Cisco 7600 Series/Catalyst 6500 Series IPSec VPN Shared Port Adapter

The Cisco® I-Flex design combines shared port adapters (SPAs) and SPA interface processors (SIPs), leveraging an extensible design that enables service prioritization for voice, video and data services. Enterprise and service provider customers can take advantage of improved slot economics resulting from modular port adapters that are interchangeable across Cisco routing platforms. The I-Flex design maximizes connectivity options and offers superior service intelligence through programmable interface processors that deliver line-rate performance. I-Flex enhances speed-to-service revenue and provides a rich set of QoS features for premium service delivery while effectively reducing the overall cost of ownership. This data sheet contains the specifications for the Cisco® 7600 Series/Catalyst® 6500 Series IPSec VPN Shared Port Adapter (Cisco IPSec VPN SPA).

Product Overview

Enterprises and service providers require ubiquitous and secure connectivity to address today's mission-critical high-bandwidth applications. Many enterprises replace their traditional WANs with site-to-site and remote-access VPNs while service providers are offering managed VPN services, including virtualized network-based VPNs. The Cisco IPSec VPN SPA offers next-generation encryption technology as well as a form factor designed to enable a more flexible and scalable network infrastructure (refer to Figure 1).

Figure 1. Cisco IPSec VPN SPA

The Cisco IPSec VPN SPA delivers scalable and cost-effective VPN performance for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers. Using the Cisco 7600 Series/Catalyst 6500 Series Services SPA Carrier-400 (Cisco Services SPA Carrier-400), each slot of the Cisco Catalyst 6500 or Cisco 7600 can support up to two Cisco IPSec VPN SPAs. Although the Cisco IPSec VPN SPA does not have physical WAN or LAN interfaces, it takes advantage of the breadth of LAN and WAN interfaces of each of the platforms.

Key Features and Benefits

Table 1 gives the primary features of the Cisco IPSec VPN SPA.

Table 1. Features of Cisco IPSec VPN SPA

Feature	Description
Next-Generation Encryption Technology	In addition to supporting Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES), the Cisco IPSec VPN SPA supports Advanced Encryption Standard (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 2.5 Gbps of AES and 3DES IPSec throughput with large packets and 1.6 Gbps with Internet mix (IMIX) traffic.
Scalability	Up to 10 Cisco IPSec VPN SPAs can be installed in a system to provide up to 25 Gbps of total throughput, enabling wire-speed secured transport for native 10-Gigabit Ethernet interfaces.
Attractive Form Factor	Using the Cisco Services SPA Carrier-400, each slot of the Cisco Catalyst 6500 or Cisco 7600 supports up to two IPSec VPN SPAs. The half-slot form factor of the SPA reduces slot consumption and increases total performance per slot.
Jumbo-Frame Support	The Cisco IPSec VPN SPA supports jumbo frames up to 9100 bytes without the need for fragmentation by the supervisor module.
Full Integration of VPN into the Network Infrastructure	The Cisco IPSec VPN SPA supports Cisco Catalyst 6500 Series and Cisco 7600 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 IPSec VPN SPA 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 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, dead-peer detection (DPD), Hot Standby Router Protocol (HSRP) plus reverse route injection (RRI), and intra-chassis and inter-chassis 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.
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 (RMC) and VPN monitor 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 (ISC) for service provider and large enterprise VPN, security, and quality of service (QoS).

The features listed above provide the following benefits for enterprises and service providers:

- **Security integrated into network infrastructure:** The Cisco IPSec VPN SPA supports Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers. By integrating VPNs 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 within the same platform.

- **Industry-leading technology:** In addition to DES and 3DES, the Cisco IPSec VPN SPA introduces AES, the new standard in encryption technology demanded by most government agencies and the leading financial institutions in the most secure network environments.
- **High performance:** Each Cisco IPSec VPN SPA can deliver up to 2.5 Gbps of AES and 3DES encrypted data traffic. Additionally, the Cisco IPSec VPN SPA can terminate up to 8000 site-to-site or remote-access IPSec tunnels simultaneously and can set up those tunnels at a rate of up to 60 new tunnels per second. Furthermore, DMVPN helps enable a zero-touch and fully dynamic deployment of IPSec over a hub-and-spoke topology.
- **Scalable form factor:** Taking advantage of the standardized SPA architecture, each slot of the Cisco Catalyst 6500 and Cisco 7600 can support up to 2 Cisco IPSec VPN SPAs. Up to 10 Cisco IPSec VPN SPAs can be combined in a single chassis to provide maximum throughput of 25 Gbps. Additionally, the half-slot form factor of the Cisco IPSec VPN SPA allows the customer to reduce slot consumption, potentially reducing cost while enhancing per-slot and overall system encryption performance.
- **VPN resiliency and high availability:** Using innovative features, such as stateful failover for both IPSec and GRE, HSRP + RRI, DPD, and support of dynamic routing updates over site-to-site tunnels, the Cisco IPSec VPN SPA provides superior VPN resiliency and high availability.
- **Advanced security services:** Adding strong encryption, authentication, and integrity to network services is easy with the Cisco IPSec VPN SPA. Secured campus and provider-edge VPN applications, including integrated data-, voice-, and video-enabled VPN, storage-area networks, and integration of IPSec and Multiprotocol Label Switching (MPLS), VPNs are now easily deployable. The Cisco IPSec VPN SPA provides advanced site-to-site and remote-access IPSec services over both LAN and WAN interfaces.

Product Specifications

Table 2 gives specifications of the Cisco IPSec VPN SPA.

Table 2. Product Specifications

Features	Descriptions
VPN Tunneling	IPSec (RFCs 2401–2411 and 2451)
Encryption	• Encapsulating Security Payload (ESP) • DES • 3DES • AES
Authentication	• X.509 digital certificates (RSA signatures) • Preshared keys • Simple Certificate Enrollment Protocol (SCEP) • RADIUS (RFC 2138) • TACACS+ • Challenge Handshake Authentication Protocol/Password Authentication Protocol (CHAP/PAP; RFC 1994)
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) active/active IPSec stateful failover • Interchassis (box-to-box) active/standby IPSec stateful failover • DPD • Dynamic routing across IPSec (see “Routing Protocols” section of this table)
Network Management	• CiscoWorks VMS and Router MC • Cisco ISC • Secure command-line interface (CLI) using Secure Shell (SSH) Protocol or Kerberized Telnet
Routing Protocols	• Border Gateway Protocol Version 4 (BGPv4) • Routing Information Protocol (RIP) and RIP Version 2 (RIPv2) • Open Shortest Path First (OSPF) • Enhanced Interior Gateway Routing Protocol (EIGRP) and IGRP • Intermediate System-to-Intermediate System (IS-IS)
Supervisor Engines	• Supervisor Engine 2 with Multilayer Switch Feature Card 2 (MSFC2) • Supervisor Engine 720 with policy feature card (PFC)-3A, PFC-3B, or PFC-3BXL
Supported LAN Interfaces	• Multiport Fast Ethernet • Multiport Fast Ethernet with inline power • Multiport Gigabit Ethernet • 10 Gigabit Ethernet (10GE)
Supported WAN Interfaces	• FlexWAN and Enhanced FlexWAN • Optical services module (OSM) and enhanced OSM • 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
Interoperable Services Modules	• Cisco Catalyst 6500 Series Firewall Services Module • Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2 (IDSM-2) • Cisco Catalyst 6500 Series Network Analysis Module (NAM-1 and NAM-2) • Cisco Catalyst 6500 Series SSL Services Module • Cisco Catalyst 6500 Series Content Switching • Cisco Catalyst 6500 /7600 Series Multiprocessor WAN Application Module (MWAM) • Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM)
Physical Dimensions	• Length: 5.92 in. (15 cm) • Width: 6.75 in. (17.15 cm) • Height: 1.52 in. (3.9 cm)—(double height)
Power	25 Watts

Features	Descriptions
Compliance and Agency Approvals	**Safety** • UL 60950 • IEC 60825-1, -2 • IEC 60950 • EN 60950 • EN 60825-1, -2 • CAN/CSA-C22.2 No. 60950-00 • AS/NZS 3260-1993 • 21CFR1040 **EMC** • FCC Part 15 (CFR 47) Class A • ICES-003 Class A • EN55022 Class A • CISPR22 Class A • AS/NZSCISPR Class A • VCCI Class A • EN55024 • EN300 386 • EN50082-1 • EN61000-3-2 • EN61000-3-3 **NEBS and Environmental Standard Compliance** • GR-63-Core NEBS Level 3 • GR-1089-Core NEBS Level 3 • ETSI 300 019 Storage Class 1.1 • ETSI 300 019 Transportation Class 2.3 • ETSI 300 019 Stationary Use Class 3.1

Ordering Information

To place an order, visit the Cisco Ordering Home Page or refer to Table 3.

Table 3. Ordering Information

Product Name	Part Number
Cisco 7600 Series/Catalyst 6500 Series IPSec VPN Shared Port Adapter	SPA-IPSEC-2G
Cisco 7600 Series/Catalyst 6500 Series Services SPA Carrier-400	7600-SSC-400

Service and Support

Cisco Systems® 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 IPSec VPN SPA 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 C78-525386-00 03/09