



DATA SHEET

CISCO IPSEC AND SSL VPN SOLUTIONS

Cisco VPN 3000 Series Concentrators, Cisco PIX Security Appliances, Cisco ASA 5500 Series Adaptive Security Appliances, Cisco IOS VPN Security Routers, and Cisco Catalyst 6500 Series Switches

VPNs allow organizations to securely connect remote offices and remote users using cost-effective, third-party Internet access rather than expensive dedicated WAN links. By deploying VPNs over high-bandwidth transport such as DSL, Ethernet, and cable, organizations can easily reduce their connectivity costs while increasing remote connection bandwidth. VPNs are an alternative to the Frame Relay and leased-line WAN infrastructures typically used to provide network connectivity for branch offices, home office intranets, and business partner extranets.

Encrypted VPNs provide the highest possible levels of security through advanced encryption and authentication protocols that protect data from unauthorized access. With encrypted VPNs, corporations are able to increase the capacity of data, users, and connections without significantly adding to an existing infrastructure. Encrypted VPNs provide more flexibility and scalability than Frame Relay and leased-line connections by enabling corporations to take advantage of the easy-to-provision Internet infrastructure within ISPs and easily add new users. As a result, corporations are able to dramatically increase capacity without the need to significantly expand infrastructure.

There are two types of encrypted VPNs: site-to-site and remote-access. Site-to-site encrypted VPNs provide the same benefits as private WANs—they help to ensure private communications from one trusted site to another, and provide multiprotocol support, high reliability, and extensive scalability. Site-to-site encrypted VPNs are cost-effective and secure, and allow for greater administrative flexibility than legacy private WANs.

Remote-access VPNs are a flexible and cost-effective alternative to private dialup solutions; in fact, VPNs have become the logical solution for remote-access connectivity. Deploying a remote-access VPN helps reduce organizations' communications expenses by using the local dialup infrastructures of ISPs. Similarly, remote-access VPNs allow mobile workers, telecommuters, partners, and day extenders to take advantage of broadband connectivity.

VPN SOLUTIONS TO MEET EVERY NEED

Cisco Systems® offers a wide range of VPN products, from VPN-optimized routers, firewalls, and dedicated VPN concentrators to hardware- and software-based VPN clients and Secure Sockets Layer (SSL)-based VPNs, resulting in a complete portfolio of VPN solutions able to meet the requirements of any organization.

The extensive portfolio of Cisco VPN solutions includes Cisco IOS® VPN security routers, Cisco Catalyst® 6500 Series switches, Cisco VPN 3000 Series concentrators, Cisco PIX® security appliances, and the new Cisco ASA 5500 Series of adaptive security appliances. These solutions are designed with mission-specific feature sets, and implement leading VPN technologies such as IP Security (IPSec) and SSL to allow customers to deploy the best technologies available based on their network environments and requirements.

Site-to-Site VPN

Site-to-site VPNs allow businesses to extend their network resources to branch offices, home offices, and business partner sites. All traffic sent between the sites is encrypted using IPSec, which provides network-layer encryption for sensitive data passing across the VPN tunnel.

Remote-Access VPN

IPSec VPN provides remote users with the most robust remote-access environments by extending 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.

Cisco WebVPN

Cisco WebVPN provides SSL VPN-based remote-access connectivity from almost any Internet-enabled location using only a Web browser and its native SSL encryption, enabling companies to securely extend their enterprise networks to any authorized user by providing remote-access connectivity to corporate resources from any Internet-enabled location. SSL VPN enables access from non-corporate-owned machines such as home PCs, Internet kiosks, or wireless hotspots, where an IT department cannot easily deploy and manage the VPN client software necessary for IPSec VPN connections. The Cisco WebVPN solution delivers three levels of SSL VPN access: clientless, thin-client, and SSL tunneling client access, enabling the appropriate level of application access based on the end-system deployment environment requirements. SSL VPNs allow users to access Webpages and Web-enabled services—including the ability to access files, send and receive e-mail, and run TCP-based applications—without the use of IPSec VPN client software. SSL-based VPNs are an excellent fit for user populations that require per-application or per-server access control, or access from non-enterprise-owned desktops.

SSL VPNs and IPSec VPNs are complementary technologies that can be deployed together to better address the unique access requirements of diverse user communities. Cisco has enhanced its widely deployed IPSec VPN products to deliver SSL-based VPN (clientless, Web browser-based) services as well, providing the benefits of both technologies on a single device.* This strategy eases deployment and management by using the existing installed infrastructure, preserving customer investments in existing VPN equipment.

In addition, the innovative Cisco Easy VPN capabilities found in Cisco VPN 3000 Series concentrators, Cisco PIX Security Appliances, Cisco ASA 5500 Series appliances, and Cisco IOS routers deliver a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture. Built upon the foundation of dynamic policy distribution and effortless provisioning, Cisco Easy VPN eliminates the operational costs associated with maintaining remote-device configurations typically required by traditional VPN solutions. Easy VPN enables Cisco customers to enjoy the many benefits that VPNs provide—such as increased employee productivity as a result of high-speed broadband connectivity, and significantly reduced operational costs that result from eliminating legacy dialup architecture expenses—without the problems commonly associated with other remote-access VPN solutions.

Cisco Easy VPN consists of two components: Easy VPN Server and Easy VPN Remote. Cisco Easy VPN Server allows Cisco IOS routers, Cisco PIX Security Appliances, Cisco ASA 5500 Series adaptive security appliances, and Cisco VPN 3000 Series concentrators to act as VPN head-end devices in site-to-site or remote-access VPNs, where the remote office devices are using Cisco Easy VPN Remote. Using Cisco Easy VPN Remote, security policies defined at the head-end are pushed to the remote VPN device, helping to ensure that those connections have up-to-date policies in place before connections are established. The Cisco Easy VPN Remote feature is supported by a wide range of platforms, including Cisco IOS routers, Cisco PIX Security Appliances, Cisco adaptive security appliances, Cisco VPN 3002 hardware clients, and Cisco VPN software clients.

Table 1 shows the Cisco product matrix and feature benefits for site-to-site and remote-access VPNs.

* This capability is available at no additional cost for Cisco VPN 3000 Series concentrators with Release v4.7.

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 PIX Security Appliances	Y	Y	N
Cisco VPN 3000 Series	Y	Most feature-rich	Most feature-rich
Cisco IOS Software or Cisco Catalyst Switches	Most feature-rich	Y	N
Cisco ASA 5500 Series	Y	Most feature-rich	Y

CISCO VPN 3000 SERIES CONCENTRATORS

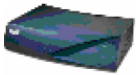





The Cisco VPN 3000 Series offers best-in-class remote-access VPN devices that provide businesses with unprecedented cost savings through flexible, reliable, and high-performance remote-access solutions. The Cisco VPN 3000 Series is Cisco’s most feature-rich remote-access VPN platform, offering solutions for the most diverse remote-access deployment scenarios. By offering both IPSec and SSL VPN connectivity on a single platform—without the expense of individual feature licensing—customers can achieve significant cost savings while experiencing the industry-leading advanced features required by today’s remote-access VPN deployments.

To fully realize the benefits of high-performance, secure remote access, a robust, highly available VPN solution is needed. The Cisco VPN 3000 Concentrator with version 4.7 software incorporates the most advanced, high-availability capabilities with a unique purpose-built, remote-access architecture that enables corporations to build high-performance, scalable, and robust VPN infrastructures to support their mission-critical, remote-access application requirements.

The Cisco VPN 3000 Concentrator Software with version 4.7 software delivers extensive application access with the SSL VPN client for WebVPN, best-in-market endpoint security and data integrity protection with the Cisco Secure Desktop, leading network infrastructure access with truly clientless Citrix server support, and network compliance validation controls with IPSec-enabled Network Admission Control (NAC).

Cisco VPN 3000 Series concentrators are ideal for organizations that require the most advanced and flexible remote-access VPN technology and that prefer the operational simplicity and management segregation of a focused-function VPN device. Purpose-built for remote-access VPN, Cisco VPN 3000 Series concentrators incorporate high availability, high performance, and scalability with the most diverse encryption and authentication techniques available today (Figure 1).

Figure 1. Cisco VPN 3000 Series Concentrators

Teleworkers/SOHO	Small Branch	Medium-Sized Branch	Enterprise Branch	Enterprise Headquarters
 Cisco VPN 3002	 Cisco VPN 3005	 Cisco VPN 3020 Cisco VPN 3030	 Cisco VPN 3060	 Cisco VPN 3080
	 Cisco VPN 3015			

Features of the Cisco VPN 3000 Series platform include:

- **Customized application access with Cisco WebVPN v4.7** delivering clientless, thin-client, and SSL tunneling client access methods. This enables deployment of the appropriate level of application access based on the end-system deployment environment, such as employees, extranets, and non-company-managed devices.
 - The SSL VPN Client for WebVPN is a lightweight, centrally configured, and easy-to-support SSL VPN software client which allows access to virtually any application. The SSL VPN Client for WebVPN is compatible with any SSL-enabled browser, and is dynamically pushed to the user in one of three methods—ActiveX, Java, or an .exe file.
 - Thin-client access with Cisco WebVPN v4.7 is achieved through a port forwarding mechanism enabled by a small Java applet download. Port forwarding relays data requested by the port on the local machine to the corresponding application port on the network side—granting the user access to more applications and network resources than a Web browser offers.
 - Clientless access with Cisco WebVPN allows users to connect to a corporate network with little requirements beyond a basic Web browser, and the ability to access Web servers or resources such as file shares and e-mail through Outlook Web Access 2003.
- The Cisco Secure Desktop is an industry-leading endpoint security solution offering advanced endpoint security and data theft prevention. At session initiation, the Cisco Secure Desktop performs a pre-connection security posture assessment, checking for the presence of antivirus software and personal firewall software, and ensures a keystroke logger is not running on the endpoint prior to the session initiation. During the session, all session data is encrypted and written to a secure vault, or partition to the hard drive, and cannot be saved to the host system by the user, knowingly or unknowingly. At the close of the session, the secure vault is eradicated using a U.S. Department of Defense (DoD) sanitization algorithm, erasing all session information, including cache files, history, cookies, file downloads, and passwords.
- Cisco VPN 3000 Concentrator Software v4.7 offers fully clientless Citrix support for terminal service environments, without the need for any SSL VPN client software. This increases application performance and reduces endpoint software compatibility issues, providing users with rapid and highly stable system access regardless of browser or security settings.
- Cisco VPN 3000 Concentrator Software v4.7 is NAC-enabled for IPSec remote-access scenarios, allowing the concentrator to act as a NAC enforcement point. This reduces the risk associated with extending network resources in remote-access scenarios by preventing vulnerable hosts from obtaining and retaining normal network access.
- Standards-based, easy-to-use VPN client with touchless Cisco Easy VPN configuration management and broad operating system support, including Windows, Mac, Linux, and Solaris.
- Integrated Web-based management system that enables corporations to easily install, configure, and monitor their remote-access VPNs.
- Integrated clustering and load-balancing capabilities that enable customers to scale their Cisco VPN 3000 Series deployments to tens of thousands of users with low operational expense.
- Broad user authentication support, including single-use passwords, RADIUS, Active Directory, Security Dynamics' SDI, digital certificates, and many others

Cisco VPN 3000 Series concentrators supports the widest range of connectivity options, including WebVPN, Cisco VPN Client, Cisco VPN 3002 Hardware Client, Microsoft Layer 2 Tunneling Protocol (L2TP)/IPSec, and Microsoft Point-to-Point Tunneling Protocol (PPTP).

The Cisco VPN 3000 Series offers both award-winning IPSec capabilities and clientless SSL VPN capabilities on a single platform. The combination of Cisco WebVPN and IPSec VPN provides unparalleled deployment flexibility and ease of management for meeting the requirements of any remote-access user population. Available applications include Webpage access, Windows (CIFS) file shares (via Web interface), e-mail (Simple Mail Transfer Protocol [SMTP], point of presence [POP], Internet Message Access Protocol [IMAP], MAPI/Exchange, Outlook Web Access, Lotus Notes, and Lotus iNotes), and most TCP-based client-server applications. Cisco WebVPN supports load balancing, multidevice clustering for pay-as-you-go scalability and resiliency, user-group-based management, and all user authentication methods supported by the Cisco VPN 3000, including single-use passwords, RADIUS, Active Directory, SDI, and digital certificates and many others.

Table 2 gives performance data for Cisco VPN 3000 Series concentrators.

Table 2. Cisco VPN 3000 Series Concentrator Performance

Cisco VPN 3000 Series Concentrators	Simultaneous IPSec Remote-Access Users*	Maximum LAN-to-LAN Sessions	Simultaneous WebVPN (Clientless) Users**	Encryption Throughput
Cisco VPN 3002	253***	1	–	2.2 Mbps
Cisco VPN 3005	200	100	50	4 Mbps
Cisco VPN 3015	100	100	75	4 Mbps
Cisco VPN 3020	750	250	200	50 Mbps
Cisco VPN 3030	1500	500	500	50 Mbps
Cisco VPN 3060	5000	1000	500	100 Mbps
Cisco VPN 3080	10,000	1000	500	100 Mbps

* Assumes maximum device memory and Enhanced Scalable Encryption Processing (SEP-E) modules (Cisco VPN 3020, 3030, 3060, and 3080 models). For planning purposes, a simultaneous IPSec user is considered to be a remote-access VPN user connected in all-tunneling mode; this includes one IKE security association and two unidirectional IPSec security associations. Network sizing should take into consideration number of sessions, throughput per user, and aggregate throughput of the remote access environment when choosing the appropriate VPN 3000 Concentrator model.

** Assumes maximum device memory and SEP-E modules (models 3020–3080). For planning purposes, a simultaneous WebVPN user is considered to be a clientless VPN user retrieving a Webpage at up to every 60 seconds. Users log in at the rate of one per second and pass data for the duration of the test. The average retrieval time for the Webpage is less than or equal to five seconds.

*** Refers to the number of devices on a single network behind the Cisco VPN 3002 Hardware Client.

Cisco VPN 3000 Series concentrators can be managed using any standard Web browser (HTTP or Secure HTTP [HTTPS]), as well as by Telnet, Secure Shell Protocol (SSHv1), or a console port. Files can be accessed through HTTPS, FTP, and SSH Copy (SCP). The Cisco VPN 3000 Series provides a user-friendly interface that simplifies configuration and monitoring by the enterprise and the service provider. This flexible user interface allows the configuration of access levels by user and groups, allowing thorough configuration and maintenance of security policies. For larger-scale deployments, Cisco VPN 3000 Series concentrators are supported in several Cisco network management applications, including the Cisco IP Solution Center (ISC), Cisco VPN Monitor, CiscoWorks CiscoView, and tools available from Cisco AVVID (Architecture for Voice, Video and Integrated Data) partners.

CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES

Cisco ASA 5500 Series all-in-one adaptive security appliances deliver enterprise-class security and VPN to small and medium-sized businesses (SMBs) and large enterprise networks in a modular, purpose-built appliance (Figure 2). The Cisco ASA 5500 Series incorporates a wide range of integrated security services, including firewall, intrusion prevention system (IPS), and VPN in an easy-to-deploy, high-performance solution. By integrating VPN and security services, the Cisco ASA 5500 Series provides secure VPN connectivity and communications. Integrated Adaptive Threat Defense capabilities protect 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 individuals and groups of users have access to the services and resources to which they are entitled.

The Cisco ASA 5500 Series is Cisco's most feature-rich solution for IPSec remote access, and also supports SSL VPN and IPSec site-to-site connectivity. Furthermore, the series provides higher scalability and increased throughput capabilities, relative to Cisco VPN 3000 Series concentrators. Cisco ASA 5500 Series adaptive security appliances integrate easily into any Cisco VPN 3000 Series load-balancing cluster.

Figure 2. The Cisco ASA 5500 Series Portfolio



Table 3 summarizes the VPN performance of each adaptive security appliance.

Table 3. Cisco ASA 5500 Series Appliance VPN Performance

Model	VPN Basic	VPN Plus	VPN Throughput (300/1400 Byte)
Cisco ASA 5510	50 VPN peers	150 VPN peers	50/170 Mbps
Cisco ASA 5520	300 VPN peers	750 VPN peers	100/225 Mbps
Cisco ASA 5540	500 VPN peers	2000 VPN peers 5000 VPN peers with a VPN premium license	200/325 Mbps

Licensing for the Cisco ASA 5500 Series licenses encompasses a large number of new features. There are three Cisco ASA licenses: Basic, VPN Plus, and VPN Premium. Feature licenses are available for additional security context support, failover active-active support, and GPRS Tunneling Protocol (GTP) support. Generally as you move upward in licensing class (Basic > Plus > Premium) the number of supported VPN peers increases (e.g. for the 5540 supported VPN peers changes from 500 to 2000 and finally 5000). Please see the product data sheet for more details.

Remote Access—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 via an IPSec VPN. In situations where endpoints are not company-managed, such as extranets, Internet kiosks, or employee-owned desktops, the Cisco ASA 5500 Series delivers WebVPN for SSL-based remote access. Enterprises can take advantage of Cisco’s remote-access expertise to deploy a single integrated platform with broad support for core enterprise applications.

- **Flexible platform**—Offers both IPSec and SSL VPN on a single platform, eliminating the need to provide parallel solutions. The inefficiency and added cost of deploying separate, distinct platforms for both SSL and IPSec VPNs is eliminated.
- **Resilient clustering**—Allows remote-access deployments to scale cost-effectively by evenly distributing VPN sessions across all Cisco ASA 5500 Series and VPN 3000 Series devices without requiring any user intervention. This highly resilient capability eliminates any single point of failure and helps to protect customer investments.
- **Cisco Easy VPN**—Delivers a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture. Cisco ASA 5500 Series appliances dynamically push the latest VPN security policies to remote VPN devices and clients, making sure those endpoint policies are up to date before a connection is established. This offers the ultimate flexibility, scalability, and ease of use.
- **Automatic Cisco VPN Client updates**—The Cisco ASA 5500 Series provides VPN client software “auto-update” capabilities that enable automated version upgrades for Cisco VPN Client software operating on remote desktops.

Site-to-Site—Using the standards-based site-to-site VPN capabilities provided by the Cisco ASA 5500 Series, businesses can securely extend their networks across low-cost Internet connections to business partners and remote and satellite offices worldwide.

- **VPN infrastructure for today’s applications**—The Cisco ASA 5500 Series provides a VPN infrastructure capable of converged voice, video, and data across a secure IPSec network, by combining robust site-to-site VPN support with rich inspection capabilities, quality of service (QoS), routing, and stateful failover features, allowing businesses to take advantages of the many benefits that converged networks deliver.
- **Robust security and performance**—Branch and remote offices extend a company’s reach into different markets and locations. Cisco ASA 5500 Series-based VPN solutions enable secure, high-speed communications between multiple locations, offering the performance, reliability, and availability that businesses need to communicate.

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

CISCO PIX SECURITY APPLIANCES

World-leading Cisco PIX Security Appliances provide robust, enterprise-class, integrated network security services, including stateful inspection firewalling, deep protocol and application inspection, IPSec VPN, multivector attack protection, and rich multimedia and voice security—in cost-effective, easy-to-deploy solutions. Cisco PIX Security Appliances range from compact, “plug-and-play” desktop security appliances for small and home offices to modular, carrier-class gigabit security appliances for the most demanding enterprise and service provider environments (Figure 3). Cisco PIX Security Appliances are ideal for those looking for the best-of-breed firewall combined with comprehensive VPN support. They are also an excellent option for organizations whose security policies recommends separate management of the security infrastructure, setting a clear demarcation between security and network operation.

Figure 3. Cisco PIX Security Appliance Portfolio

Teleworker/SOHO	Small Branch	Medium-Sized Branch	Enterprise Branch Enterprise Edge	Enterprise Headquarters Data Center
				
Cisco PIX 501	Cisco PIX 506E	Cisco PIX 515E	Cisco PIX 525	Cisco PIX 535

Note: The figure above provides general guidelines. Network environments should be scaled on application requirements, not solely on the size of the network.

Built upon a hardened, purpose-built operating system designed for delivering rich security services, Cisco PIX Security Appliances provide the highest levels of security. The appliances have earned numerous industry evaluations and certifications, including Common Criteria Evaluation Assurance Level (EAL) 4 status, as well as ICSA Labs Firewall and IPSec certifications.

Cisco PIX Security Appliances provide market-leading protection for a wide range of voice-over-IP (VoIP) and multimedia standards, allowing businesses to securely take advantage of the many benefits that converged data, voice, and video networks deliver. By combining VPN with the rich stateful inspection firewall services that Cisco PIX Security Appliances provide for these converged networking standards, businesses can securely extend voice and multimedia services to home-office and remote-office environments for additional cost savings, improved productivity, and competitive advantage.

Using the standards-based site-to-site VPN capabilities provided by Cisco PIX Security Appliances, businesses can securely extend their networks across low-cost Internet connections to business partners and remote and satellite offices worldwide. Built upon the IKE and IPSec VPN standards, Cisco PIX Security Appliances encrypt data using 56-bit Data Encryption Standard (DES), 168-bit Triple DES (3DES), or up to 256-bit Advanced

Encryption Standard (AES). Cisco PIX Security Appliances can also participate in X.509-based Public Key Infrastructures (PKIs) and provide easy, automated certificate enrollment using the Simple Certificate Enrollment Protocol (SCEP)—another Internet standard that Cisco Systems helped pioneer.

Remote-access users can be authenticated against the internal user ID/password database on the Cisco PIX security appliance itself (which also integrates with Kerberos [Windows Active Directory], Lightweight Directory Access Protocol [LDAP], and RSA SecurID backend systems), or via an external source using TACACS+ or RADIUS. Access to network resources can be strongly authenticated through the Cisco PIX security appliance’s local user database or through integration with enterprise databases, either directly using TACACS+/RADIUS or indirectly with Cisco Secure Access Control Server (ACS). Additionally, Cisco PIX Security Appliances support dynamic downloading and enforcement of access control lists (ACLs) on a per-user basis, upon user authentication with the device. Cisco PIX Security Appliances support a wide range of VPN clients, from Cisco VPN Client to the Microsoft embedded PPTP clients, L2TP VPN clients, and clients for mobile personal digital assistant (PDA) devices.

Certain Cisco PIX models have integrated hardware VPN acceleration capabilities. The Cisco VPN Accelerator Card+ (VAC+) delivers up to 425 Mbps of DES, 3DES, or AES IPsec encryption throughput. Well beyond full-duplex OC-3 line rates, the Cisco PIX security appliance with VAC+ provides excellent price and performance for small to very large enterprise-class site-to-site aggregation. Moreover, it supports up to 2000 encrypted tunnels for mixed VPN environments that have both site-to-site and remote-access VPN requirements. These performance features, along with upgradable encryption accelerators and LAN interfaces, make Cisco PIX Security Appliances some of the most scalable, upgradable, and cost-effective central-site VPN and security solutions on the market. This high level of modularity provides unmatched investment protection. Individual components of the solution can be upgraded as requirements grow, helping customers avoid costly upgrades of the entire chassis to enable new features or performance levels.

Table 4 summarizes the crypto performance of each Cisco PIX security appliance model (using 3DES and AES-128 with 1400-byte packets).

Table 4. Cisco PIX Security Appliance IPsec Performance

Model	Maximum Site-to-Site and Remote User Tunnels	3DES Performance	AES-128 Performance
Cisco PIX 501	10	3 Mbps	4.5 Mbps
Cisco PIX 506E	25	15 Mbps	30 Mbps
Cisco PIX 515E with VAC+	2000	130 Mbps	130 Mbps
Cisco PIX 525 with VAC+	2000	145 Mbps	135 Mbps
Cisco PIX 535 with VAC+	2000	425 Mbps	495 Mbps

Cisco PIX Security Appliances provide up to 16 levels of customizable administrative roles so that enterprises can grant administrators and operations personnel the appropriate level of access to each device (for example, monitoring-only, read-only access to the configuration, VPN configuration only, or firewall configuration only).

Administrators can choose from products that meet their operational requirements for remotely configuring, monitoring, and troubleshooting Cisco PIX Security Appliances. Administrators can manage Cisco PIX Security Appliances using a convenient CLI through a variety of methods, including Telnet, SSH, or out-of-band via a console port. Alternatively, Cisco ASDM, an easy to use, Web-based device configuration tool embedded within the appliances, lets users graphically set up, configure, and monitor their Cisco PIX Security Appliances without requiring extensive knowledge of the CLI. In addition, a wide range of informative, real-time, and historical reports provides critical insight into usage trends, performance baselines, and security events. Cisco PIX Security Appliances also include robust “auto update” capabilities, a set of revolutionary secure remote-management services that help keep device configurations and software images up to date. For large-scale deployments, Cisco PIX Security Appliances are supported by several Cisco network management applications, including CiscoWorks VPN/Security Management Solution (VMS), Cisco ISC, and a variety of solutions from Cisco AVVID partners.

CISCO IOS VPN SECURITY ROUTERS AND CISCO CATALYST SWITCHES

The Cisco IOS VPN security routers and Cisco Catalyst switches are the most widely deployed and most diverse family of VPN solutions in the industry today. Based on Cisco IOS Software, these solutions deliver the leading VPN services required for the most demanding and complex VPN deployments. With Cisco IOS Software, organizations can 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**—a security-specific option for Cisco IOS Software—combines the richest VPN feature set available for site-to-site VPNs, with state-of-art firewall, intrusion prevention, and extensive Cisco IOS capabilities, including QoS, multiprotocol, multicast, and advanced routing support.

Cisco VPN security routers and switches represent the best options for customers of all sizes that are looking to take advantage of their existing network infrastructures to deploy VPNs and security, while integrating all services in a single device, and with the widest selection of WAN and LAN interfaces.

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

Figure 4. Cisco IOS VPN Security Portfolio

Teleworkers/SOHO	Small Branch	Medium-Sized Branch	Enterprise Branch	Enterprise Edge	Enterprise Headquarters Data Center
 Cisco 830	 Cisco 1760	 Cisco 2600XM Cisco 2691	 Cisco 3700	 Cisco 7301	 Cisco Catalyst 6500 Cisco 7600
 Cisco SOHO 90	 Cisco 1700			 Cisco 7200	
 Cisco 800 Series ISR	 Cisco Series 1800 ISR	 Cisco 2800 Series ISR	 Cisco 3800 Series ISR		

Note: The figure above provides general guidelines. Network environments should be scaled on application requirements, not solely on the size of the network.

** The Cisco Advanced Security feature set has been introduced in Cisco IOS Software Release 12.3 as part of a new Cisco IOS packaging strategy that simplifies Cisco IOS Software feature sets. Prior to Cisco IOS Software Release 12.3, Cisco IOS Firewall was bundled in the Cisco IOS Firewall feature set. For more details on the new Cisco IOS packaging, please visit: <http://www.cisco.com/warp/public/732/releases/packaging/docs/pb.pdf>

The rich Cisco IOS feature sets incorporate advanced VPN features such as:

- **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 maximum uptime of mission-critical applications.
- **AES**, the latest industry encryption standard, provides stronger and faster encryption (128-, 192-, and 256-bit).
- **Dynamic Multipoint VPN (DMVPN)** enables autoprovisioning of site-to-site IPSec VPNs, combining three Cisco IOS Software features: Next-Hop Routing Protocol (NHRP), multipoint generic routing encapsulation (mGRE), and IPSec VPN. This combination eases the provisioning challenges for customers and provides secure connectivity between all locations. DMVPN dynamically discovers remote locations using standard routing protocols, and then automatically enables IPSec VPN in a multipoint meshed design. It significantly reduces the configuration complexities confronted by today's customers.
- **IPSec and Multiprotocol Label Switching (MPLS)** integration enables service providers to map IPSec sessions directly into an MPLS VPN. This solution can be deployed on collocated edge routers that are connected to a Cisco IOS Software MPLS provider-edge network, which can include Cisco 7200, 7301, 7500, MGX 8800, 10000, or 12000 series routers. This approach enables the service provider to securely extend its VPN service beyond the boundaries of the MPLS network by using the public IP infrastructure that securely connects enterprise customers' remote offices, telecommuters, and mobile users from anywhere to the corporate network. By extending the MPLS footprint into the Internet or partner networks, a service provider can offer its enterprise customers a more comprehensive portfolio of end-to-end VPN services. Cisco further extends the MPLS solution into the customer edge router with support of multi-VPN routing and forwarding (VRF) in a single router, extending limited MPLS capabilities to customer edge routers. Multi-VRF allows a customer edge router to maintain separate VRF tables in order to extend the privacy and security of an MPLS VPN to a branch office, rather than just at the provider edge router node.
- **VPN hardware modules for Cisco routers** provide up to 10 times the performance over software-only encryption by offloading the encryption processing from the router central processing unit (CPU).

For further flexibility and cost savings, Cisco offers VPN security router bundles based on the Cisco 1700, 1841, 2600XM, 2691, 2800, 3700, 3800, 7200, and 7301 multiservice router platforms. A comprehensive list of router security bundles can be found at <http://www.cisco.com/go/securitybundles>. These are ideal solutions for small and medium-sized offices—they allow customers to use a single part number when ordering a Cisco router with all the necessary Cisco VPN and security components at a reduced price compared to ordering each component separately. Optional modules can be added to each Cisco VPN bundle as needed (except for the Cisco 7301, which has its one slot filled by the VPN Acceleration Module 2 [VAM2] or VAM2+); however, all bundles include the selected router platform, a Cisco VPN hardware card, additional memory, and the Cisco IOS Software to run IPSec 3DES or AES encryption and Cisco IOS Firewall with intrusion detection system (IDS). In addition, the Cisco 2600XM, 2800, 3700, and 3800 series now have advanced security network modules available for URL filtering and hardware-based IDSs.

Cisco also offers the Cisco Catalyst 6503 and 6506 IPSec VPN systems—two bundles that include the Cisco IPSec VPN Services Module (VPNSM) and provide unmatched flexibility and integration for data centers, enterprise headends, and distribution points. The 1.9-Gbps Cisco Catalyst 6503 IPSec VPN system has one open slot for flexible I/O options. The integration of the high-performance Cisco IPSec VPNSM with the Cisco Catalyst 6503 creates a flexible, high-performance VPN solution in campus and WAN edge VPN deployment scenarios. The Cisco Catalyst 6506 IPSec VPN system delivers the same 1.9-Gbps IPSec VPN performance, with four open slots to provide additional flexibility, redundancy, and the addition of high-density I/O or other service options. The open slots in both bundles can be filled with other advanced security services modules, such as the Firewall Services Module (FWSM), the Intrusion Detection Module (IDS-2), and the Network Analysis Module (NAM-1 and NAM-2). This modular approach allows customers to take advantage of the existing switching and routing infrastructure at a low cost, while obtaining the highest performance available in the industry.

Table 5 shows the VPN performance of different Cisco IOS router platforms.

Table 5. VPN Performance of Cisco IOS Routers

Cisco VPN Security Router	Maximum Tunnels	Maximum 3DES Throughput	Maximum AES Throughput
Cisco SOHO 90	8	1 Mbps	–
Cisco 830	10	7 Mbps	2 Mbps
Cisco 850 Series ISR	5	8 Mbps	8Mbps
Cisco 870 Series ISR	10	30Mbps	30Mbps
Cisco 1700 with VPNSM	100	15 Mbps	–
Cisco 1800 Series Fixed ISR	50	40Mbps	40Mbps
Cisco 1841 with Onboard VPN	100	45 Mbps	45 Mbps
Cisco 1841 with AIM-VPN/BPII-PLUS	800	95 Mbps	95 Mbps
Cisco 2600XM with AIM-VPN/EPII-PLUS	800	22 Mbps	22 Mbps
Cisco 2691 with AIM-VPN/EPII-PLUS	800	150 Mbps	150 Mbps
Cisco 2801 with Onboard VPN	150	50 Mbps	50 Mbps
Cisco 2801 with AIM-VPN/EPII-PLUS	1500	100 Mbps	100 Mbps
Cisco 2811 with Onboard VPN	200	55 Mbps	55 Mbps
Cisco 2811 with AIM-VPN/EPII-PLUS	1500	130 Mbps	130 Mbps
Cisco 2821 with Onboard VPN	250	56 Mbps	56 Mbps
Cisco 2821 with AIM-VPN/EPII-PLUS	1500	140 Mbps	140 Mbps
Cisco 2851 with Onboard VPN	300	66 Mbps	66 Mbps
Cisco 2851 with AIM-VPN/EPII-PLUS	1500	145 Mbps	145 Mbps
Cisco 3700 with AIM-VPN/HPII-PLUS	2000	190 Mbps	190 Mbps
Cisco 3825 with Onboard VPN	500	170 Mbps	170 Mbps
Cisco 3800 with Onboard VPN	700	180 Mbps	180 Mbps
Cisco 3800 with AIM-VPN/HPII-PLUS	2500	185 Mbps	185 Mbps
Cisco 3825 with AIM-VPN/EPII-PLUS	2000	175 Mbps	175 Mbps
Cisco 3845 with Onboard VPN	700	180 Mbps	180 Mbps
Cisco 3845 with AIM-VPN/HPII-PLUS	2500	185 Mbps	185 Mbps
Cisco 7200VXR NPE-G1 with a Single SA-VAM2+	5000	280 Mbps	280 Mbps
Cisco 7301 with SA-VAM2+	5000	379 Mbps	379 Mbps
Cisco Catalyst 6500/7600 with a Single VPNSM	8000	1.9 Gbps	–

* Up to 10 VPNSMs can be installed in the same chassis, providing an unmatched 14 Gbps of VPN capacity per chassis.

Cisco IOS VPN security routers and Cisco Catalyst switches can be managed using a convenient CLI through a variety of methods, including Telnet, SSH v2.0, or out-of-band via a console port. Alternatively, Cisco IOS routers can be configured and monitored using Cisco SDM, an intuitive and secure Web-based device management tool embedded within Cisco IOS access routers. Cisco SDM simplifies device and security configuration through smart wizards to enable customers to quickly and easily deploy, configure, and monitor VPNs without requiring extensive knowledge of the Cisco IOS CLI. Cisco IOS routers can also be configured and monitored using tools available from Cisco AVVID partners.

CISCO SECURITY MANAGEMENT SOLUTIONS

In addition to the embedded device managers on Cisco VPN security solutions, Cisco provides standalone security management applications for customers looking to manage devices beyond those that the embedded device managers are designed for.

For customers looking for comprehensive security management, policy administration, monitoring, and analysis for Cisco VPN security solutions, Cisco provides CiscoWorks VMS, an integral part of the SAFE Blueprint from Cisco that protects the productivity of organizations by combining Web-based tools for configuring, monitoring, and troubleshooting VPNs, firewalls, and network- and host-based IDS/IPSs. CiscoWorks VMS delivers VPN configuration management, firewall management, surveillance, device inventory, and software version management features from a single management console.

Customers looking to offer VPN managed services built on Cisco VPN security solutions, can take advantage of the Cisco IP Solution Center (ISC). Cisco ISC implements a business-centric, policy-level management model that allows customers to define high-level security policies, while the application of those policies to specific network devices is offloaded to the Cisco ISC software. The Cisco ISC Security Management module provides full support for the provisioning and management of LAN-to-LAN VPN, remote-access VPN, EZ VPN and DMVPN, firewall, NAT, and QoS technologies for numerous Cisco security devices.

Complementing the above security management applications, Cisco offers the CiscoWorks Security Information Management Solution (SIMS). With CiscoWorks SIMS, customers can manage a growing multivendor security infrastructure without increasing the size of existing security staff. CiscoWorks SIMS lets customers normalize, aggregate, correlate, and visualize the thousands of security alerts received every day from security devices and applications. CiscoWorks SIMS is available for ordering as a software-only option that provides the flexibility to implement a multitier server architecture, which is suitable for larger deployments, and as an appliance option, which consists of the CiscoWorks SIMS preinstalled on the Cisco 1160 hardware solution platform.

PRODUCT ORDERING INFORMATION

Table 6 includes product numbers for Cisco IOS VPN security routers, Cisco VPN 3000 Series concentrators, Cisco PIX Security Appliances, and IPSec VPN services modules for Cisco Catalyst 6500 Series switches and 7600 Series routers. A comprehensive list of router security bundles can be found at <http://www.cisco.com/go/securitybundles>.

Table 6. Part Numbers and Descriptions

Product Number	Description
CISCOSOHO91-K9	Cisco SOHO 91 Ethernet Router
CISCOSOHO96-K9	Cisco SOHO 96 ADSL over ISDN router
CISCOSOHO97-K9	Cisco SOHO 97 ADSL router
CISCO831-K9	Cisco 831 Ethernet router
CISCO836-K9	Cisco 836 ADSL over ISDN router
CISCO837-K9	Cisco 837 ADSL router
CISCO1710-VPN-M/K9	Dual-Ethernet security router VPN/FW/IDS; 16 MB Flash, 64 MB DRAM
CISCO1711-VPN/K9	Cisco 1711 security access router with integrated 4-port switch, 10/100BASE-TX for WAN and analog modem backup
CISCO1712-VPN/K9	Cisco 1712 security access router with integrated 4-port switch, 10/100BASE-TX for WAN and ISDN S/T backup
CISCO1721-VPN/K9	Cisco 1721 VPN bundle with VPN module, 64 MB DRAM, IP Plus/FW/3DES
CISCO1751-VPN/K9	Cisco 1751 VPN bundle with VPN module, 64 MB DRAM, IP Plus/FW/3DES
CISCO1760-VPN/K9	Cisco 1760 VPN bundle with VPN module, 64 MB DRAM, IP Plus/FW/3DES
CISCO1760-V3PN/K9	Cisco 1760 VPN bundle with VPN module, 96 MB DRAM, IP Plus/VOX/FW/3DES

Product Number	Description
CISCO1841-SEC/K9	Cisco 1841 security bundle with Advanced Security Cisco IOS Software
CISCO1841-HSEC/K9	Cisco 1841 enhanced security bundle with AIM-VPN BP11-PLUS, Advanced IP Cisco IOS Software
CISCO2611XM-2FE/VPN/K9	Cisco 2611XM/VPN bundle, AIM-VPN/BP11/2FE/IOS FW/IPSec 3DES, 128 MB DRAM
CISCO2621XM-2FE/VPN/K9	Cisco 2621XM/VPN bundle, AIM-VPN/BP11/2FE/IOS FW/IPSec 3DES, 128 MB DRAM
CISCO2651XM-2FE/VPN/K9	Cisco 2651XM/VPN bundle, AIM-VPN/BP11/2FE/IOS FW/IPSec 3DES, 128 MB DRAM
CISCO2691-VPN/K9	Cisco 2691 VPN bundle, AIM-VPN/EP11-PLUS FW/IPSEC 3DES, 128 MB DRAM
CISCO2801-SEC/K9	Cisco 2801 security bundle with Advanced Security Cisco IOS Software
CISCO2811-SEC/K9	Cisco 2811 security bundle with Advanced Security Cisco IOS Software
CISCO2821-SEC/K9	Cisco 2821 security bundle with Advanced Security Cisco IOS Software
CISCO2851-SEC/K9	Cisco 2851 security bundle with Advanced Security Cisco IOS Software
CISCO2801-HSEC/K9	Cisco 2801 enhanced security bundle with AIM-VPN EP11-PLUS, Advanced IP Cisco IOS Software
CISCO2811-HSEC/K9	Cisco 2811 enhanced security bundle with AIM-VPN EP11-PLUS, Advanced IP Cisco IOS Software
CISCO2821-HSEC/K9	Cisco 2821 enhanced security bundle with AIM-VPN EP11-PLUS, Advanced IP Cisco IOS Software
CISCO2851-HSEC/K9	Cisco 2851 enhanced security bundle with AIM-VPN EP11-PLUS, Advanced IP Cisco IOS Software
CISCO2801-V3PN/K9	Cisco 2801 V3PN bundle with AIM-VPN EP11-PLUS, PVDM2-8, Advanced IP Cisco IOS Software, 64 MB Flash, 256 MB DRAM
CISCO2811-V3PN/K9	Cisco 2811 V3PN bundle with AIM-VPN EP11-PLUS, PVDM2-16, Advanced IP Cisco IOS Software, FL-SRST-36, 64 MB Flash, 256 MB DRAM
CISCO2821-V3PN/K9	Cisco 2821 V3PN bundle with AIM-VPN EP11-PLUS, PVDM2-32, Advanced IP Cisco IOS Software, FL-SRST-48, 64 MB Flash, 256 MB DRAM
CISCO2851-V3PN/K9	Cisco 2851 V3PN bundle with AIM-VPN EP11-PLUS, PVDM2-48, Advanced IP Cisco IOS Software, FL-SRST-72, 64 MB Flash, 256 MB DRAM
CISCO3725-VPN/K9	Cisco 3725 VPN bundle, AIM-VPN/EP11-PLUS IOS FW/IPSEC 3DES, 128 MB DRAM
CISCO3745-VPN/K9	Cisco 3745 VPN bundle, AIM-VPN/HP11-PLUS IOS FW/IPSEC 3DES, 128 MB DRAM
CISCO3825-SEC/K9	Cisco 3825 security bundle with Advanced Security Cisco IOS Software
CISCO3845-SEC/K9	Cisco 3845 security bundle with Advanced Security Cisco IOS Software
CISCO3825-HSEC/K9	Cisco 3825 enhanced security bundle with AIM-VPN EP11-PLUS, Advanced IP Cisco IOS Software
CISCO3845-HSEC/K9	Cisco 3845 enhanced security bundle with AIM-VPN HP11-PLUS, Advanced IP Cisco IOS Software
CISCO3825-V3PN/K9	Cisco 3825 V3PN bundle with AIM-VPN HP11-PLUS, PVDM2-64, FL-SRST-168, Advanced IP Cisco IOS Software, 64 MB Flash, 256 MB DRAM
CISCO3845-V3PN/K9	Cisco 3845 V3PN bundle with AIM-VPN HP11-PLUS, PVDM2-64, FL-SRST-240, Advanced IP Cisco IOS Software, 64 MB Flash, 256 MB DRAM
CISCO7206VXR400/2+VPNK9	Cisco 7206VXR, NPE-400, 2 10/100 Fast Ethernet I/O controller, VAM2+, 512 MB system memory, 64 MB Flash, single AC power supply, Cisco IOS Software with IP FW/IDS IPSec 3DES (168-bit)
CISCO7206VXRG1/2+VPNK9	Cisco 7206VXR, NPE-G1 with 3 onboard 10/100/1000 Ethernet interfaces, VAM2+, 512 MB system memory, 64 MB Flash, single AC power supply, Cisco IOS Software with IP FW/IDS IPSec 3DES (168-bit)
CISCO7301/2+VPNK9	Cisco 7301 with 3 fixed 10/100/1000 Ethernet interfaces, VAM2+, 512 MB system memory, 64 MB Flash, single AC power supply, Cisco IOS Software with IP FW/IDS IPSec 3DES (168-bit)
CISCOVPN3002-BUN-K9	Cisco VPN 3002 Hardware Client; includes hardware, software, and U.S. power cord
CISCOVPN3002-8E-BUN-K9	Cisco VPN 3002 Hardware Client; includes 8-port switch, hardware, software, and U.S. power cord
CISCOVPN3005-E/FE	Cisco VPN 3005 Concentrator with two 10/100 Ethernets; 100 users @ 4 Mbps
CISCOVPN3015-NR-BUN	Cisco VPN 3015 Concentrator with three 10/100 Ethernets; 100 users @ 4 Mbps
CISCOVPN3020E-RDBUN-K9	Redundant Cisco VPN 3020 Concentrator with latest software and 2 U.S. power cords, 2 SEP-Es, 2 power supplies, for 750 users

Product Number	Description
CISCOVPN3030E-RDBUN-K9	Redundant Cisco VPN 3030 Concentrator with latest software and 2 U.S. power cords, 2 SEP-Es (AES support), 2 power supplies; upgradable to Cisco VPN 3060 Concentrator
CISCOVPN3060E-RDBUN-K9	Redundant Cisco VPN 3060 Concentrator with latest software and 2 U.S. power cords, 4 SEP-Es (AES support), 2 power supplies
CISCOVPN3080E-RDBUN-K9	Redundant Cisco VPN 3080 Concentrator with latest software and 2 U.S. power cords, 4 SEP-Es (AES support), 2 power supplies
WS-SVC-IPSec-1	IPSec VPN Services Module for the Cisco Catalyst 6500 Series and Cisco 7600 Series
WS-CISCO6503-IPSec-K9	Cisco Catalyst 6503 VPN system: Cisco Catalyst 6503 chassis, Supervisor Engine 2 (512 MB memory), MSFC2, integrated dual gigabit interface converter (GBIC), VPN services module, and single AC power supply with one open slot for expansion

All part descriptions, part numbers, and prices of Cisco products can be accessed using the online Cisco Pricing Tool at <http://www.cisco.com/cgi-bin/front.x/pricing>.

The Cisco Pricing tool requires a user name and password. If you are not already registered, go to <http://www.cisco.com/register> and follow the instructions. After you have registered, you will be able to access the Pricing Tool.

ADDITIONAL INFORMATION

For more information, please visit the following links:

Cisco router security: <http://www.cisco.com/go/routersecurity>

Cisco router security bundles: <http://www.cisco.com/go/securitybundles>

Cisco IPSec VPN: <http://www.cisco.com/go/ipsec>

Cisco VPN 3000 Series concentrators: http://www.cisco.com/warp/public/cc/pd/hb/vp3000/prodlit/vpn3k_ov.pdf

Cisco IPSec VPN services modules: http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/ps4221/prodlit/vpns_m_ds.pdf

Cisco ASA 5500 Series adaptive security appliances: <http://www.cisco.com/go/asa>

Cisco PIX Security Appliances: <http://www.cisco.com/go/pix>

Cisco Security Device Manager: <http://www.cisco.com/go/sdm>

CiscoWorks VPN/Security Management Solution: <http://www.cisco.com/en/US/products/sw/cscowork/ps2330/index.html>

Cisco IP Solution Center: <http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/index.html>

CiscoWorks Security Information Management Solution: <http://www.cisco.com/en/US/products/sw/cscowork/ps5209/index.html>

SAFE Blueprint from Cisco: <http://www.cisco.com/go/safe>

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R) 205226.T_ETMG_KM_8.05

