Cisco Catalyst 6500 Series VPN Services Port Adapter

Product Overview

Today's businesses operate less on local/country or even regional levels, and more on a global level. With greater and more ubiquitous connectivity also comes greater opportunity for enterprises to discover new ways to connect and collaborate. New tools such as video telephony, web collaboration, e-communities, information sharing, and the like are growing in maturity and value. At the heart of these communications and collaboration models is the network, which serves as the primary conduit of business interactions and services among various sites, evolving at a greater speed. As the network evolves and grows, security technologies should evolve to transparently protect the data and various applications in the network.

The Cisco® VPN Services Port Adapter (VSPA) is the next-generation VPN module designed to support next-generation VPN technologies with system bandwidths of 8 Gbps in a modular, flexible, and scalable form factor (refer to Figure 1). The Cisco VSPA requires the Cisco Catalyst® 6500 Series Services SPA Carrier-600 (SSC-600) to operate in the Cisco Catalyst 6500 Series Switches. Each SSC-600 module takes up one slot in a Cisco Catalyst 6500 Series Switch and can support up to two Cisco VPN Services Port Adapters. The Cisco VSPA, accompanied with the SSC-600, delivers scalable and cost-effective VPN performance for Cisco Catalyst 6500 Series Switches.

Figure 1. Cisco VSPA

Although the Cisco VSPA does not have physical WAN or LAN interfaces, it takes advantage of the breadth of LAN and WAN interfaces in the Cisco Catalyst 6500 Series Switches, making it very attractive for enterprises deploying the Cisco Catalyst 6500 Series Switch.

Primary VPN features delivered by the Cisco VSPA include:

- **Security integrated into network infrastructure:** The Cisco VSPA supports IPsec VPN encryption in the Cisco Catalyst 6500 Series Switches. When VPNs are integrated into these infrastructure platforms, the network can be secured without extra overlay equipment or network alterations. Furthermore, the broad range of LAN and WAN interfaces, as well as the entire line of security services modules (VPN, firewall, network anomaly detection, intrusion detection and prevention, content services, Secure Sockets Layer [SSL], and wireless LAN) can now be used together within the same platform.

- **Support for industry-leading encryption technology:** In addition to Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES), the Cisco VSPA also supports Advanced Encryption Stanced (AES) 192 and AES 256, the latest standard in encryption technology demanded by most government agencies and the leading financial institutions in the most secure network environments.
- **High performance:** Using the latest in encryption hardware acceleration modules, each Cisco VSPA can deliver up to 8 Gbps of AES traffic at large packet sizes and 7 Gbps at average packet sizes as defined by internet mix traffic (IMIX) traffic.
- **Modular design and scalability:** The Cisco VSPA can terminate up to 16,000 site-to-site or remote-access IPsec tunnels simultaneously and can establish those tunnels at up to 65 new tunnels per second. Taking advantage of modular architecture, each slot of the Cisco Catalyst 6500 can support up to 2 Cisco VSPAs, and up to 10 Cisco VSPAs can be combined in a single chassis. Additionally, the half-slot form factor of the Cisco VSPA allows the customer to reduce slot consumption, potentially reducing cost while enhancing per-slot and overall system encryption performance.
- **Enhanced quality of service (QoS):** The VSPA is designed to handle preencryption QoS configured on IPsec tunnel interfaces and provides priority, bandwidth, and traffic shaping services. Because the VSPA does not rely on the physical interface for QoS classification of outbound packets, packets are less likely to be dropped because of antireplay issues.
- **Scalable IPv6 encryption:** Support for multigigabit IPv6 networks based on Static Virtual Tunnel Interfaces (sVTIs).
- **Engine sharing:** Physical ports can terminate multiple tunnels on multiple VSPAs simultaneously.
- **VPN resiliency and high availability:** Using innovative features such as stateful failover for IPsec and generic routing encapsulation (GRE), Hot Standby Router Protocol with Reverse Route Injection (HSRP+RRI), Dead Peer Detection (DPD), and support of dynamic routing updates over site-to-site tunnels, the Cisco VSPA provides superior VPN resiliency and high availability.
- **Advanced security services:** Adding strong encryption, authentication, and integrity to network services is easy with the Cisco VSPA. Secured campus and provider-edge VPN applications, including integrated data, voice, and video-enabled VPN; storage area networks; and integration of IPsec and MPLS VPNs, are now easily deployable. The Cisco VSPA provides advanced site-to-site and remote-access IPsec services over both LAN and WAN interfaces.

Key Features and Benefits

Table 1 gives the primary features of the Cisco VSPA.

Table 1. Features of Cisco VSPA

Feature	Description
Next-Generation Encryption Technology	In addition to supporting DES and 3DES, the Cisco VSPA supports AES, including all key sizes (128-, 192-, and 256-bit keys). Designed to be the next-generation encryption technology, AES offers the ultimate in IPsec VPN security and interoperability.
High-Speed VPN Performance	High-speed VPN performance provides up to 8 Gbps of AES IPsec throughput and 7 Gbps of IMIX traffic.
Modular Design/Scalability	Up to 10 Cisco Services SPA Carrier-600 modules and 10 Cisco VSPAs in a Cisco Catalyst 6500 chassis.

Feature	Description
Enhanced QoS Support	Enhanced QoS to avoid congestion and improve application performance. • Preencryption QoS ◦ Aggregate tunnel shaper ◦ 8 classes of traffic allowing bandwidth reservation ◦ Low latency queuing (LLQ) for delay-sensitive traffic
Scalable IPv6 Encryption	Scalable support for multiple gigabit IPv6 networks.
Attractive Form Factor	Using the Cisco Services SPA Carrier-600, each slot of the Cisco Catalyst 6500 supports up to two VSPAs. The half-slot form factor of the SPA reduces slot consumption and increases total performance per slot.
Jumbo Frame Support	The Cisco VSPA supports jumbo frames up to 9216 bytes without the need for fragmentation by the supervisor module.
Full Integration of VPN into Network Infrastructure	The Cisco VSPA supports the Cisco Catalyst 6500 Series chassis as well as both 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).
Comprehensive VPN Features	The Cisco VSPA provides hardware acceleration for both IPsec and 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 Dynamic Multipoint VPNs (DMVPNs) for meshed and hierarchical network topologies, maximizing deployment flexibility while minimizing operational complexity and cost.
VPN Resiliency and High Availability	Routing over IPsec tunnels, DPD, HSRP+RRI, and intrachassis and interchassis stateful failover for both IPsec and GRE provide superior VPN resiliency and high availability.
DMVPN	DMVPN helps enable a dynamic partial-mesh or full-mesh site-to-site VPN while greatly simplifying the management of large VPN deployments. This feature helps dynamic spoke-to-spoke tunnel establishment without preconfiguration in the spoke routers and helps enable the VPN to dynamically add or remove spoke routers without any change to other spoke configurations. This improves network performance by reducing latency and jitter while optimizing main-office bandwidth use. This includes advanced voice-over-IP (VoIP) support for full-service branch deployments.
Virtual Routing and Forwarding (VRF)-Aware IPsec VPN	VRF-aware IPsec features help enable mapping of 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.

Product Specifications

Table 2 gives specifications of the Cisco VSPA.

Table 2. Product Specifications

Features	Descriptions
VPN Tunneling	IPsec (RFCs 2401-2411 and 2451)
Encryption	• Encapsulating Security Payload (ESP) • DES • 3DES • AES 128, 192, 256
Authentication	• X.509 digital certificates (RSA signatures) • Encrypted Nonces (RSA encryption) • Preshared keys • Simple Certificate Enrollment Protocol (SCEP) • RADIUS (RFC 2138) • TACACS+
Integrity	Hashed Message Authentication Code with MD5 (HMAC-MD5) and with Secure Hash Algorithm-1 (HMAC-SHA-1) (RFCs 2403 and 2404)
Key Management	Internet Key Exchange (IKE; RFCs 2407-2409) IKE-XAUTH IKE-CFG-MODE

Features	Descriptions
CA/PKI Support	• Entrust • VeriSign • Microsoft • Netscape • IPlanet • Baltimore Technologies
Resiliency and High Availability	• HSRP + RRI • Intrachassis (blade-to-blade) IPsec stateful failover • Interchassis (box-to-box) active/standby IPsec stateless failover • DPD • Dynamic routing across IPsec (see "Routing Protocols" section of this table)
Supervisor Engines	Cisco Catalyst 6500 Series Supervisor Engine 32, 720 Series, or VSS_10G
Supported LAN Interfaces	• Multiport Fast Ethernet • Multiport Fast Ethernet with inline power • Multiport Gigabit Ethernet • 10 Gigabit Ethernet
Supported WAN Interfaces	• Gigabit Ethernet WAN and Enhanced Gigabit Ethernet WAN • Single- and dual-port T3/E3 • Single- and dual-port High-Speed Serial Interface (HSSI) • Multiport T1/E1 • Multichannel T1/T3/E3 • OC-3 ATM single-mode (SM) and multimode (MM) • OC-3 packet over SONET/SDH (POS) SM and MM • OC-12 ATM SM and MM • OC-12 POS SM and MM • OC-48 POS SM • OC-48 POS-Dynamic Packet Transport (DPT) SM
Physical Dimensions	• Length: 5.92 in. (15 cm) • Width: 6.75 in. (17.15 cm) • Height: 1.52 in. (3.9 cm) (double height)

Table 3 gives Regulatory Standards Compliance of the Cisco VSPA.

Table 3. Regulatory Standards Compliance: Safety and EMC

Specification	Description
Regulatory Compliance	Products should comply with CE Markings per directives 2004/108/EC and 2006/95/EC
Safety	• UL 60950 • CAN/CSA-C22.2 No. 60950 • EN 60950 • IEC 60950 • AS/NZS 60950
EMC—Emissions	• 47CFR Part 15 (CFR 47) Class A • AS/NZS CISPR22 Class A • CISPR2 2 Class A • EN55022 Class A • ICES003 Class A • VCCI Class A • EN61000-3-2 • EN61000-3-3 • KN22 Class A • CNS13438 Class A

Specification	Description
EMC—Immunity	• EN50082-1 • EN61000-6-1 • EN55024 • CISPR24 • EN300386 • KN immunity series

Table 4 gives NEBS Compliance and ETSI 300-019 Environmental Requirements.

Table 4. NEBS Compliance and ETSI 300-019 Environmental Requirements

Specification	Description
NEBS Criteria Levels	SR-3580 NEBS level 3 (GR-63-CORE, issue 3, GR-1089 CORE, issue 4)
Verizon NEBS Compliance	Telecommunications Carrier Group (TCG) Checklist
Qwest NEBS requirements	Telecommunications Carrier Group (TCG) Checklist
ATT NEBS Requirements	ATT TP76200 level 3, TP7645 and TCG Checklist
ETSI	• ETS 300 019-1-1, Class 1.2 Storage • ETS 300 019-1-2, Class 2.3 Transportation • ETS 300 019-1-3, Class 3.2 Stationary Use

Ordering Information

To place an order, visit the Cisco Ordering Home Page or refer to Table 5.

Table 5. Ordering Information

Product Name	Part Number
Cisco Catalyst 6500 Series VPN Services Port Adapter	WS-IPSEC-3
Cisco Catalyst 6500 Series Services SPA Carrier-600	WS-SSC-600
Cisco Catalyst 6500 IPsec VSPA Bundle 1 (system only)	WS-IPSEC-SSC600-L1
Cisco Catalyst 6500 IPsec VSPA Bundle 2 (system only)	WS-IPSEC-SSC600-L2
Cisco Catalyst 6504E IPsec VSPA Security System	WS-C6504-E-VPN+-K9
Cisco Catalyst 6506E IPsec VSPA Security System	WS-C6506-E-VPN+-K9
Cisco Catalyst 6509E IPsec VSPA Security System	WS-C6509-E-VPN+-K9
Cisco Catalyst 6513 IPsec VSPA Security System	WS-C6513-VPN+-K9

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco Services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, refer to Cisco Technical Support Services or Cisco Advanced Services.

For More Information

For more information about the Cisco VSPA and the Cisco SPA/SIP portfolio, visit http://www.cisco.com/go/spa or contact your local Cisco account representative.

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 C78-492120-00 08/08