

Integrated Services Module (ISM)



Overview

The Integrated Services Module (ISM) for Cisco 7100 series VPN routers provides high-performance, hardware-assisted tunneling and encryption services suitable for virtual private network (VPN) remote access and site-to-site intranet and extranet applications. As an integral component of the Cisco VPN solution, the ISM provides platform scalability and security while working seamlessly with all services necessary for successful VPN deployments—security, quality of service (QoS), firewall and intrusion detection, service-level validation, and management. This integration, combined with ISM support for the broad set of WAN media and services

offered by the Cisco 7100 series router, ensures the smooth integration of VPN technology into any enterprise or service provider network.

The high-performance acceleration of Cisco IP Security (IPSec) offered by the ISM provides privacy, integrity, and authenticity for VPN—crucial requirements for transmission of sensitive information over the Internet. The ISM supports up to 2000 Data Encryption Standard (DES) or Triple DES encrypted tunnels for remote access applications and supports up to full duplex DS-3 line rate (90 Mbps) for site-to-site VPNs. The ISM coprocessor architecture offloads these processor-intensive functions from the main route processor of Cisco 7100 series routers, minimizing impact on system resources, thus delivering increased tunneling and encryption scalability for the most demanding VPN deployments. In addition, ISM support for advanced IPSec system facilities, such as the Cisco Tunnel Endpoint Discovery (TED) protocol, allows customers to implement IPSec transparently into the network infrastructure without the need for time-consuming crypto map management and without affecting individual workstations or PCs.

The ISM also supports Microsoft's Point-To-Point Tunneling Protocol (PPTP) and Microsoft Point-to-Point Encryption (MPPE), providing highly scalable remote access VPN capabilities to Microsoft Windows 95/98/NT systems. The ISM supports up to 2000 simultaneous PPTP/MPPE remote VPN users protected with strong, 128-bit RC-4 encryption. With support for IPSec or PPTP, the ISM provides flexible options in remote access deployment models, enabling enterprises to utilize software resident in Microsoft Windows 95/98/NT or Cisco Secure VPN client software based on IPSec (or other qualified third-party IPSec clients).

Public

Copyright © 1999 Cisco Systems, Inc. All Rights Reserved.

Page 1 of 6

Features at a Glance

| Feature | Description |
|--------------------------------------|---|
| Physical | Service module |
| Platform Support | Cisco 7120, 7140 |
| Hardware Prerequisites | None |
| Throughput | Up to full duplex DS3 (90 Mbps) using 3 DES |
| Number of Tunnels | Up to 2000 IPsec protected tunnels Up to 2000 PPTP tunnels protected by MPPE |
| Encryption | Data protection: IPsec DES and 3 DES, 40 and 128-bit RC4 MPPE (stateful or stateless) Authentication: RSA and Diffie Hellman, MS Chap Data integrity: SHA-1 and MD5 |
| VPN Tunneling | IPsec tunnel mode, GRE, LT2P, L2F protected by IPsec, PPTP protected by MPPE |
| Number of ISMs per Router | One ISM per chassis |
| Minimum Cisco IOS® Release Supported | Please use latest 12.0XE or 12.1E release available at time of shipment |
| Standards Supported | IPsec/IKE: RFCs 2401–2410, 2411, 2451 MPPE: draft-ietf-pppext-mppe-* |

Cisco VPN solutions encompass all segments of the networking infrastructure—platforms, security, network services, network appliances, and management. The services offered by Cisco VPN solutions include encryption, tunneling, firewall, and QoS capabilities. The ISM accelerates the encryption components of a VPN, including bulk data transfer, public key authentication, and key exchange.

By offering the following features, the ISM is a key component in creating an accelerated VPN solution:

IPsec—IPsec 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 (AH) support.

- *DES and 3 DES*—DES and 3 DES encryption are very CPU intensive, potentially impacting router performance in high-throughput configurations. The ISM makes it possible to send DES or 3 DES encrypted data at data rates up to 90 Mbps while still providing the full range of VPN services available from the Cisco 7100 router.

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

- *RSA and Diffie-Hellman*—These CPU-intensive protocols are used every time a new IPsec tunnel is established. RSA authenticates the remote device while Diffie-Hellman exchanges keys that will be used for DES or 3DES encryption. The ISM implements these protocols in specialized hardware ensuring fast tunnel setup and high overall encryption throughput.
- *IKE Keepalive*—The IKE keepalive mechanism provides enhanced availability for IPsec configurations by automatically sending “keepalive” messages, allowing peers to recognize availability of tunnel endpoints. This setup ensures tunnel availability during periods of network inactivity.
- *Tunnel Endpoint Discovery (TED)*—This protocol improves the scalability and availability of VPNs in intranet and extranet configurations. Rather than defining each tunnel endpoint for protected traffic in the configuration, the network manager can simply configure which traffic to protect and let TED automatically determine the other endpoint in real time.
- *MPPE*—This feature provides strong, 128-bit RC-4 encryption for PPTP tunneling. MPPE can impact router performance in high-throughput configurations. The ISM ensures high encryption throughput for remote access VPNs using PPTP/MPPE.

VPN Tunneling—The ISM provides a variety of tunneling options, enabling extensive flexibility in designing remote access and site-to-site VPNs.



- *Layer 2 Tunneling Protocol/Layer 2 Forwarding (L2TP/L2F)*—L2TP/L2F tunnels provide remote access VPNs with full support for Cisco IOS authentication, authorization and accounting (AAA) services, including authentication services through TACACS+ and Remote-Access Dial-In User Service (RADIUS), per-user authorization, and accounting capabilities for tracking VPN usage. IPsec protects the L2TP/L2F tunnel by encrypting the tunnel itself. The combination of L2TP/L2F and IPsec provides a secure remote access VPN solution.
- *GRE*—Generic routing encapsulation (GRE) tunnels provide site-to-site intranet or extranet VPNs with multiprotocol support, routing support, and tunneling reliability. GRE tunnels can be used in conjunction with IPsec, to provide a secure site-to-site VPN solution.
- *PPTP*—PPTP tunnels provide easy-to-provision remote access VPNs for customers with Microsoft Windows 95/98/NT clients. PPTP tunnels can be encrypted via MPPE for a secure remote access VPN solution.
- *IPsec*—IPsec tunneling, alone, is appropriate for remote access or site-to-site VPNs when the added features of L2TP/L2F or GRE tunneling are not required. IPsec has lower packet overhead than other tunneling protocols, and supports IP packets only.

Certificate management—The ISM supports the X509.V3 certificate system for device authentication, and the Certificate Enrollment Protocol (CEP) for communicating with certificate authorities. This setup enables deployment of large VPN deployments requiring authentication between many locations and devices. Several vendors, including Verisign and Entrust Technologies, support Cisco CEP and are interoperable with Cisco devices.

Enhanced security—Hardware-based encryption solutions, such as the ISM, offer several security advantages over software-based implementations, including enhanced protection of keys and other confidential materials and tamper-resistant chip-based cryptographic algorithms.

Features and Benefits

| Feature | Benefit |
|--|---|
| ISM offers hardware-based DES and 3 DES Encryption. | Ensures high-encryption throughput in complex, high-services networks and improves overall encryption capabilities over software encryption methods |
| ISM offloads high-overhead IPsec and MPPE processing from the main processor. | Reserves critical processing resources for other VPN services, such as QoS and firewalling |
| ISM supports up to 2000 IPsec or PPTP tunnels. | Enables deployment of large-scale remote access VPNs by increasing the number of encrypted links supported in a single router |
| ISM is integrated in the Cisco 7100 Integrated VPN router. | Significantly reduces the system costs, management complexity, and deployment effort over multiple box solutions |
| IPsec provides confidentiality, data integrity and data origin authentication. | Enables the secure use of public switched networks and the Internet for wide area networking |
| Certificate support enables automatic authentication using digital certificates. | Scales encryption use for large networks requiring secure connections between multiple locations |
| Automatically negotiates security associations. | Enables ad-hoc secure communications without costly manual preconfiguration |
| Automatically determines IPsec tunnel endpoint in real time. | Alleviates need to manually define each tunnel endpoint; enables IPsec to scale to very large mesh networks |
| IKE keepalives send “keepalives” in order to allow peers to recognize availability of tunnel endpoints. | Provides enhanced availability for IPsec configurations |
| Traffic can be selected for encryption based on extended access lists, providing flexible security policies. | Fine control over what traffic requires encryption improves overall performance; in addition, traffic can be classified for encryption with different keys or different algorithms, thus providing application-level protection |
| ISM is a standards-based solution solution. | Insures multivendor interoperability among network devices, client software, and other computing systems |

Using the ISM

The ISM is fully compatible with network-layer IPsec and Layer 3 encryption software services found in Cisco IOS Software. Throughput is simply enhanced through the use of specialized hardware to perform the complex mathematical transformations necessary to generate keys, authenticate devices, authenticate packets, and encrypt/decrypt data.

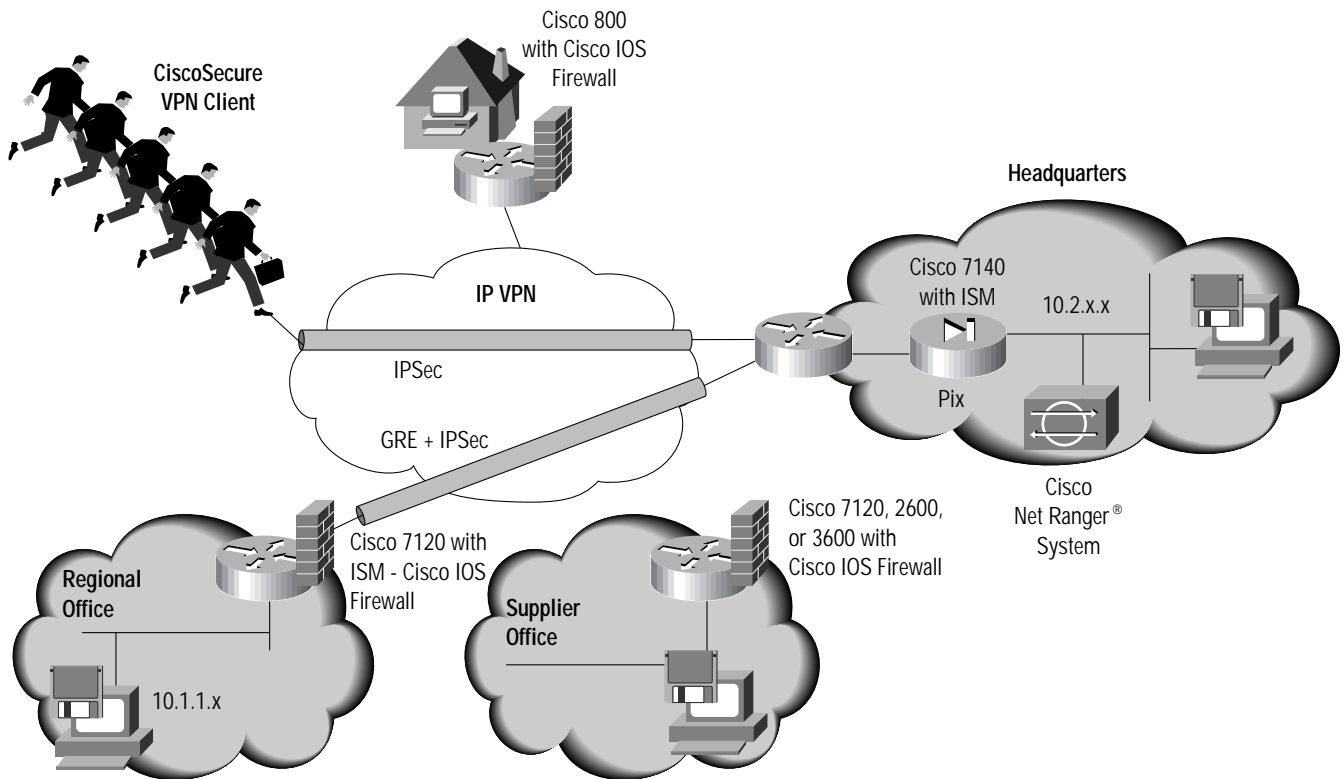
Encryption Engine Choices for Cisco 7100 Systems

The Cisco 7100 series routers can be configured to encrypt data by main route processors, or by the Integrated Services Module. This flexibility enables the use of the routers main CPU of the routers for modest encryption requirements, reducing overall system costs. In order to provide the highest IPsec performance available, the ISM can be used. Cisco IOS software automatically detects the presence of the ISM encryption engine and transfers all encryption activities to the hardware accelerator without configuration changes. With this ability to match performance needs with resource utilization requirements, the Cisco 7100 VPN router offers the best mix of value, performance, and cost for any encryption environment. Figure 1 illustrates a typical VPN deployment.

A Cisco 7140 VPN router with an ISM card connects a corporation's headquarters to the Internet over a T3 line terminating VPN tunnels from remote offices, extranet partners, and remote users. The use of the ISM ensures high encryption performance without impacting the routing and services capabilities of the platform.

A Cisco 7120 with ISM connects the regional office to the Internet for intranet VPN and provides a full complement of VPN capabilities, including integrated firewall services with the Cisco IOS Firewall. Suppliers connect to the VPN using local branch or regional office routers, such as the Cisco 1700, 2600, or 3600, enabling extranet VPNs. The Cisco 800 series routers or the Cisco Secure VPN client software provide remote access for telecommuters and mobile users.

Figure 1 Using the ISM in a typical VPN deployment



Ordering Information—Cisco 7100 Software Support

To enable either 56-bit DES/40-bit MPPE or 168-bit DES/128-bit MPPE encryption services, please select the appropriate software image. ISM support for IPsec and PPTP/MPPE available in Cisco IOS 12.0XE or 12.1E software images beginning with Release 12.0(5)XE4. ISM support for PPTP/MPPE is anticipated for a Cisco IOS 12.0(5)XE software release in Cisco IOS Software images beginning with release 12.0(5)XE image at time of shipment.

Table 1 Cisco IOS Software Release 12.0XE or 12.1E

| Part number | Cisco 7100 Series Cisco IOS Software Feature Set | VPN Features |
|----------------|---|---|
| S71CK2 | Cisco 7100 series Cisco IOS IP IPSec 3DES | Tunneling, bandwidth management/QoS, 40-bit and 128-bit MPPE, 56- and 168-bit IPSec encryption |
| S71CHK2 | Cisco 7100 series CiscoIOS IP/FW/IDS IPSec 3DES | Tunneling, bandwidth management/QoS, 40-bit and 128-bit MPPE, 56-bit and 168-bit IPSec encryption, firewall, intrusion detection |
| S71CL | Cisco 7100 series Cisco IOS IP IPSec 56 | Tunneling, bandwidth management/QoS, 40-bit MPPE, 56-bit IPSec encryption |
| S71CHL | Cisco 7100 series Cisco IOS IP/FW/IDS IPSec 56 | Tunneling, bandwidth management/QoS, 40-bit MPPE, 56-bit IPSec encryption, firewall, intrusion detection |
| S71AK2 | Cisco 7100 series Cisco IOS Enterprise IPSec 3DES | Tunneling, bandwidth management/QoS, multiprotocol support, 40-bit and 128-bit MPPE, 56 and 168-bit IPSec encryption |
| S71AHK2 | Cisco 7100 series Cisco IOS Enterprise/FW/IDS IPSec3DES | Tunneling, bandwidth management/QoS, multiprotocol support, 40 bit and 128-bit MPPE, 56 and 168-bit IPSec encryption, firewall, intrusion detection |
| S71AL | Cisco 7100 series IOS Enterprise IPSec 56 | Tunneling, bandwidth management/QoS, multiprotocol support, 40-bit MPPE, 56-bit IPSec encryption |
| S71AHK2 | Cisco 7100 series IOS Enterprise/FW/IDS IPSec 56 | Tunneling, bandwidth management/QoS, multiprotocol support, 40-bit and 128-bit MPPE, 56-bit IPSec encryption, firewall, intrusion detection |

An unrestricted license for the Cisco Secure VPN client is included with every ISM card at no additional charge if selected at time of order. However, a separate support contract for the client is required. The Cisco Secure VPN client is available in DES or 3DES versions. For more information on the Cisco Secure VPN client, please see:

<http://www.cisco.com/warp/public/cc/cisco/mkt/security/vpncli/index.shtml>

Export Considerations

The ISM and associated software may be export controlled. Please refer to the export compliance Web site at:

<http://www.cisco.com/wwl/export/encrypt.html> for guidance.

For specific export questions, please contact export@cisco.com

Table 2 ISM Ordering Information

| Part Number | Description |
|---------------|----------------------------|
| SM-ISM | Integrated Services Module |

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 526-4100

European Headquarters

Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France

<http://www-europe.cisco.com>
Tel: 33 1 69 18 61 00

Fax: 33 1 69 28 83 26

Americas**Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

<http://www.cisco.com>

Tel: 408 526-7660

Fax: 408 527-0883

Asia Headquarters

Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan

<http://www.cisco.com>

Tel: 81 3 5219 6250

Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco Connection Online Web site at <http://www.cisco.com/offices>.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE Finland • France
• Germany • Greece • Hong Kong • 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 • Singapore Slovakia • Slovenia • South Africa • Spain •
Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

Copyright © 1999 Cisco Systems, Inc. All rights reserved. Printed in the USA. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and NetRanger are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9910R) 11/99 LW