Cisco IPsec and SSL VPN Solutions Portfolio

Cisco ASA 5500 Series Adaptive Security Appliances, Cisco Integrated Services Routers, Cisco ASR 1000 Series Aggregation Services Routers, Cisco 7200 Series and 7301 Routers, Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers.

VPNs allow organizations to securely connect remote offices and remote users using cost-effective, third-party Internet access rather than expensive dedicated WAN links or long-distance remote dial links. Using high-bandwidth Internet connectivity—such as DSL, Ethernet, and cable—and securing it with encrypted VPN tunnels enables organizations to reduce WAN bandwidth costs while increasing connectivity speeds.

VPNs provide high levels of security through encryption and authentication technologies that protect data from unauthorized access. VPNs provide more flexibility and scalability than Frame Relay, leased lines, or dialup remote-access connections by enabling the quick addition of new sites or users through the easy-to-provision Internet infrastructure within ISPs. As a result, organizations can dramatically increase the reach of their networks without significantly expanding their infrastructures.

There are two types of encrypted VPNs: site-to-site and remote-access. Site-to-site VPNs are an alternative to Frame Relay or leased-line WANs, which allow businesses to extend network resources to branch offices, home offices, and business partner sites. All traffic between sites is encrypted using IP Security (IPsec). Routing, quality of service (QoS), and other network features help ensure the reliability and quality of VPN traffic. Site-to-site VPNs are also used to increase the security of other WAN technologies such as Multiprotocol Label Switching (MPLS) and Frame Relay through data encryption and authentication.

Remote-access VPNs are a flexible and cost-effective alternative to private dialup solutions; in fact, VPNs have become the primary solution for remote-access connectivity. Remote-access VPNs extend almost any data, voice, or video application to remote working locations, helping to create a user experience that emulates working in the main office location. All traffic between the user desktop and the office site is encrypted. Remote-access VPNs may be deployed using Secure Sockets Layer (SSL) VPN, IPsec, or both, depending on deployment requirements.

Cisco VPN Solutions

The extensive portfolio of Cisco® VPN solutions includes Cisco ASA 5500 Series Adaptive Security Appliances, Cisco Integrated Services Routers, Cisco ASR 1000 Series Aggregation Services Routers, Cisco 7200 Series and 7301 Routers, Cisco Catalyst® 6500 Series Switches, Cisco 7600 Series Routers, and Cisico ASA 5500 Series Adaptive Security Appliances. These solutions include mission-specific feature sets based on IPsec and SSL VPN technologies to provide the most suitable technologies for diverse network environments and requirements.

Site-to-Site VPN

Cisco's site-to-site VPN solutions integrate advanced network intelligence and routing to deliver reliable transport for complex mission-critical traffic, such as voice and client-server applications, without compromising communications quality. Site-to-site VPN technologies such as Dynamic

Multipoint VPN (DMVPN), Easy VPN, Routed Generic Routing Encapsulation (GRE), and tunnel-less Group Encrypted Transport VPN (GET VPN) deliver customized solutions for network designs ranging from traditional hub-and-spoke to networks with “any-to-any” intersite connectivity. These technologies also help streamline provisioning and minimize ongoing operational tasks. Integrated network features such as routing, QoS, and multicast support deliver any traffic type—including latency-sensitive voice/video and terminal services—while preserving transport reliability and quality over the Internet-based VPN.

Remote-Access VPNs

Remote-access VPNs extend almost any data, voice, or video application available in the office to remote working locations, helping to create a user experience that emulates working in the main office location. There are two primary methods for deploying remote-access VPNs: IPsec and SSL. Each method has its advantages based on the access requirements of your users and your organization’s IT processes. Many remote-access VPN solutions offer either IPsec or SSL, but Cisco solutions integrate both technologies on a single platform with unified management. Having both IPsec and SSL technologies enables customization of remote-access VPN deployments without any additional hardware or management complexity.

SSL VPNs

SSL-based VPNs provide remote-access connectivity from almost any Internet-enabled location using a standard Web browser and its native SSL encryption. They do not require any special-purpose client software to be pre-installed on the system. Thus, SSL VPNs are capable of “anywhere” connectivity from company-managed desktops and non-company-managed desktops, such as employee-owned PCs, contractor or business partner desktops, and Internet kiosks. All software required for application access across the SSL VPN connection is dynamically downloaded on an as-needed basis, thereby minimizing desktop software maintenance.

SSL VPNs provide two different types of access: clientless access and full network access. Clientless access requires no specialized VPN software on the user desktop; all VPN traffic is transmitted and delivered through a standard Web browser. Because all applications and network resources are accessed through a browser, only Web-enabled and some client-server applications—such as intranets, applications with Web interfaces, e-mail, calendaring, and file servers—can be accessed using a clientless connection. This limited access is suitable for partners or contractors that should be provided access to a limited set of resources on the network. And because no special-purpose VPN software has to be delivered to the user desktop, provisioning and support concerns are minimized.

Full network access enables access to virtually any application, server, or resource available on the network. Access is delivered through a lightweight VPN client that is dynamically downloaded to the user desktop (through a browser) upon connection to the SSL VPN gateway. This VPN client, because it is dynamically downloaded and updated without any manual software distribution or interaction from the end user, requires little or no desktop support by IT staff, thereby minimizing deployment and operations costs. Like clientless access, full network access offers fully customized access control based on the access privileges of the end user. Full network access is a natural choice for employees who need remote access to the same applications and network resources they use when in the office or for any client-server application that cannot be delivered across a Web-based clientless connection.

IPsec VPNs

IPsec-based VPNs are the deployment-proven remote-access technology used by most organizations today. Connections are established using VPN client software preinstalled on the user desktop, making it primarily useful on company-managed desktops. The client software can also be extensively modified through its APIs for use in special applications such as unattended kiosks and to provide integration with other desktop applications.

Working Together

SSL VPNs and IPsec VPNs are complementary technologies that can be deployed together to better address the unique access requirements of diverse user communities. Both offer access to virtually any network application or resource. SSL VPNs offer additional features such as easy connectivity from desktops outside your company's management, little or no desktop software maintenance, and user-customized Web portals upon login.

Cisco offers remote-access VPN solutions on the Cisco ASA 5500 Series VPN Edition and Cisco Integrated Services Routers, and Cisco ASR 1000 Series Aggregation Services Router. Features include Web-based clientless access and full network access without preinstalled desktop VPN software, a threat-protected VPN to guard against malware and hackers, and single-device solutions for both SSL- and IPsec-based VPNs. In addition, the innovative Cisco Easy VPN and Cisco VPN Client auto-update capabilities found in Cisco remote-access VPN solutions deliver a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture. With a foundation of dynamic policy distribution and effortless provisioning, Cisco Easy VPN and Cisco VPN Client auto-update features make it easy to maintain remote-device and VPN client configurations typically required by IPsec remote-access VPN solutions.

Table 1 shows Cisco products and feature benefits for site-to-site and remote-access VPNs.

Table 1. Cisco Product Matrix and Feature Benefits for Site-to-Site and Remote-Access VPN

	Site-to-Site VPN	IPsec Remote-Access VPN	SSL Remote-Access VPN
Cisco Routers or Cisco Catalyst Switches	Most feature-rich	Yes	Yes (routers only)
Cisco ASR 1000 Series Router	Most feature-rich	Yes	No
Cisco ASA 5500 Series Appliances	Yes	Most feature-rich	Most feature-rich

Cisco ASA 5500 Series Adaptive Security Appliances

Cisco ASA 5500 Series all-in-one adaptive security appliances deliver enterprise-class security and VPN capabilities to small and medium-sized businesses and large enterprise networks in a modular, purpose-built appliance (Figure 1). The Cisco ASA 5500 Series incorporates a wide range of integrated security services, including firewall, intrusion prevention system (IPS), and Anti-X services with SSL and IPsec VPN services in an easy-to-deploy, high-performance solution. By integrating VPN and security services, the Cisco ASA 5500 Series protects the VPN deployment from becoming a conduit for network attacks such as worms, viruses, malware, or hacking. Detailed application and access control policy is applied to VPN traffic, so legitimate users have access to services and resources.

The Cisco ASA 5500 Series is Cisco's most feature-rich solution for SSL and IPsec-based remote access, supporting robust site-to-site connectivity. The series provides higher scalability and greater throughput capabilities than the widely deployed Cisco VPN 3000 Series Concentrators and can integrate easily into any Cisco VPN 3000 Series load-balancing cluster.

Figure 1. The Cisco ASA 5500 Series Portfolio

Table 2 summarizes the VPN performance of each Cisco ASA 5500 Series model.

Table 2. Cisco ASA 5500 Series Appliance VPN Performance.

Model	SSL/IPsec Scalability	Maximum VPN Throughput
Cisco ASA 5505	25 simultaneous VPN connections	100 Mbps
Cisco ASA 5510	250 simultaneous VPN connections	170 Mbps
Cisco ASA 5520	750 simultaneous VPN connections	225 Mbps
Cisco ASA 5540	2500/5000 simultaneous VPN connections	325 Mbps
Cisco ASA 5550	5000 simultaneous VPN connections	425 Mbps
Cisco ASA 5580-20 and 5580-40	10,000 simultaneous VPN connections	1 Gbps

Remote-access and site-to-site IPsec VPN services are included as a base feature of all Cisco ASA 5500 Series models. SSL VPN features are available on the Cisco ASA 5500 Series VPN Edition or as a licensed feature set that can be added to any Cisco ASA 5500 Series model. Please see the product data sheet for more details.

The Cisco ASA 5500 Series offers flexible technologies that deliver tailored solutions to suit connectivity requirements. It provides employees with company-managed desktops robust, customizable remote access through an IPsec VPN. For endpoints that are not company-managed, such as extranets, Internet kiosks, or employee-owned desktops, the Cisco ASA 5500 Series delivers SSL-based remote-access VPN services. Organizations can take advantage of Cisco's remote-access expertise to deploy a single integrated platform with broad support for all networked applications.

Benefits of the Cisco ASA 5500 Series include:

- **Flexible platform:** Providing both IPsec and SSL VPN on a single platform eliminates the inefficiency and added cost of deploying separate platforms.
- **Superior clientless network access:** Clientless SSL VPN-based remote access does not require desktop client software. Superior content rewriting capabilities help ensure reliable rendering of complex applications or Webpages with Java, JavaScript, and ActiveX content.

- **Advanced client-based full network access:** Customizable connectivity is provided through the dynamically downloaded Cisco SSL VPN Client or Cisco IPsec VPN Client. For IPsec deployments, Cisco Easy VPN dynamically pushes the latest VPN security policies to remote VPN devices and clients, providing flexibility, scalability, and ease of use.
- **Resilient clustering:** Remote-access deployments can scale cost-effectively by evenly distributing VPN sessions across all Cisco ASA 5500 Series and Cisco VPN 3000 Series devices without user intervention or external load-balancing equipment. This highly resilient capability eliminates any single point of failure and helps to protect network investments.
- **Threat-protected VPN:** VPNs are a primary source of entry for malware, such as worms, viruses, spyware, keyloggers, Trojan horses, and rootkits, into organizations' networks. The Cisco ASA 5500 Series' deep intrusion prevention, antivirus, application-aware firewall, and VPN endpoint security capabilities help ensure that VPN connections do not become a conduit for security threats.

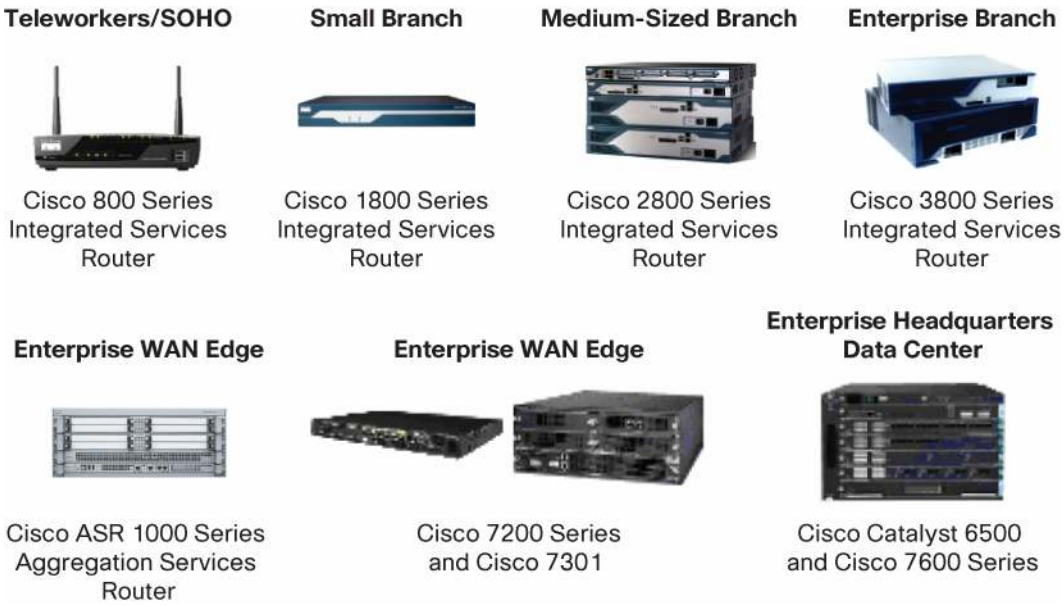
Cisco ASA 5500 Series Adaptive Security Appliances are managed through the integrated Web-based Cisco Adaptive Security Device Manager (ASDM). Cisco ASDM manages all security and VPN functions of the appliances.

Cisco Routers and Cisco Catalyst Switches

Cisco Integrated Services Routers, Cisco Aggregation Services Routers, and Cisco Catalyst switches (Figure 2) use Cisco IOS® Software to easily deploy and scale site-to-site VPNs of any topology, from hub-and-spoke to the more complex fully meshed VPNs. In addition, the Cisco IOS Advanced Security feature set combines a rich VPN feature set with advanced firewall, intrusion prevention, and extensive Cisco IOS Software capabilities, including QoS, multiprotocol, multicast, and advanced routing support. Cisco integrated services routers and Cisco Catalyst 6500 Series switches are suitable for deploying VPNs and security on networks of all sizes, integrating all services in a single device, and featuring a wide selection of WAN and LAN interfaces.

Cisco IPsec VPN technology has earned industry evaluations and certifications such as Common Criteria Evaluation Assurance Level (EAL) 4, and FIPS-140-1, Level 2.

Figure 2. Cisco IOS VPN Security Portfolio and Suggested Applications



These devices incorporate many advanced VPN features:

- **IPsec and SSL VPN services integration** enables routers to provide both remote-access and site-to-site services from a single device.
- **Dynamic Multipoint VPN (DMVPN)** enables autoprovisioning of site-to-site IPsec VPNs. DMVPN eases provisioning by dynamically discovering remote locations using standard routing protocols, then automatically enabling an on-demand IPsec VPN tunnel between remote sites for a multipoint meshed design.
- **Group Encrypted Transport VPN (GET VPN)** is a new category of VPN that eliminates the need for traditional VPN tunnels. GET VPN delivers highly scalable and manageable intersite any-to-any VPN connectivity without the complexity typically encountered with meshed network designs. GET VPN supplements DMVPN by enabling high-scale, always-on, any-to-any site connectivity that is critical for maintaining the transmission quality of latency-sensitive traffic such as voice, video, and terminal services.
- **Voice and Video Enabled VPN (V3PN)** integrates IP telephony, QoS, and IPsec, providing an end-to-end VPN service that helps ensure the timely delivery of latency-sensitive applications such as voice and video.
- **IPsec stateful failover** provides fast and scalable network resiliency for VPN sessions between remote and central sites. With both stateless and stateful failover solutions available, options such as Dead Peer Detection (DPD), Hot Standby Router Protocol (HSRP), Reverse Route Injection (RRI), and Stateful Switchover (SSO) help ensure uptime of mission-critical applications.
- **IPsec and MPLS integration** enables service providers to map IPsec sessions directly into an MPLS VPN or use GET VPN to accomplish this without traditional tunnels. This solution can be deployed on colocated edge routers that are connected to a Cisco IOS Software-based MPLS provider-edge network, which can include Cisco 7200, 7500, 10000, or 12000 Series Routers or Cisco 7301 Routers. This approach enables service providers to securely extend VPN service beyond the MPLS network by using the public IP infrastructure to connect enterprise customers' remote offices, telecommuters, and mobile users to the corporate network. Cisco further extends the MPLS solution with support of multi-Virtual Route Forwarding (VRF) in a single router, enabling customer-edge routers to maintain

separate VRF tables to extend an MPLS VPN beyond the provider-edge router node to a branch office.

- **VPN hardware modules for Cisco routers** provide up to 10 times the performance of software-only encryption by offloading encryption processing from the router CPU.
- **Integrated security features** such as firewall and IPS help ensure that VPNs do not become a conduit for hackers and malware.

Cisco offers VPN security router bundles on most router platforms. (A comprehensive list of router security bundles can be found at http://www.cisco.com/go/securitybundles.) All bundles include the selected router platform, a Cisco VPN hardware card and additional memory where required, and the Cisco IOS Software to run IPsec Triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES) encryption and Cisco IOS Firewall with IPS. Options can be added to each bundle as needed to add capabilities.

Cisco also offers four IPsec VPN bundles based on Cisco Catalyst 6500 Series Switches. The bundles include the Cisco IPsec VPN Shared Port Adapter (SPA) and provide flexibility and integration for data centers, enterprise headends, and distribution points. Integrating the SPA with the switch creates a flexible, high-performance, 2.5-Gbps VPN solution in campus and WAN edge deployment scenarios while providing additional flexibility, redundancy, and the addition of high-density I/O or other service options. The open slots in the switches can accommodate other advanced security services modules, such as the Cisco Catalyst 6500 Series Firewall Services Module (FWSM), the Cisco Catalyst 6500 Series Intrusion Detection System Module (IDSM-2), and the Cisco Catalyst 6500 Series Network Analysis Module (NAM-1 and NAM-2). This modular approach allows organizations to take full advantage of their installed switching and routing infrastructure at a relatively low cost.

Cisco ASR 1000 Series: A Powerful New Paradigm for the WAN Edge

The new Cisco ASR 1000 Series Aggregation Services Router uses the onboard Cisco Embedded Services Processor (ESP) to deliver scalable, integrated, and secure connectivity. The routers deliver multigigabit IPsec VPN aggregation services concurrent with high-speed WAN, Internet edge routing, QoS, and multicast. The Cisco Embedded Services Processor uses the Cisco QuantumFlow Processor—the industry's first massive parallel processor hardware and software architecture—as a key subsystem to control packet flow and assure high performance, scalability, service quality, and security.

Positioned between the Cisco 7200 Series and the Cisco 7600 and Catalyst 6500 Series, Cisco ASR 1000 Series routers make a compelling case for integrating headend IPsec VPN termination into enterprise WANs and Internet edge routers. It delivers unparalleled WAN availability in a carrier-class design and with very efficient power consumption.

- All Cisco ASR 1000 Series Aggregation Services Routers ship with high-speed encryption acceleration chips (include software developed by Cavium Networks) onboard, in the Embedded Services Processor. No additional or external crypto engine modules are required.
- The Cisco Embedded Services Processor-20G scales to 7.0 Gbps of IPsec encryption throughput, supporting up to 10,000 IPsec tunnels.
- The balance of total system bandwidth (5,10, 20 Gbps, depending on the Embedded Services Processor) is available to route clear-text traffic through the network at high speeds.
- Cisco ASR 1000 Series routers provide superior multicast and encryption processing with advanced packet scheduling and distribution mechanisms between the encryption and forwarding engines.
- Pre- and post-encryption QoS, scalable to support thousands of spokes, is available and embedded within the Cisco ASR 1000 Series Embedded Services Processor.

Cisco IPsec VPN solutions are supported on all Cisco Aggregation Services Routers with the Cisco IOS XE ASR 1000 Series RP1 Advanced IP Services and Advanced Enterprise Services software options.

For more information on Cisco ASR 1000 Series solutions, visit http://www.cisco.com/go/asr1000.

Table 3 summarizes the VPN performance of different Cisco router platforms.

Table 3. VPN Performance of Cisco Routers and Switches

Cisco VPN Security Router	Maximum Tunnels	Maximum 3DES Throughput	Maximum AES Throughput
Cisco 850 Series Integrated Services Router	5	8 Mbps	8 Mbps
Cisco 870 Series Integrated Services Router	10	30 Mbps	30 Mbps
Cisco 1800 Series Integrated Services Router (Fixed Configuration)	50	40 Mbps	40 Mbps
Cisco 1841 Integrated Services Router with onboard VPN	100	45 Mbps	45 Mbps
Cisco 1841 Integrated Services Router with AIM-VPN/SSL-1	800	95 Mbps	95 Mbps
Cisco 2801 Integrated Services Router with onboard VPN	150	50 Mbps	50 Mbps
Cisco 2801 Integrated Services Router with AIM-VPN/SSL-2	1500	160 Mbps	160 Mbps
Cisco 2811 Integrated Services Router with onboard VPN	200	55 Mbps	55 Mbps
Cisco 2811 Integrated Services Router with AIM-VPN/SSL-2	1500	130 Mbps	130 Mbps
Cisco 2821 Integrated Services Router with onboard VPN	250	56 Mbps	56 Mbps
Cisco 2821 Integrated Services Router with AIM-VPN/SSL-2	1500	140 Mbps	140 Mbps
Cisco 2851 Integrated Services Router with onboard VPN	300	66 Mbps	66 Mbps
Cisco 2851 Integrated Services Router with AIM-VPN/SSL-2	1500	160 Mbps	160 Mbps
Cisco 3825 Integrated Services Router with onboard VPN	500	170 Mbps	170 Mbps
Cisco 3825 Integrated Services Router with AIM-VPN/SSL-3	2000	185 Mbps	185 Mbps
Cisco 3845 Integrated Services Router with onboard VPN	700	180 Mbps	180 Mbps
Cisco 3845 Integrated Services Router with AIM-VPN/SSL-3	2500	210 Mbps	210 Mbps
Cisco 7301 Router with SA-VAM2+	5000	280 Mbps	280 Mbps
Cisco 7200VXR Series Router and NPE-G1 with a single SA-VAM2+	5000	280 Mbps	280 Mbps
Cisco 7200VXR Series Router and NPE-G2 with a single SA-VAM2+	5000	280 Mbps	280 Mbps
Cisco 7200VXR Series Router and NPE-G2 with a single VSA	5000	950 Mbps	950 Mbps
Cisco ASR 1000 Series Aggregation Services Routers with Embedded Services Processor-5G	5,000	1.8 Gbps	1.8 Gbps
Cisco ASR 1000 Series Aggregation Services Routers with Embedded Services Processor-10G	10,000	4.0 Gbps	4.0 Gbps
Cisco ASR 1000 Series Aggregation Services Routers with Embedded Services Processor-20G	10,000	7.0 Gbps	7.0 Gbps
Cisco Catalyst 6500 Series/Cisco 7600 Series VPN Bundle (includes one or more IPsec VPN SPAs)	16,000	2.5–25 Gbps*	2.5–25 Gbps*
Cisco Catalyst 6500 Series VPN Services Port Adapter Bundle (includes one or more IPsec VSPAs)	16,000	8–80 Gbps*	8–80 Gbps*

* Up to 10 VPN SPAs / VSPAs can be installed in a single chassis, providing increased VPN bandwidth.

Cisco IOS Software-based VPN security routers and Cisco Catalyst switches can be managed using a convenient command-line interface (CLI) through a variety of methods, including Telnet, Secure Shell (SSH) Protocol Version 2.0, or out-of-band through a console port. Alternatively, Cisco IOS Software-based routers can be configured and monitored using Cisco Router and Security Device Manager (SDM), an intuitive and secure Web-based tool embedded within Cisco IOS Software-based access routers. Cisco SDM simplifies device and security configuration by offering wizards to help users quickly and easily deploy, configure, and monitor VPNs without extensive knowledge of the Cisco IOS CLI. Cisco IOS Software-based routers can also be configured and monitored using tools available from Cisco technology partners.

Cisco Security Management Solutions

In addition to the device managers embedded in Cisco VPN security solutions, Cisco provides standalone security management applications for those who need to manage a wider range of devices.

Cisco Security Manager, an integral part of the Cisco Self-Defending Network, combines Web-based tools for configuring, monitoring, and troubleshooting VPNs, firewalls, and network- and host-based intrusion detection systems (IDSs) and intrusion prevention systems (IPSs). Cisco Security Manager delivers VPN configuration management, firewall management, surveillance, device inventory, and software version management features from a single console.

Complementing Cisco Security Manager is the Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS). Cisco Security MARS is a family of high-performance, scalable threat mitigation appliances that fortify deployed network devices and security countermeasures by combining network intelligence, events correlation, and mitigation capability. Cisco Security MARS can readily identify, manage, and eliminate network attacks and maintain regulatory compliance.

Additional Product and Ordering Information

For more information, please visit the following links.

- Cisco router security bundles: http://www.cisco.com/go/securitybundles
- Cisco ASR 1000 Series Aggregation Services Routers: http://www.cisco.com/go/asr1000
- Cisco ASA 5500 Series VPN Edition: http://www.cisco.com/en/US/products/ps6120/prod_brochure0900aecd80402e39.html
- Cisco Catalyst 6500 Series and Cisco 7600 Series IPsec Shared Port Adapter: http://www.cisco.com/en/US/products/ps6917/index.html
- Cisco SSL VPN: http://www.cisco.com/go/sslvpn
- Cisco IPsec VPN: http://www.cisco.com/go/ipsec
- Cisco Router and Security Device Manager: http://www.cisco.com/go/sdm
- Cisco Adaptive Security Device Manager for the Cisco ASA 5500 Series: http://www.cisco.com/en/US/products/ps6121/index.html
- Cisco Security Manager: http://www.cisco.com/en/US/products/ps6498/index.html
- Cisco Security MARS: http://www.cisco.com/en/US/products/ps6241/index.html
- Cisco Ordering Page: http://www.cisco.com/en/US/ordering/index.shtml

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C78-364489-04 09/08