

# Integrated Services Adapter (ISA)

## Overview

The Integrated Services Adapter (ISA) for Cisco 7100 and 7200 series routers provides high-performance, hardware-assisted tunneling and encryption services suitable for private WAN and virtual private network (VPN) applications. As an integral component of Cisco security solutions, the ISA provides encryption scalability while working seamlessly with advanced WAN and VPN services such as quality of service (QoS), firewall and intrusion detection, and service-level validation. This feature integration, combined with ISA support for the broad set of LAN/WAN media and services, ensures the smooth integration of encryption technology into virtually any enterprise or service provider network environment.

The high-performance acceleration of Cisco IP Security (IPSec) offered by the ISA also provides privacy, integrity, and authenticity for fast-emerging VPN deployments—crucial requirements for transmission of sensitive information over the Internet. The ISA supports Data Encryption Standard (DES) or Triple DES IPSec encryption at full duplex DS-3 line rate (90 Mbps) for site-to-site VPNs. For mixed VPN environments with both site-to-site and remote access VPN requirements, the ISA supports up to 2000 encrypted tunnels. The ISA co-processor architecture offloads these processor-intensive functions from the main route processor, minimizing impact on system resources, thus delivering increased tunneling and encryption scalability for the most demanding encryption deployments. In addition, ISA 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 ISA 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 ISA supports up to 2000 simultaneous PPTP/MPPE remote VPN users protected with strong, 128-bit RC-4 encryption. With support for IPSec or PPTP/MPPE, the ISA provides flexible options in remote access deployment models, enabling enterprises to utilize software resident in Microsoft Windows 95/98/NT, L2TP/IPSec software resident in Microsoft Windows 2000 or Cisco Secure VPN client software based on IPSec (or other qualified third-party IPSec clients). For VPN environments requiring concurrent support of both IPSec and MPPE acceleration in the same Cisco 7200 system, multiple ISA cards may be installed in any open port adapter slots. In a Cisco 7100 series system, the primary encryption service is provided by the Integrated Services Module (ISM). The ISA, however, can be installed in the open port adapter slot of a Cisco 7100 series system to deliver concurrent IPSec and MPPE acceleration.

## Features at a Glance

Feature	Description
Physical	Service adapter - installs in port adapter slot
Platform Support	Cisco 7100 and 7200
Hardware Prerequisites	None; ISA works with any Cisco 7200VXR compatible port adapter
Throughput	Up to full duplex DS3 (90 Mbps) using 3DES
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, L2TP and L2F protected by IPSec; PPTP protected by MPPE
Number of ISAs per Router	Up to two: one for IPSec acceleration, one for MPPE acceleration
Minimum Cisco IOS <sup>®</sup> Release Supported	Please use 12.1E release available at time of shipment
Standards Supported	IPSec/IKE: RFCs 2401–2410, 2411, 2451 MPPE: draft-ietf-pppext-mppe-*

By offering the following features, the ISA is a key component in delivering an accelerated encryption solutions:

**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 3DES**—DES and 3DES encryption are very CPU intensive, potentially impacting router performance in high-throughput configurations. The ISA makes it possible to send DES or 3DES encrypted data at rates up to 90 Mbps while still providing the full range of advanced services available from Cisco 7100 and 7200 series routers.

**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 ISA 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 ISA ensures high encryption throughput for remote access VPNs using PPTP/MPPE.

**VPN Tunneling**—The ISA provides encryption for 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. Scalable support for L2TP+IPSec enables use of VPN client software resident in Microsoft Windows 2000. 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 ISA 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 ISA, 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
ISA 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
ISA offloads high-overhead IPSec and MPPE processing from the main processor.	Reserves critical processing resources for other WAN and VPN services, such as QoS and firewalling
ISA 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
ISA is integrated in the Cisco 7100 and 7200 series routers.	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
ISA is a standards-based solution.	Ensures multivendor interoperability among network devices, client software, and other computing systems

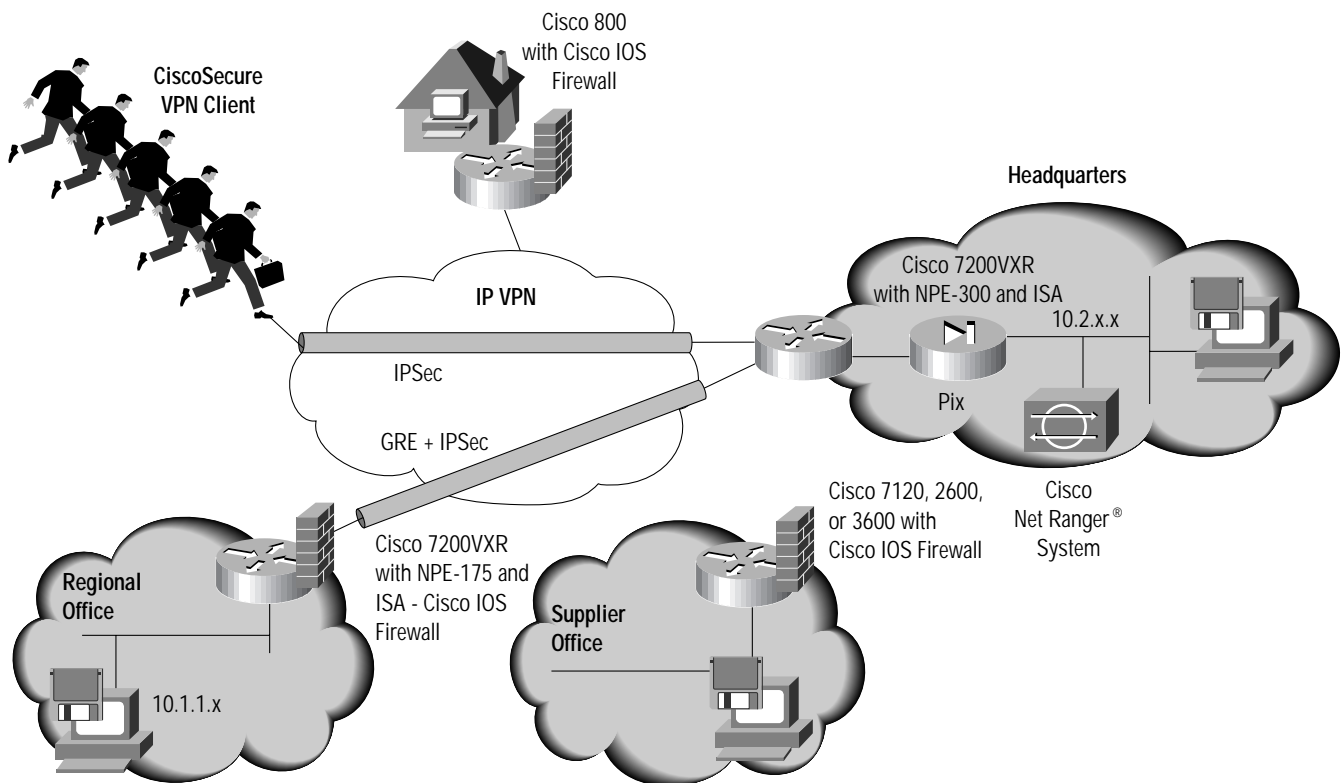
## Using the ISA

The ISA 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 and 7200 Series Routers

The Cisco 7200 series router can be configured to encrypt data by main route processor, or by the Integrated Services Adapter. Furthermore, Cisco 7200 series routers can provide concurrent IPSec and MPPE acceleration using two ISA cards. The Cisco 7100 series VPN router can be configured to encrypt data using the main route processor or the Integrated Services Module (ISM). The ISA card is installed on a Cisco 7100 system to complement the ISM, enabling concurrent acceleration of both IPSec and MPPE. 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 encryption performance available, the ISA can be used. Cisco IOS software automatically detects the presence of the ISA 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 and 7200 series offers the best mix of value, performance, and cost for any encryption environment. Figure 1 illustrates ISA deployed on a Cisco 7200 series router in a typical VPN environment.

Figure 1 Using the ISA in a typical VPN deployment



A Cisco 7200VXR router with an NPE-300 and an ISA card connects a corporation's headquarters to the Internet over a T3 line terminating VPN tunnels from remote offices, extranet partners, and remote users. A Cisco 7200VXR with an NPE-175 and an ISA provides nxT1/E1 encryption scalability up to 50 Mbps suitable for regional office VPN environments. The use of the ISA ensures high encryption performance without impacting the routing and services capabilities of the platform. 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. Cisco IOS software features provides a full complement of VPN capabilities, including integrated firewall services with the Cisco IOS Firewall, and content-aware QoS features.

### Ordering Information—Cisco 7100 and 7200 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. ISA support for IPSec and PPTP/MPPE available in Cisco IOS 12.1E software images beginning with Release 12.1(1)E.

An unrestricted license for the Cisco Secure VPN client is included with every ISA 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 ISA 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](mailto:export@cisco.com)

Table 1 ISA Ordering Information

Part Number	Description
SA-ISA	Integrated Services Adapter

CISCO SYSTEMS



**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  
11, Rue Camille Desmoulins  
92782 Issy Les Moulineaux  
Cedex 9  
France  
<http://www-europe.cisco.com>  
Tel: 33 1 58 04 60 00  
Fax: 33 1 58 04 61 00

**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/go/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 © 2000, Cisco Systems, Inc. All rights reserved. Printed in the USA. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, 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. (9912R) 3/00 LW