Cisco VPN Internal Service Module for Cisco ISR G2

Compact Versatile High-Performance VPN Module

The Cisco® VPN Internal Service Module (VPN ISM) is a module for the Cisco Integrated Services Routers Generation 2 (ISR G2) that provides the capability to considerably increase performance for VPN encrypted traffic. The module has a multicore processor that operates independently of the host router resources, helping ensure maximum concurrent encrypted application performance while maintaining competitive performance for other types of traffic. The Cisco VPN ISM supports the latest versions of cryptography standards, including stronger National Security Agency (NSA) regulated cryptographic algorithms such as Suite B Cryptography.

The Cisco VPN ISM is ready to use, allowing quick and easy installation of the module for increasing VPN encryption performance on Cisco ISR G2 routers. The VPN ISM is compatible with all Cisco ISR G2 routers that support the ISM card slot and runs the same level of feature-rich functions as found on the Cisco ISR G2. It integrates all elements necessary to optimize branch-office IT infrastructure for delivery of encrypted application data from the data center and deployment of branch-office applications on demand, and houses them under a single chassis - the Cisco ISR G2.

Figure 1 shows the Cisco VPN Internal Service Module (VPN ISM).

Figure 1. Cisco VPN Internal Service Module (VPN ISM)



© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Features and Benefits

Table 1 describes the features supported by the Cisco VPN ISM and Table 2 describes the benefits of the Cisco VPN ISM features.

Table 1. Supported Features of Cisco VPN ISM

Feature	Description
Physical	The Cisco VPN ISM fits in the ISM slot in the Cisco ISR G2.
Platform support	The Cisco VPN ISM supports the Cisco 1941 and the Cisco 2900 and 3900 Series Integrated Services Routers (ISRs).
Hardware prerequisites	An ISM slot for the Cisco 1941 and the Cisco 2900 and 3900 Series is required.
IP Security (IPsec) encryption supported	Authentication: • Rivest, Shamir, and Adelman (RSA) • Elliptic-Curve Digital Signature Algorithm (ECDSA) • Advanced Encryption Standard (AES) in Galois Message Authentication Code (GMAC) Key exchange: • Diffie Hellman and Elliptic-Curve Diffie Hellman (ECDH) Data integrity: • Message Digest Algorithm 5 (MD5) • Secure Hash Algorithm 1 (SHA-1) and Secure Hash Algorithm 2 (SHA-2) Encryption: • Data Encryption Standard (DES) • Triple DES (3DES) • Advanced Encryption Standard (AES) in Cipher-Block Chaining (CBC) and Galois/Counter Mode (GCM)
Hardware Secure Sockets Layer (SSL) encryption supported	The Cisco VPN ISM supports SSL VPN encryption.
Number of encryption modules per router	The Cisco VPN ISM uses one encryption module per router.
Minimum Cisco IOS Software version required	The Cisco VPN ISM requires Cisco IOS Software Version 15.2(1)T1 or later. The SEC-K9 and HSEC-K9 licenses are required.
Maximum number of IPsec encrypted tunnels	The Cisco VPN ISM supports up to 500 tunnels on the Cisco 1941, up to 2000 tunnels on the Cisco 2900 Series, and up to 3000 tunnels on the Cisco 3900 Series.
Standards supported	The Cisco VPN ISM supports the IPsec Internet Key Exchange (IKE): RFCs 2401 to 2410, 2411, 2451, 4306, 4718, 4869, and 5996.

Table 2. Features and Benefits of Cisco VPN ISM

Features	Benefits
Ability to offload encryption to a dedicated service module	Dedicated encryption protects performance while using CPU for other services.
Small physical, energy, and carbon footprint	You can save on energy bills, hardware support contracts, and onsite visits.
Maximum performance while also maintaining strong encryption protection	You have two to three times better onboard performance with the strongest Suite B encryption support.
High-overhead IPsec processing from the main processor	Critical processing resources are reserved for other services such as routing, firewall, and voice.
IPsec MIB	Cisco IPsec configuration can be monitored and can be integrated into a variety of VPN management solutions.
Certificate support to facilitate automatic authentication using digital certificates	Encryption use scales for large networks requiring secure connections between multiple sites.
Easy integration of VPN modules into existing Cisco 1941 and Cisco 2900 and 3900 Series Routers	System costs, management complexity, and deployment effort are reduced significantly compared to multiple-device solutions.

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Features	Benefits
Confidentiality, data integrity, and data origin authentication through IPsec	Secure use of public switched networks and the Internet for WANs is facilitated.
Cisco IOS SSL VPN	Businesses can 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, email, network file shares, Citrix, and the Cisco SSL VPN Client, enabling full network access remotely to virtually any application.

Platforms Supported

Cisco VPN ISM acceleration module platform support is outlined in Table 3.

Table 3. Supported Platforms

Platform	Support
880	No
890	No
1921	No
1941	Yes
2901	Yes
2911	Yes
2921	Yes
2951	Yes
3925	Yes
3945	Yes
3925E	No
3945E	No

Cisco VPN ISM IPsec VPN Performance

IPsec

- The Cisco 1941 Series Module (ISM-VPN-19) can provide hardware-based IPSec encryption services of 140 and 500 Mbps in the Cisco 1941 (IPSec Internet mix [IMIX] and 1400-byte packets).
- The Cisco 2900 Series Module (ISM-VPN-29) can provide hardware-based IPSec encryption services of 145 and 550 Mbps in the Cisco 2001, 150 and 600 Mbps in the Cisco 2011, 220 and 700 Mbps in the Cisco 2921, and 385 and 900 Mbps in the Cisco 2951 (IPSec IMIX and 1400-byte packets).
- The Cisco 3900 Series Module (ISM-VPN-39) can provide hardware-based IPSec encryption services of 550 and 1100 Mbps in the Cisco 3925 and 600 and 1200 Mbps in the Cisco 3945 (IPSec IMIX and 1400-byte packets).

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Product Specification

Table 4 gives specifications for the Cisco VPN ISM.

Table 4. Cisco VPN ISM Product Specifications

Feature	Specification
Product part number	ISM-VPN-19 ISM-VPN-29 ISM-VPN-39 CISCO1941-HSEC+/K9 CISCO2901-HSEC+/K9 CISCO2911-HSEC+/K9 CISCO2921-HSEC+/K9 CISCO2951-HSEC+/K9 CISCO3925-HSEC+/K9 CISCO3945-HSEC+/K9
Form factor	ISM
Internal network interfaces	Gigabit Ethernet connectivity to router backplane
Cisco IOS Software	15.2(1)T1 or higher
IPsec Support	
Encryption	Data Encryption Standard (DES), 3DES, Advanced Encryption Standard (AES) in Cipher-Block Chaining (CBC) and Galois/Counter Mode (GCM) (128-, 192-, and 256-bit)
Key exchange	Diffie Hellman (DH) and Elliptic-Curve Diffie Hellman (ECDH)
Digital signature	Rivest, Shamir, and Adelman (RSA) and Elliptic-Curve Digital Signature Algorithm (ECDSA)
Integrity	Message Digest Algorithm 5 (MD5), Secure Hash Algorithm 1 and 2 (SHA-1 and SHA-2, respectively) (384- and 512-bit), and AES-GMAC (128-, 192-, 256- bit)
Power Specification	
Power consumption (maximum)	20W
Physical Specification	
Dimensions (H x W x D)	0.85 x 4 x 6.1 in. (2.2 x 10.2 x 15.5 cm)
Shipping dimensions (H x W x D with packaging)	9.45 x 7.18 x 2.38 in. (24 x 18.4 x 6.05 cm)
Maximum weight	0.5 lb (0.206 kg)
Operating Conditions	
Operating temperature	Cisco 1941 and 2901: 32 to 104℉ (0 to 40℃) normal Cisco 2911, 2921, 2951, 3925, and 3945: 32 to 122℉ (0 to 50℃) normal
Humidity	10 to 95% operating
Altitude (operating)	104℉ (40℃) at sea level 104℉ (40℃) at 6,000 ft (1,800m) 86℉ (30℃) at 13,000 ft (4,000m) 81℉ (27.2℃) at 15,000 ft (4,600m) Note: De-rate 34.5℉ (1.4℃) per 1,000 ft above 6,00 0 ft (per 300m above 2,600m)
Transportation and Storage Conditions	
Temperature	-4 to 149℉ (-20 to +65℃)
Relative humidity	9 to 95% operating
Altitude	10,000 ft (3,050m)

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Feature	Specification
Regulatory Compliance	
Safety	• UL 60950-1, 2nd Edition, Standard for safety for information deployable platform technology equipment (US) • CAN/CSA-C22.2 No. 60950-1-03, Safety of information technology equipment including electrical business equipment (Canada) • IEC 60950-1:3rd edition [PRC] Safety of information technology equipment/Second Edition [Mexico] • EN 60950 -1:2001, Safety of information technology equipment (CENELEC; includes EU and EFTA) • AS/NZS 60950-1, Safety of information technology equipment including electrical business equipment (Australia)
EMC	Emissions: • 47 CFR Part 15 Class A • CISPR22 Class A • EN300386 Class A • EN55022 Class A • EN61000-3-2 • EN61000-3-3 • ICES Class A • KN 22 Class A • VCCI Class I Immunities: • CISPR24 • EN300386 • EN55024 • EN61000-6-1

Ordering Information

For information about how to order the Cisco VPN Internal Service Module, please visit the Cisco ISR G2 Ordering Guide. To place an order, visit the Cisco Ordering Home Page and refer to Tables 5 and 6. For additional product numbers, including the Cisco VPN ISM bundle offerings, please check the Cisco price list or contact your local Cisco account representative.

To download software, please visit the Cisco Software Center.

Table 5. Cisco VPN ISM Ordering Information

Product Number	Product Description
ISM-VPN-19	VPN Internal Service Module for support on 1941 platform
ISM-VPN-29	VPN Internal Service Module for support on 2901,2911,2921 and 2951 platforms
ISM-VPN-39	VPN Internal Service Module for support on 3925 and 3945 platforms

Table 6. Cisco VPN ISM and ISR G2 Bundles

Ordering SKU	Description
CISCO1941-HSEC+/K9	Security bundle for 1941 ISR G2 Platform, including VPN ISM
CISCO2901-HSEC+/K9	Security bundle for 2901 ISR G2 Platform, including VPN ISM
CISCO2911-HSEC+/K9	Security bundle for 2911 ISR G2 Platform, including VPN ISM
CISCO2921-HSEC+/K9	Security bundle for 2921 ISR G2 Platform, including VPN ISM
CISCO2951-HSEC+/K9	Security bundle for 2951 ISR G2 Platform, including VPN ISM
CISCO3925-HSEC+/K9	Security bundle for 3925 ISR G2 Platform, including VPN ISM
CISCO3945-HSEC+/K9	Security bundle for 3945 ISR G2 Platform, including VPN ISM

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Warranty Information

Warranty information is available on Cisco.com at the Product Warranties page.

Service and Support Information

Cisco VPN ISM hardware service and support is covered by the Cisco SMARTnet® Service contract for the router in which the module will reside. For more information about Cisco Technical Services visit http://www.cisco.com/go/ts.

For More Information

For more information about the Cisco VPN ISM, please visit http://www.cisco.com/go/vpnism 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1110R)

Printed in USA C78-682436-00 10/11

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.