Q&A

VPN Modules for Cisco 1841 and Cisco 2800 and 3800 Series Integrated Services Routers

OVERVIEW

Q. What is a VPN?

A. A VPN, or virtual private network, delivers the benefits of private network security, manageability, and quality of service (QoS) to a public network, such as the Internet, while reducing costs and increasing flexibility.

Q. What is IP Security (IPsec)?

A. IPsec is an industrywide standard for helping ensure the privacy, integrity, and authenticity of information crossing public IP networks.

Q. What is the Advanced Encryption Standard (AES)?

A. Cisco Systems® supports AES in addition to the Data Encryption Standard (DES) and Triple DES (3DES) supported in Cisco IOS® Software Release 12.2(13)T with IPsec. AES is privacy transform for IPsec and Internet Key Exchange (IKE). It uses a variable key length; the algorithm can specify a 128-bit key (default), a 192-bit key, or a 256-bit key. The AES feature adds support for the new AES encryption standard, with Cipher Block Chaining (CBC) mode, to IPsec.

The National Institute of Standards and Technology (NIST) created AES as a new Federal Information Processing Standard (FIPS) publication. Computer scientists at the National Institute of Standards and Technology , an agency of the Commerce Department's Technology Administration, organized an international competition to develop a strong information encryption formula to protect sensitive information in federal computer systems. Researchers from 12 countries worked on the development of advanced encoding methods during the global competition, and NIST invited the worldwide cryptographic community to "attack" the encryption formulas in an attempt to break the codes. The standard selected was Rijndael, developed by for AES. The Rijndael developers are Belgian cryptographers Joan Daemen (pronounced Yo'-ahn Dah'-mun) and Vincent Rijmen (pronounced Rye'-mun), both. Both are highly regarded experts within the international cryptographic community. For more information about details on AES, refer to the NIST Website: http://csrc.nist.gov/encryption/aes/

Q. What are Cisco IOS WebVPN and Secure Sockets Layer (SSL) VPN?

A. SSL-based VPN and Cisco IOS WebVPN comprise an emerging technology that provides remote-access connectivity from almost any Internet-capable location using a Web browser and its native SSL encryption. SSL VPN provides the flexibility to support secure access for all users, regardless of the endpoint host from which they are establishing the connection. If application access requirements are modest, SSL VPN does not require a VPN client to be preinstalled on the endpoint host.

Q. What do I need to activate SSL VPN or Cisco IOS WebVPN on my Cisco IOS Software router?

A. The Cisco IOS WebVPN/SSL VPN comprehensive feature set is available with Advanced Security images and higher starting with Cisco IOS Software Release 12.4(6)T (the Base IP image does not include this feature set). Cisco IOS WebVPN is not yet supported on a mainline train (General Deployment or Limited Deployment). All SSL VPN and Cisco IOS WebVPN features are included in a single, cost-effective license that can be purchased separately.

Q. What is IPsec for IP Version 6 (IPv6)?

A. IPsec is a framework of open standards, developed by the Internet Engineering Task Force (IETF), that provide security for transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers), such as Cisco® routers. IPsec provides the following optional network security services; in general, local security policy will dictate the use of one or more of these services:

- Data confidentiality—The IPsec sender can encrypt packets before sending them across a network.
- Data integrity—The IPsec receiver can authenticate packets sent by the IPsec sender to help ensure that the data has not been altered during transmission.
- Data origin authentication—The IPsec receiver can authenticate the source of the IPsec packets sent. This service depends on the data integrity service.
- Anti-replay—The IPsec receiver can detect and reject replayed packets.

With IPsec, data can be sent across a public network without observation, modification, or spoofing. IPsec functions are similar in both IPv6 and IPv4; however, only Ipv6 supports site-to-site tunnel mode.

In IPv6, IPsec is implemented using the AH authentication header and the Encapsulated Security Protocol (ESP) extension header. The authentication header provides integrity and authentication of the source. It also provides optional protection against replayed packets. The authentication header protects the integrity of most of the IP header fields and authenticates the source through a signature-based algorithm. The ESP header provides confidentiality, authentication of the source, connectionless integrity of the inner packet, anti-replay, and limited traffic flow confidentiality.

The Internet Key Exchange (IKE protocol is a key management protocol standard that is used in conjunction with IPsec. IPsec can be configured without IKE, but IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard.

Q. What is Cisco IOS Secure Multicast?

A. Cisco IOS Secure Multicast is a set of hardware and software features necessary to secure IP Multicast group traffic originating on or flowing through a Cisco IOS Software device. It combines the keying protocol Group Domain of Interpretation (GDOI) with hardware-based IPsec encryption to provide users with an efficient method for securing IP Multicast group traffic. With Cisco IOS Secure Multicast, a router can apply encryption to IP Multicast traffic without having to configure tunnels.

Cisco IOS Secure Multicast provides the following benefits:

- Multicast traffic protection—Protects multicast traffic without any form of additional encapsulation
- Scalability—Allows one-to-many and many-to-many relationships
- Manageability—Allows easy configuration and enhanced manageability
- Native IPsec encapsulation—Provides native IPsec encapsulation for IP Multicast traffic
- Key and policies distribution—Offers a centralized key and policies distribution mechanism through the GDOI key server
- Simplified troubleshooting—Simplifies troubleshooting by reducing overall complexity
- Extensible standards-based framework—Uses an extensible, standards-based framework

Q. How are these features processed on Cisco 1841 and Cisco 2800 and 3800 Series Integrated Services Routers and their VPN modules?

A. Table 1 shows the processing capabilities of these features on the modular integrated services routers.

Table 1. Feature Processing on ISRs

	IPsec 3DES	IPsec AES (256)	IP Payload Compression Protocol (IPPCP) Hardware Acceleration	IPv6 IPsec	Cisco IOS WebVPN or SSL VPN	Cisco IOS Secure Multicast
Cisco 1841 onboard crypto accelerator	X	X	–	–	–	–
Cisco 2800 Series onboard crypto accelerator	X	X	–	–	–	–
Cisco 3800 Series onboard crypto accelerator	X	X	–	–	–	–
AIM-VPN-II-PLUS Series	X	X	X	–	–	–
Cisco AIM-VPN/SSL Series	X	X	X	X	X	X

SSL VPN processing is different from that of the other features in that SSL VPN involves both termination of the SSL tunnel and the use of an application proxy. The Cisco AIM-VPN/SSL terminates the SSL tunnel, and the router CPU provides the application proxy services for the published applications. Without the Cisco AIM-VPN/SSL, the router CPU also terminates the SSL tunnel.

Q. What encryption modules are available for the Cisco Integrated Services Routers?

A. Table 2 lists the VPN modules supported in Cisco Integrated Services Routers.

Table 2. VPN Modules Supported in Cisco Integrated Services Routers

Cisco 1841	Cisco 2801-51	Cisco 3825	Cisco 3845
AIM-VPN/BPII-PLUS	AIM-VPN/EPII-PLUS	AIM-VPN/EPII-PLUS	AIM-VPN/HPII-PLUS
AIM-VPN/SSL-1	AIM-VPN/SSL-2	AIM-VPN/SSL-2	AIM-VPN/SSL-3

Q. What functions do the VPN modules perform?

A. Table 3 lists the features of each VPN module.

Table 3. VPN Module Features

Module	Features	Supported Platform
AIM-VPN/BP II-PLUS, AIM-VPN/EP II-PLUS, and AIM-VPN/HPII-PLUS	DES, 3DES, AES (256), Layer 3 compression (IPPCP), hashing, key exchange, and SA storage	Cisco 1841, Cisco 2800 Series, Cisco 3800 Series, Cisco 2600XM, Cisco 2691 Multiservice Platform, and Cisco 3700 Series Multiservice Access Routers
AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3	Cisco IOS WebVPN (SSL) termination, IPv6 IPsec, Cisco IOS Secure Multicast (GDOI), DES, 3DES, AES (256), Layer 3 compression (IPPCP), hashing, key exchange, and SA storage	Cisco 1841, Cisco 2800 Series, Cisco 3800 Series, and Cisco 3700 Series

Q. With the introduction of the new Cisco AIM-VPN/SSL cards, will the Cisco AIM-VPN-II-PLUS Series move to end-of-sale status?

A. There are no current plans to stop selling the Cisco AIM-VPN-II-PLUS cards; however, Cisco encourages customers to switch to the newer cards for their enhanced functions and performance.

Q. Where can I find IPsec and SSL VPN performance information?

A. The document at http://www.cisco.com/application/pdf/en/us/guest/netsol/ns125/c643/ccmigration_09186a00801f0a72.pdf provides an overview of the Cisco VPN-capable platforms and performance information. The routers are summarized in Table 5, which lists performance with and without VPN modules, tunnel counts, and throughput.

Q. What are the main features of the VPN modules?

A. These are the main features of the VPN modules:

- Modules accelerate IPsec at speeds suitable for multiple full-duplex T1/E1.
- Modules implement 3DES or DES for data protection in hardware.
- Modules support Rivest, Shamir, and Adelman algorithm (RSA) signatures and Diffie-Hellman for authentication.
- Modules use Secure Hash Algorithm 1 (SHA-1) or Message Digest 5 (MD5) hashing algorithms for data integrity.
- Cisco AIM-VPN/BPII-PLUS, AIM-VPN/EPII-PLUS, and AIM-VPN/HPII-PLUS add hardware support optimized for all primary AES configurations (AES128, AES192, and AES256) and Layer 3 (IPPCP) compression.
- New Cisco AIM-VPN/SSL Series cards support all of the features of the previous cards and also add SSL VPN termination, IPv6 IPsec acceleration using virtual tunnel interfaces (VTI), and Cisco IOS Secure Multicast, also known as GDOI.

Q. What other requirements should I consider when using the encryption modules?

A. You will need a Cisco IOS IPsec encryption image. The Advanced Security, Advanced IP Services, and Advanced Enterprise Services feature sets all support the encryption modules and activate the onboard encryption accelerators.

Q. Can I mix and match Cisco VPN solutions to meet my customers' needs?

A. Yes. That is the Cisco VPN advantage. Today the Cisco PIX® Firewall Software or Cisco Adaptive Security Appliances (ASA) IPsec, the Cisco VPN 3000 Series Concentrators IPsec, and the router Cisco IOS Software IPsec are all compatible. Routers with IPsec can talk to Cisco PIX Firewall Software or Cisco ASA with IPsec and also with Cisco VPN 3000 Series Concentrators.

SOFTWARE FEATURES

Q. Do the VPN modules support an IPsec MIB?

A. Yes. Both the Cisco AIM-VPN-II-PLUS Series and the new Cisco AIM-VPN/SSL Series modules support the Cisco IOS Software IPsec MIB.

Q. What benefits does the IPsec MIB provide?

A. The IPsec MIB allows MIB-2-compliant management applications to poll the host device and retrieve VPN-specific monitoring and performance data, delivering information useful for identifying VPN trouble areas and assessing overall performance. For more information, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps2326/products_data_sheet09186a00800888822.html

Q. Which IPsec RFCs are supported?

A. Cisco fully supports the entire set of RFCs describing IPsec and related protocols:

- IPsec (RFC 2401-10)
- IPsec ESP using DES and 3DES (RFC 2406)
- IPsec authentication header using MD5 or SHA (RFC 2403-4)
- IKE (RFC 2407-9)

Q. What kind of IPsec support does Cisco IOS Software provide?

A. IPsec uses encryption technology to provide data confidentiality, integrity, and authenticity between participating peers in a private network. Cisco provides full ESP and authentication header (AH) support.

Q. What is IKE?

A. IKE , or Internet Key Exchange, provides security association management. IKE authenticates each peer in an IPsec transaction, negotiates security policy, and handles the exchange of session keys.

Q. What type of certificate management support does Cisco IOS Software provide?

A. 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, Baltimore Technologies, and Microsoft, support SCEP and are interoperable with Cisco devices.

Q. What is SCEP?

A. SCEP, or Simple Certificate Enrollment Protocol, is a certificate enrollment protocol based on common and well-understood Public Key Cryptology Standards (PKCSs) 10 and 7 and standards using hypertext transfer protocol (HTTP transport methods. SCEP provides a standard way to enroll network devices with a certificate authority, as well as to look up and retrieve certificate revocation list (CRL) information from Lightweight Directory Access Protocol (LDAP) or HTTP methods. The 1.1 Version supports registration authority (RA) mode for SCEP enrollment.

Q. What management tools are available that support VPN module configuration and monitoring?

A. For management of firewall and VPN features on Cisco routers, use Cisco Security Manager, part of the Cisco Security Management Suite. For more information about Cisco Security Manager, see the data sheet at: http://www.cisco.com/en/US/products/ps6498/products_data_sheet0900aecd803ffd5c.html

Q. What mechanisms are available for IPsec VPN recovery and failover?

A. Three main features are available for the recovery and failover of IPsec VPNs. For dynamic route recovery, a combination of generic routing encapsulation (GRE) and IPsec tunnels can be used. For dynamic failover of IPsec tunnels, IPsec keepalives are recommended. For dynamic failover of IPsec gateways, tunnel endpoint discovery (TED) can be implemented.

IPsec stateful failover is a feature added to the Cisco 3800 Series Integrated Services Routers in Cisco IOS Software Release 12.4(6)T and made available by the use of the VPN accelerator modules. IPsec stateful failover works in conjunction with the Hot Standby Router Protocol (HSRP) to replicate the state of security associations on the standby router, thus preventing existing IPsec tunnels from having to reestablish associations if the active router fails.

Q. What is IETF Extended Authentication (Xauth)?

A. IETF Xauth provides user authentication within the IKE protocol. IETF Xauth prompts the user for authentication information (a user name and password) and verifies this information through an authentication, authorization, and accounting (AAA) server (using either RADIUS or TACACS+). Authentication occurs after IKE phase 1 but before IKE phase 2. If the user successfully authenticates, phase 2 security association establishment commences, after which data can be sent securely to the protected network.

Q. What is Mode-Config?

A. This Internet Security Association Key Management Protocol (ISAKMP) allows configuration items such as IP addresses. In the case of the VPN client, the VPN gateway can push an IP address to the client to use for communication with private networks.

HARDWARE FEATURES

Q. What government and industry certification requirements do the VPN modules meet?

A. For information about Cisco security and VPN certification and evaluation status, please see: http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking_solutions_audience_business_benefit0900aecd8009a16f.html

For the latest information about FIPS, refer to the following:

- http://csrc.nist.gov/cryptval/140-1/1401val2000.htm
- http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking_solutions_audience_business_benefit0900aecd8009a16f.html

ADDITIONAL INFORMATION

Q. Does the VPN module support Layer 3 IP compression?

A. Yes. The Cisco AIM-VPN/BPII-PLUS, AIM-VPN/EPII-PLUS, and AIM-VPN/HPII-PLUS, as well as the Cisco AIM-VPN/SSL Series, support hardware-enabled Layer 3 (IPPCP) compression.

With the Cisco Integrated Services Router onboard cryptographic accelerator, IPPCP compression is performed by the router CPU.

Q. What is the Canterbury Corpus?

A. The Canterbury Corpus is a benchmark tool to help researchers evaluate lossless compression methods. This site includes test files and compression test results for many research compression methods: http://corpus.canterbury.ac.nz/

Q. What are the average compression ratios for the Cisco AIM-VPN-II-PLUS and AIM-VPN/SSL Series using the Calgary Corpus?

A. Table 4 shows the average compression ratios as determined from the Calgary Corpus.

Table 4. Average Compression Ratios Using the Calgary Corpus

Files	Average Compression Ratio
alice29.txt	1.3
asyoulike.txt	1.3
cp.html	1.4
fields.c	1.7
grammar.lsp	2.6
kennedy.xls	1.3
lcet10.txt	1.2
plrabn12.txt	3.9
ptt5	1.6
sum	1.4
xargs.1	1.4
Average	1.76
Additional tests	
Microsoft Word	2.6
FrameMaker	1.6

These values are average compression ratios, and network data may differ depending on the exact traffic type compressed.

Q. Do the Cisco Integrated Services Routers support manual IPsec?

A. Yes, both the onboard encryption acceleration engine and the VPN modules support manual IPsec.

Q. Do the VPN modules function with Cisco Easy VPN Remote client or server mode?

A. A Cisco Easy VPN server is any headend model that supports the Cisco Unity® workgroup specification for the VPN server. A Cisco Easy VPN client is any customer premises equipment (CPE) that receives IPsec configuration from a Cisco Easy VPN server. All Cisco access routers can act as Cisco Easy VPN clients or servers.

Please also refer to the application note at:
http://www.cisco.com/en/US/products/sw/secursw/ps5299/prod_brochure09186a00800a4b36.html

Q. What Cisco IOS Software release supports the VPN encryption modules for the Cisco Integrated Services Routers?

A. Cisco IOS Software Release 12.3(8)T supported the Cisco AIM-VPN-II-PLUS modules when they were introduced for the Cisco 1841 and the Cisco 2800 Series, and Cisco IOS Software Release 12.3(11)T supported the Cisco 3800 Series. The Cisco AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3 were introduced in Cisco IOS Software Release 12.4(9)T.

Q. What are the export restrictions?

A. DES, 3DES, and AES software for the VPN modules is controlled by U.S. export regulations for encryption products. The modules themselves are 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, 3DES, and AES software enforces these requirements. For more information, refer to:
http://www.cisco.com/wwl/export/crypto/

Q. Where can I find more information about Cisco IOS WebVPN or SSL VPN?

A. More information can be found at:
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns347/networking_solutions_sub_solution_home.html

Q. Where can I find more information about Cisco IOS Secure Multicast?

A. More information can be found at: http://www.cisco.com/en/US/products/ps6552/products_white_paper0900aecd8047191e.shtml

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.com 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

Printed in USA C67-362469-00 08/06