

Refurbished CISCO AIM-VPN-SSL-3 Datasheet

CISCO > ROUTERS

Cisco 1800 Series Integrated Services Routers

Supported Modules and Features, by Platform

Cisco 3725	X
Cisco 3825	X
Cisco 3745	X
Cisco 3845	X
AES and Triple Data Encryption Standard (3DES)	X
IPPCP	X
WebVPN SSL Encryption	X
IPv6 Cryptography in Hardware	X

Supported Features of Cisco IPsec and SSL VPN AIM

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/netso/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.

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
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

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

Width	5.25 in. (13.3 cm)
Height	0.95 in. (2.41 cm)
Depth	3.25 in. (8.26 cm)
Weight	0.60 lb (0.27 kg)

The next steps...

ORDER NOW

VIEW ONLINE

Tel: +44 (0)1279 408 777

Email: sales@gocomsys.com

Website: www.gocomsys.com