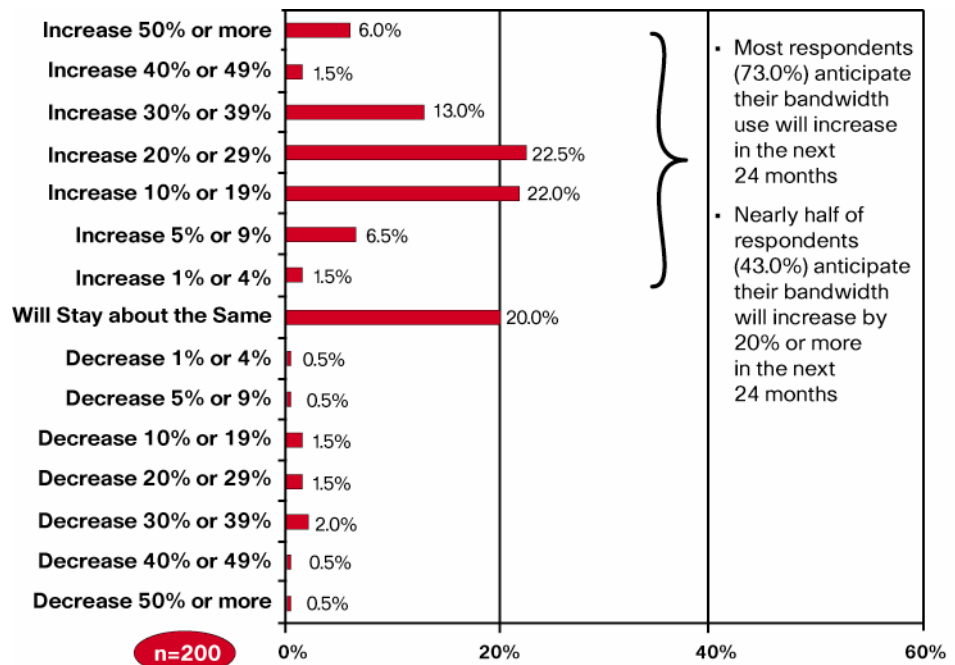


Cisco Catalyst 6500 Series VPN Services Port Adapter: Secure High-Performance Communications for Collaborative Business

Challenge

Enterprises today operate on a more global scale than ever before. Tools such as video telephony, web collaboration, and e-communities applications are growing in maturity and value. Enterprises must keep pace with the bandwidth needs (Figure 1) associated with using these developing communications models to extend WAN and MAN services at any time to users in any location. Today's network is the platform for business interactions across organizations and locations. It is an ongoing challenge to meet the escalating needs of the business while minimizing operational complexity and cost.

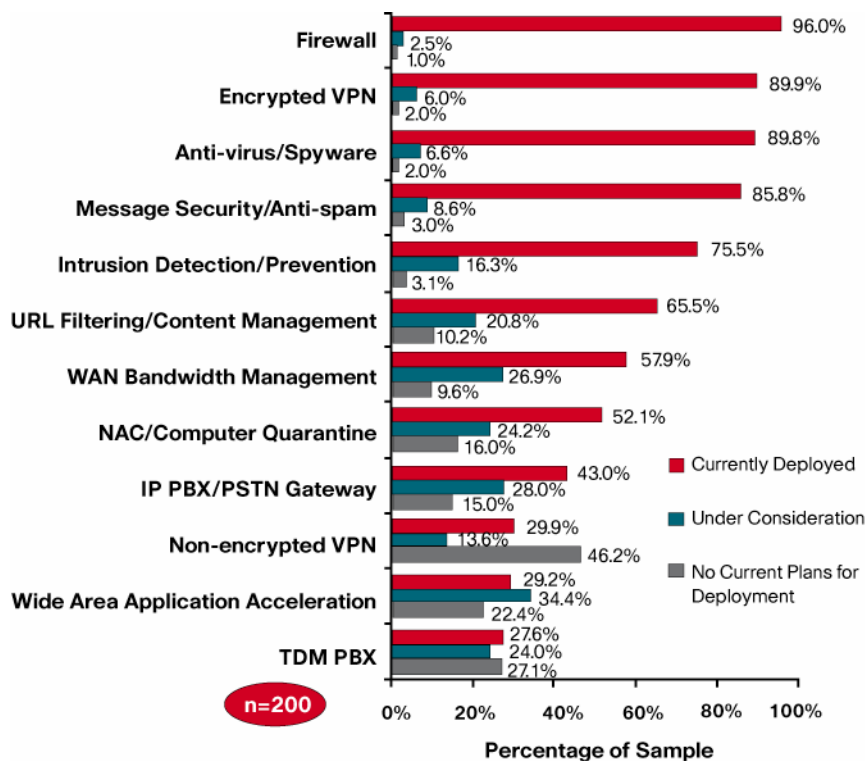
Figure 1. Future Bandwidth Requirements



Source: IDC Research, Enterprise WAN Study, November 2007.

Security technologies must evolve alongside the network to protect company assets. Whether an organization reaches across the globe or to the other end of a corporate campus, securing all communications is a standard requirement (Figure 2), often driven by federal or industry mandates. Further, it is becoming increasingly critical for organizations to be able to scale encrypted WANs in transport environments supporting 10 Gigabit Ethernet, and more.

Figure 2. Deployed Encrypted VPN



Source: IDC Research, Enterprise WAN Study, November 2007.

Business Benefits

Virtual private networks (VPNs) provide a high level of data security through a combination of encryption and authentication technologies. They allow an organization to dramatically increase the reach of the network without significantly expanding its physical infrastructure.

Securing company communications with IP Security (IPsec) encryption is beneficial for a variety of reasons. IPsec allows organizations to securely:

- Extend campus and branch services to teleworkers and mobile users
- Save money with lower-cost transport services, such as Internet and broadband, compared to private WAN services
- Include a secondary WAN connection for backup or for high-bandwidth, less-critical traffic
- Encrypt existing traditional private WANs (e.g., Frame Relay, ATM, leased line)
- Comply with government and industry regulations such as HIPAA and Sarbanes-Oxley in the United States, and the Basel Agreement in Europe

Cisco Catalyst 6500 Series VPN Solutions

Designed to meet the more demanding requirements of high-speed, collaborative business communications, the Cisco® Catalyst® 6500 Series VPN Services Port Adapter can help ensure secure business collaboration. Integrating the VPN Services Port Adapter with a Cisco Catalyst switch creates a flexible, high-performance VPN solution in campus and WAN edge deployment scenarios while providing additional flexibility, redundancy, and high-density I/O or other service options. The open slots in the Cisco Catalyst 6500 Series Switches can accommodate other advanced security services modules, such as the Intrusion Detection System Module (IDSM-2)

and Network Analysis Modules (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.

The Cisco VPN Services Port Adapter supports next-generation VPN technologies with system bandwidths of 5 to 8 Gbps in a modular, flexible, and scalable form factor. When used with the Cisco Catalyst 6500 Series Services Shared Port Adapter Carrier-600, the VPN Services Port Adapter delivers scalable and cost-effective VPN performance for Cisco Catalyst 6500 Series Switches.

The Cisco VPN Services Port Adapter supports the complete range of innovative Cisco IPsec VPN solutions, including:

- Standards-based IPsec VPN (point-to-point IPsec)
- Enhanced Easy VPN
- Dynamic Multipoint VPN (DMVPN)
- Group Encrypted Transport VPN (GET VPN)

Standards-Based IPsec VPN

Considered a “no-frills,” site-to-site VPN solution for connecting remote locations to headquarters, standards-based IPsec VPN is generally used for simpler deployments where there are no requirements for dynamic routing, quality of service (QoS), or IP Multicast (Figure 3).

Enhanced Easy VPN

Adding advanced capabilities to the standards-based IPsec VPN, Enhanced Easy VPN eases the administration and management of point-to-point VPNs by actively pushing new security policies from the central headend router to remote sites. Enhanced Easy VPN features integration with a dynamic virtual tunnel interface (VTI) for maximum ease of use and advanced per-user and tunnel-specific capabilities (Figure 3).

Enhanced Easy VPN also supports remote-access IPsec VPN communications for the utmost flexibility. The remote-access feature increases flexibility and enhances productivity by extending the corporate network and applications to the home or other remote locations (Figure 3).

Dynamic Multipoint VPN (DMVPN)

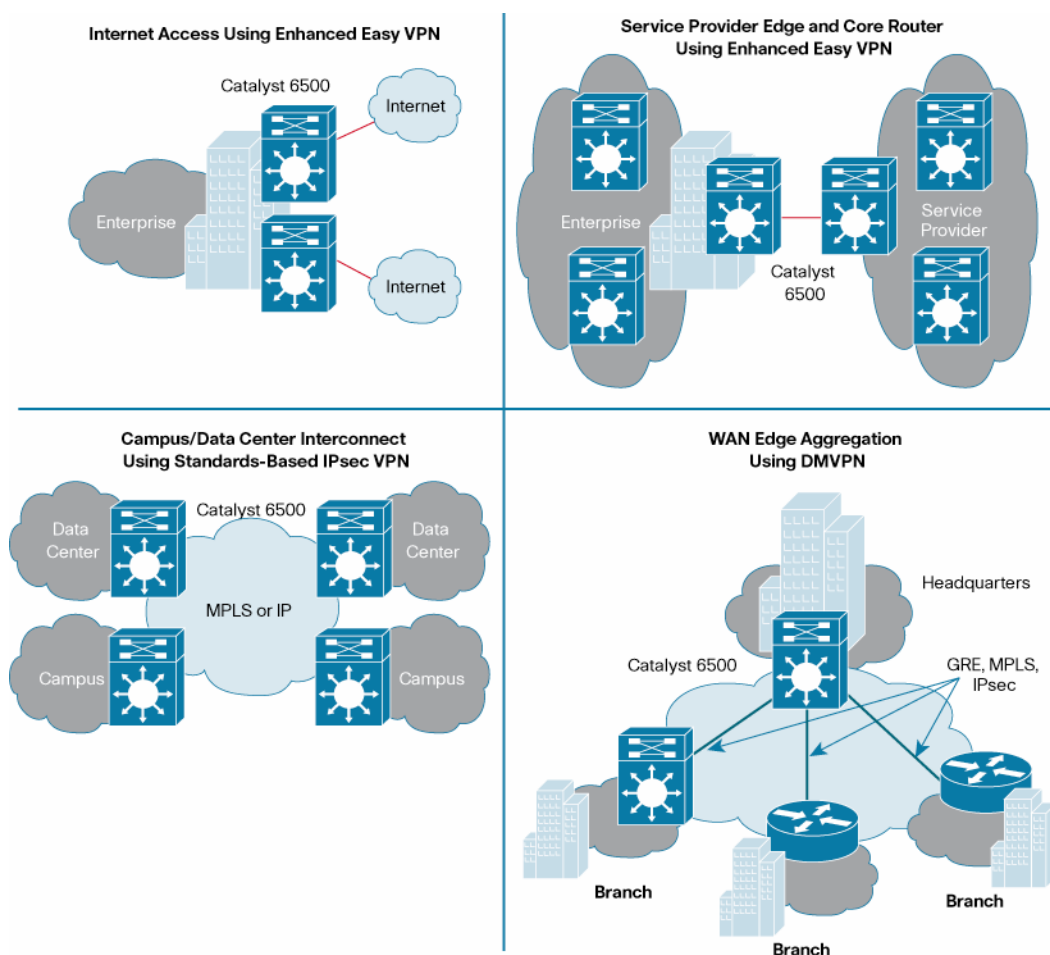
DMVPN is a Cisco innovation for site-to-site VPNs. DMVPN provides a scalable and flexible way to establish virtual full-meshed IPsec connectivity between multiple locations over the public Internet. It features advanced spoke-to-spoke capabilities that enhance the performance of latency-sensitive converged voice and video applications. For the traditional hub-and-spoke model, DMVPN significantly reduces deployment complexity (Figure 3).

Group Encrypted Transport VPN (GET VPN)

GET VPN, another Cisco VPN innovation for private WANs, is based on a new standards-based IPsec security model that is centered on the concept of “trusted” group members. Trusted member routers use a common security methodology, not point-to-point IPsec tunnels. GET VPN simplifies the provisioning and management of VPN and provides optimum bandwidth efficiency while securing communications. Note: GET VPN will be available on the Cisco VPN Services Port Adapter after platform general availability.

For additional information on Cisco IOS® Software-based VPNs, please visit

<http://www.cisco.com/go/vpn>.

Figure 3. Cisco IOS VPN Technology Solutions with Cisco VSPA

Cisco VPN Services Port Adapter Feature and Benefits

Table 1 describes the primary features and benefits of the Cisco VPN Services Port Adapter.

Table 1. Cisco VPN Services Port Adapter Features and Benefits

Feature	Description
High-speed VPN performance*	The VPN Services Port Adapter provides up to 8 Gbps of Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) IPsec throughput.
Scalability	Up to 10 VPN Services Port Adapters can be installed in a system for increased total throughput.
Enhanced QoS support	Features such as pre-encryption egress QoS, shaping to address traffic burstiness, bandwidth control, priority queuing, and queue limit (depth) by packet help to avoid network congestion and improve application performance.
Scalable IPv6 encryption	The VPN Services Port Adapter provides scalable support for multiple-gigabit IPv6 networks.
Compact form factor	Using the Cisco Services SPA Carrier-600, each slot of the Cisco Catalyst 6500 Series Switch supports up to two VPN Services Port Adapters. The half-slot form factor of the VPN Services Port Adapter reduces slot consumption and increases total performance per slot.
Cisco Smart Call Home capability	The VPN Services Port Adapter supports the award-winning Cisco Catalyst 6500 Series Smart Call Home function which offers proactive diagnostics, real-time alerts, and personalized web-based reports on Cisco devices such as the Cisco Catalyst 6500 Series.
Full integration of VPN into the network infrastructure	The VPN Services Port Adapter supports the Cisco Catalyst 6500 Series chassis as well as LAN and WAN interfaces, enabling an integrated security approach to building a VPN in your infrastructure. No separate VPN devices are needed within your campus, intranet, Internet data center, or point of presence (POP).

Feature	Description
Comprehensive VPN features	The Cisco VPN Services Port Adapter provides hardware acceleration for both IPsec and generic routing encapsulation (GRE), comprehensive support of site-to-site IPsec, remote-access IPsec, and certificate authority/public key infrastructure (CA/PKI).
Diverse network traffic types and topologies	Cisco IOS Software supports secure, reliable transport of virtually any type of network traffic, including multiprotocol, multicast, and IP telephony, across the IPsec VPN. Rich routing capabilities enable DMVPNs for meshed and hierarchical network topologies, maximizing deployment flexibility while minimizing operational complexity and cost.
VPN resiliency and high availability	The VPN Services Port Adapter provides superior VPN resiliency and high availability through features such as routing over IPsec tunnels, dead peer detection (DPD), Hot Standby Router Protocol (HSRP) with reverse route injection (RRI), and intrachassis and interchassis stateful failover for both IPsec and GRE.
DMVPN	DMVPN enables a dynamic partial- or full-mesh site-to-site VPN while greatly simplifying the management of large VPN deployments. This feature creates dynamic spoke-to-spoke tunnels without requiring preconfiguration on the spoke routers, and allows for the addition or removal of spoke routers without any change to other spoke configurations. This improves network performance by reducing latency and jitter while optimizing main-office bandwidth use. DMVPN includes advanced voice-over-IP (VoIP) support for full-service branch deployments.
Virtual routing and forwarding (VRF)-aware IPsec VPN	VRF-aware IPsec features map IPsec tunnels to VRF instances to provide network-based IPsec VPNs, and the integration of IPsec with MPLS VPNs. This feature helps service providers, large enterprises, and educational institutions build secure, scalable, and virtualized VPN services across their network infrastructures.
VPN and network infrastructure management	Comprehensive systems help manage solutions, from a single platform to hundreds or even thousands of platforms. Element management uses the Cisco Router Management Center and VPN monitoring components of the CiscoWorks VPN/Security Management Solution (VMS). These features allow comprehensive end-to-end VPN management of numerous platforms throughout your network using the Cisco IP Solution Center for service provider and large enterprise VPN, security, and QoS.

*Using large packets

Conclusion

VPNs provide high levels of security through encryption and authentication, protecting data from unauthorized access. Cisco VPN solutions are easy to provision, and deliver flexibility and scalability by enabling the quick addition of new sites or users. As a result, organizations can dramatically increase the reach of their networks without significantly expanding their infrastructures.

Cisco Catalyst 6500 Series IPsec VPNs now support a range of advanced services that combine flexibility with performance and resiliency. High availability for multigigabit IPsec, no penalty for QoS, and a clear separation of control, data, and input/output planes set this offering apart from others in its class. The VPN Services Port Adapter for the Cisco Catalyst 6500 Series supports next-generation VPN technologies. Its modular design provides the required flexibility for high-performance IPsec VPNs. It brings true integration and performance to the wide range of Cisco IOS VPN technologies.



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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0807R)