Virtual Private Network (VPN) Advanced Integration Module (AIM) for the Cisco 1841 Integrated Services Router and Cisco 2800 and 3800 Series Integrated Services Routers

The VPN Advanced Integration Module (AIM) for the Cisco® 1841 Integrated Services Router and Cisco 2800 and 3800 Series Integrated Services Routers optimizes the Cisco Integrated Services Router platforms for virtual private networks in both IP Security (IPSec) and Secure Sockets Layer (SSL) Web and VPN deployments.

Figure 1. Integrated Services Router with the "AIM-VPN/SSL" Module

Cisco Integrated Services Routers deliver advanced security services, including industry-leading VPN for site-to-site and remote-access connectivity. To facilitate robust IPsec VPN deployments such as Dynamic Multipoint VPN (DMVPN) or optimize Cisco IOS® SSL VPN performance, the Cisco VPN and SSL AIM provides hardware encryption acceleration for the Cisco 1841 and Cisco 2800 and 3800 Series routers. (See Figure 1)

The Cisco VPN and SSL AIM provides up to 40 percent better performance for IPsec VPN over the built-in IPsec encryption, and up to twice the performance for SSL VPN encryption. The Cisco VPN and SSL AIM supports all three of these functions in hardware: SSL encryption in hardware, VPN IPsec encryption in hardware using either Data Encryption Standard (DES) or Advanced Encryption Standard (AES), and the IP Payload Compression Protocol (IPPCP) in hardware. Cisco Integrated Services Routers with the Cisco IPsec and SSL VPN AIM are ideal for use in small and medium-sized businesses (SMBs) and small and large enterprise branch offices to connect remote offices, mobile users, and partner extranets. Cisco Integrated Services Routers offer the flexibility to deploy both IPsec and SSL VPN in a single-device solution, thus reducing the total cost of ownership, unlike other vendors' products requiring multiple devices and management systems. In addition, the Cisco IPsec and SSL VPN AIM is designed for service providers, offering highly scalable managed security services with zero-touch deployment ease.

Cisco Integrated Services Routers together with the Cisco IPsec and SSL VPN AIM and the Cisco IOS Advanced Security features offer a rich integrated package of routing, firewall, intrusion-protection, and VPN functions and are an integral component of the Cisco Self-Defending Network.

Table 1 lists the VPN module hardware and features supported by each platform. Table 2 describes the features supported by the Cisco IPsec and SSL VPN AIM. Table 3 describes the benefits of the Cisco IPsec and SSL VPN AIM features.

Table 1. Supported Modules and Features, by Platform

Module Part Numbers	Cisco 1841	Cisco 2801, 2811, 2821, 2851	Cisco 3725	Cisco 3825	Cisco 3745	Cisco 3845	AES and Triple Data Encryption Standard (3DES)	IPPCP	WebVPN SSL Encryption	IPv6 Cryptography in Hardware
AIM-VPN/SSL-1	X						X	X	X	X
AIM-VPN/SSL-2		X					X	X	X	X
AIM-VPN/SSL-3			X	X	X	X	X	X	X	X

Table 2. Supported Features of Cisco IPsec and SSL VPN AIM

Feature	Description
Physical	The Cisco IPsec and SSL VPN AIM fits in any open AIM slot in the Cisco Integrated Services Router.
Platform Support	The Cisco IPsec and SSL VPN AIM supports the Cisco 1841 and the Cisco 2800, 3700, and 3800 Series.
Hardware Prerequisites	An AIM slot for the Cisco 1841 and the Cisco 2800, 3700, and 3800 Series is required.
IPSec Encryption Supported	All modules support IPSec DES and 3DES; Authentication: Rivest, Shamir, and Adelman (RSA) and Diffie Hellman; data integrity: Secure Hash Algorithm 1 (SHA-1) and Message Digest Algorithm 5 (MD5); and DES, 3DES, and AES key sizes: AES128, AES192, and AES256.
Hardware SSL Encryption Supported	Only the Cisco IPsec and SSL VPN AIM in the Cisco 1841 and the Cisco 2800, 3700, and 3800 Series supports SSL VPN encryption.
IPSec Hardware-Based Compression	The Cisco IPsec and SSL VPN AIM uses Layer 3 IPPCP compression.
Software Prerequisites	The Cisco IPsec and SSL VPN AIM uses the Cisco IOS Software with the Advanced Security, Advanced IP, or Advanced Enterprise feature set.
Number of Encryption Modules per Router	The Cisco IPsec and SSL VPN AIM uses one encryption module per router.
Minimum Cisco IOS Software Version Required	The Cisco IPsec and SSL VPN AIM requires Cisco IOS Software Version 12.4(9)T or higher.
Maximum Number of IPSec Encrypted Tunnels	The Cisco IPsec and SSL VPN AIM supports up to 800 tunnels on the Cisco 1841, up to 1500 tunnels on the Cisco 2800 Series, and up to 2000 tunnels on the Cisco 3800 Series. The Maximum Tunnel Scalability test is done with no data passing over the tunnels to only determine maximum number. For site-to-site design, Cisco recommends you consult with your Cisco account team or a Cisco authorized reseller and also review the Cisco DMVPN Design Guide at: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008075ea98.pdf
Maximum Number of Cisco IOS WebVPN SSL VPN Users with VPN and SSL AIM	Only the Cisco IPsec and SSL VPN AIM supports Cisco IOS SSL VPN. On the Cisco 1841 and 2801, it supports 50 users; on the Cisco 2811 and 2821, it supports 100 users; on the Cisco 2851, it supports 150 users; on the Cisco 3725 and 3745, it supports 150 users; and on the Cisco 3825 and 3845, it supports 200 users. The Cisco IOS WebVPN SSL VPN requires the purchase of a user license. (All supported platforms include a two-user demo license at no additional cost.)
Standards Supported	The Cisco IPsec and SSL VPN AIM supports the IPSec Internet Key Exchange (IKE): RFCs 2401 to 2410, 2411, and 2451.

Table 3. Features and Benefits of the Cisco IPsec and SSL VPN AIM

Feature	Benefit
High Overhead IPSec Processing from the Main Processor	Reserves critical processing resources for other services such as routing, firewall, and voice
IPSec MIB	Allows Cisco IPSec configuration monitoring and can be integrated into a variety of VPN management solutions

Feature	Benefit
Certificate Support to Facilitate Automatic Authentication using Digital Certificates	Scales encryption use for large networks requiring secure connections between multiple sites
Easy Integration of VPN Modules into Existing Cisco 1841 and Cisco 2800, 3700, and 3800 Series Routers	Significantly reduces system costs, management complexity, and deployment effort compared to multiple-device solutions
Confidentiality, Data Integrity, and Data Origin Authentication through IPSec	Facilitates secure use of public switched networks and the Internet for WANs
Cisco IOS SSL VPN	Allows businesses to securely and transparently extend their networks to any Internet-enabled location using SSL VPN; the Cisco IOS SSL VPN supports clientless access to applications such as HTML-based intranet content, e-mail, network file shares, and Citrix and to the Cisco SSL VPN Client, enabling full network access remotely to virtually any application
Compression	Cisco IPsec and SSL VPN AIM provides hardware support for IPSec Layer 3 IPPCP and can compress a packet before encryption. This allows for higher throughput for Wide Area Networks (WAN) links

Cisco IPsec and SSL VPN AIM Performance

IPSec VPN

- The Cisco 1841 Series Module (AIM-VPN/SSL-1) can provide hardware-based IPSec encryption services of 25 and 95 Mbps in the Cisco 1841 (IPSec Internet mix [IMIX] and 1400-byte packets).[1]
- The Cisco 2800 Series Module (AIM-VPN/SSL-2) can provide hardware-based IPSec encryption services of 30 and 90 Mbps in the Cisco 2801, 35 and 100 Mbps in the Cisco 2811, 90 and 125 Mbps in the Cisco 2821, and 100 and 150 Mbps in the Cisco 2851 (IPSec IMIX and 1400-byte packets).[1]
- The Cisco 3800 Series Module (AIM-VPN/SSL-3) can provide hardware-based IPSec encryption services of 160 and 185 Mbps in the Cisco 3825 and 190 and 210 Mbps in the Cisco 3845 (IPSec IMIX and 1400-byte packets).[1]

SSL VPN

- The Cisco 1841 Series Module (AIM-VPN/SSL-1) c can provide hardware-based SSL VPN encryption of 5 Mbps with a Maximum of 50 Users.[1]
- The Cisco 2800 Series Module (AIM-VPN/SSL-2) can provide hardware-based SSL VPN encryption of 5Mbps with a Max of 50 users in the Cisco 2801, 5 Mbps with a Max of 75 users in the 2811, 10 Mbps with a Max of 100 users in the Cisco 2821, and 14 Mbps with a Max of 150 users in the Cisco 2851 routers.[2]
- The Cisco 3800 Series Module (AIM-VPN/SSL-3) can provide hardware-based SSL VPN encryption of 20 Mbps with a Max of 175 Users in the Cisco 3825, and 26 Mbps with a Max of 200 Users in the Cisco 3845 routers.[2]

[1] IPSec numbers are maximum values based on the Spirent IPSec IMIX definition and 1400-byte packet size. Each test is performed with a single tunnel. Customers are urged to consult with the Cisco account team and review all Cisco VPN solution design guides for greater detail on deployment options and scaling. Cisco recommends IPsec user to also review the Cisco Solution Design Guides for more specific information on scaling http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008075ea98.pdf and http://www.cisco.com/en/US/customer/netsol/ns656/networking_solutions_design_guidances_list.html.

[2] Customers are urged to consult the Cisco account team and review all Cisco Web VPN solution design guides for greater detail on deployment options and scaling. The IOS SSLVPN performance will vary based on which client is setup. SSLVPN client users will have higher overall performance than the SSLVPN clientless setup, which will have slightly lower performance.

Features

SSL VPN

- The Cisco IPsec and SSL VPN AIM offloads the SSL encryption processing, allowing improved SSL VPN performance.
- The Cisco IOS SSLVPN is the first router-based solution that offers SSL VPN remote-access connectivity integrated with security and industry-leading routing features on a converged data, voice, and wireless platform.
- SSL VPN is compelling because the security is transparent to the end user and easy for IT personnel to administer. Using only a Web browser, companies can extend their secure enterprise networks to any Internet-enabled location, including home computers, Internet kiosks, and wireless hotspots, thereby facilitating higher employee productivity and protecting corporate data while providing transient partner and consultant network access.
- Cisco IOS SSL VPN supports both clientless and full-network-access SSL VPN capabilities.

For further information about Cisco IOS SSL VPN, refer to http://www.cisco.com/go/iossslvpn.

IPSEC VPN

Cisco Systems® fully supports the entire set of RFCs that describe IPSec and related protocols: RFCs 2401 to 2410. In particular, Cisco supports the following features:

- DES, 3DES, and AES-the National Institute of Standards and Technology (NIST) created AES as a Federal Information Processing Standard (FIPS) publication to replace DES, IPSec and IKE. AES has a variable key length; the algorithm can specify a 128-bit key (default), a 192-bit key, or a 256-bit key. For details about AES, refer to http://csrc.nist.gov/encryption/aes/.
- IPSec-this protocol uses encryption technology to provide data confidentiality, integrity, and authenticity between participating peers in a private network. Cisco provides full Encapsulating Security Payload (ESP) and authentication header support.
- IKE-Using the Internet Security Association Key Management Protocol (ISAKMP) or Oakley, IKE provides security association management. IKE authenticates each peer in an IPSec transaction, negotiates security policy, and handles the exchange of session keys.
- Certificate management-Cisco fully supports the X509.V3 certificate system for device authentication and the Simple Certificate Enrollment Protocol (SCEP), a protocol for communicating with certificate authorities. Several vendors, including Verisign, Entrust Technologies, and Microsoft, support Cisco SCEP, and their products can operate with Cisco devices.
- RSA signatures and Diffie-Hellman-RSA and Diffie-Hellman are used every time an IPSec tunnel is established to authenticate the IKE security association. Diffie-Hellman is used to derive the shared secret encryption key for the protection of data across the IKE security association, including the negotiation of the IPSec policy to be used.
- Enhanced security-Hardware-based cryptography offers several security advantages over software-based solutions, including enhanced protection of keys.

For further information about Cisco IOS IPSec VPN, refer to http://www.cisco.com/en/US/customer/products/ps6635/products_ios_protocol_group_home.html.

Certifications

Cisco is committed to maintaining an active product certification and evaluation program for customers worldwide. Cisco recognizes that certifications and evaluations are important to its customers, and the company continues to be a leader in providing certified and evaluated products to the marketplace. Cisco also will continue to work with international security standards bodies to help shape the future of certified and evaluated products and will work to accelerate certification and evaluation processes. Certification and evaluation are considered at the earliest part of the company's product development cycle, and Cisco will continue to position its security products to ensure that customers have a variety of certified and evaluated products to meet their needs. Cisco pursues ICSA, Common Criteria (EAL), and FIPS 140-2 Certification see (Figure 2).

Figure 2.

FIPS

The Cisco VPN modules have been designed to meet FIPS 140-2 Level 2 security. Currently, only specific models have FIPS 140-2 certification. See product certifications by certification type for the current status of Cisco products certified for FIPS:

- http://www.cisco.com/en/US/customer/netsol/ns340/ns394/ns171/networking_solutions_audience_business_benefit0900aecd8009a16f.html
- http://csrc.nist.gov/cryptval/

ICSA IPSec

The Internet Computer Security Association (ICSA) is a commercial security certification body that offers ICSA IPSec and ICSA Firewall certification for various types of security products. Cisco participates in ICSA's IPSec and Firewall certification programs. See product certifications by certification type for the current status of Cisco products certified for ICSA http://www.cisco.com/en/US/customer/netsol/ns340/ns394/ns171/networking_solutions_audience_business_benefit0900aecd8009a16f.html.

Common Criteria

Common Criteria is an international standard for evaluating IT security. It was developed by a consortium of countries to replace numerous existing country-specific security assessment processes and was intended to establish a single standard for international use. Currently, 14 countries officially recognize the Common Criteria. Several versions of the Cisco ISR Routers are now being evaluated under the Information Technology Security Evaluation Criteria (ITSEC) and the Common Criteria. See product certifications by certification type for the current status of Cisco products certified for Common Criteria:

- http://www.cisco.com/en/US/customer/netsol/ns340/ns394/ns171/networking_solutions_audience_business_benefit0900aecd8009a16f.html
- http://www.commoncriteriaportal.org/

Cisco 1841 and Cisco 2800, 3700, and 3800 Series VPN Module Software

With a VPN module installed, the router will run with any feature set for the Cisco IOS Software, but the module is used only with IPSec or SSL VPN feature sets.

Export Regulations for the VPN Module

DES, 3DES, and AES software for the VPN module is controlled by U.S. export regulations for encryption products. The module itself is not controlled. U.S. regulations require the recording of names and addresses of recipients of DES and 3DES software. The Cisco ordering process for DES and 3DES software enforces these requirements.

Specifications

Table 4. Specifications

Feature	Specification
Part Number and Description	• AIM-VPN/SSL-1: Cisco 1841 DES, 3DES, AES, SSL, and Layer 3 (IPPCP) Compression VPN Encryption • AIM-VPN/SSL-2: Cisco 2800 Series DES, 3DES, AES, SSL, and Layer 3 (IPPCP) Compression VPN Encryption • AIM-VPN/SSL-3: Cisco 3800 Series DES, 3DES, AES, SSL, and Layer 3 (IPPCP) Compression VPN Encryption
IPSec RFC Support	• IPSec (RFCs 2401 to 2410) • IPSec ESP using DES and 3DES (RFC 2406) • IPSec authentication header using MD5 or SHA (RFCs 2403 to 2404) • IKE (RFCs 2407 to 2409) • GDOI (RFC 3547 – Group Domain of Interpretation)
Environmental	• Operating temperature: 32 to 104°F (0 to 40°C) • Nonoperating temperature: -4 to 149°F (-20 to 65°C) • Relative humidity: 10 to 85% noncondensing operating; 5 to 95% noncondensing, nonoperating safety

Dimensions and Weight

Table 5 lists dimensions and weight by platform.

Table 5. Dimensions and Weight

Module	AIM-VPN/SLL-1	AIM-VPN/SSL-2	AIM-VPN/SSL-3
Width	5.25 in. (13.3 cm)	5.25 in. (13.3 cm)	5.25 in. (13.3 cm)
Height	0.95 in. (2.41 cm)	0.95 in. (2.41 cm)	0.95 in. (2.41 cm)
Depth	3.25 in. (8.26 cm)	3.25 in. (8.26 cm)	3.25 in. (8.26 cm)
Weight	0.60 lb (0.27 kg)	0.60 lb (0.27 kg)	0.60 lb (0.27 kg)

Regulatory Compliance, Safety, EMC, Telecom, and Network Homologation

When installed in a Cisco 1800 (modular), 2800, 3700, or 3800 Series router, the VPN module does not change the standards (Regulatory Compliance, Safety, EMC, Telecom, or Network Homologation) of the router itself. Refer to data sheets for the Cisco 1800 (modular), 2800, 3700, and 3800 Series routers.

To Download the Software

Visit the Cisco Software Center to download the Cisco IOS Software.

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 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 VPN modules, visit http://www.cisco.com 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 C78-353932-04 02/08