incidents	Up to 10 suggested for optimum performance
Live video	Up to 10 minutes
Photos	Up to 2 MB
Mobility client	1000 mobile clients per IPICS system

Selected Part Numbers and Ordering Information

The Cisco IPICS Mobile Client requires an Apple iPhone 3G/3GS and iPhone service from a certified service provider. Note: Both the iPhone 3G/3GS can view incident media, add photos, and communicate on the Incident PTT channel. The iPhone 3GS additionally supports video uploading.

The IPICS Mobile Client is available for download free of charge from the Apple App Store. Visit the Apple iPhone website at http://www.apple.com/iphone/apps-for-iphone/. The application name is "Incident".

This application also requires a Cisco IPICS installation as well as one or more IPICS Mobile Client licenses on the IPICS Server, one license for each active IPICS Mobile Client. The Cisco IPICS solution and Mobile Client licenses are available direct from Cisco Advanced Services and through select technology partners.

CIS-MC	Mobile Client IPICS License
CIS-MC-100	Mobile Client IPICS License 100 Units

For More Information

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

Cisco Security Services

Cisco and our partners can help you accelerate business transformation, operational maturity, and agility through consultative planning, solution development, and full deployment, creating network architectures that can optimize IT services and enhance your business.

The broad portfolio of Cisco Security Services helps maintain intelligent defenses against information security threats. Services are based on proven methodologies and best practices for designing, deploying, operating, and optimizing network solutions and technologies. This integrated security services portfolio provides solutions for threat management, event management, vulnerability management, and compliance support across a broad range of industries and advanced technologies, including unified communications, storage networking, and wireless networks.

Cisco Services for Physical Security provide comprehensive offerings to help plan, design, implement, and operate physical security solutions.

Cisco has a portfolio of technical services that help maintain the health and performance of every Cisco product. These services range from traditional maintenance to proactive and predictive services that use smart services capabilities. Cisco's Security Services provide detailed diagnostics and real-time alerts on core network devices to help resolve concerns quickly and improve network availability. The Cisco Technical Services portfolio is built on foundational capabilities and expanded performance capabilities to meet the changing technology needs of our customers.

For more information about Cisco Security Services, visit http://www.cisco.com/go/services/security.