Data Sheet

Virtual Private Network Module

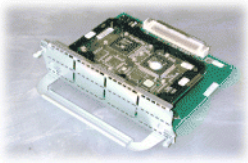
for Cisco 1700, 2600, 3600, and 3700 Series Routers

The Cisco 1700, 2600, 3600, and 3700 Series Virtual Private Network Module (VPN Module) optimizes virtual private network (VPN) platforms. The Cisco 1700, 2600, 3600 and 3700 Series VPN Module provides up to ten times the performance of software-only encryption by offloading the encryption processing from the router CPU. Ideal for use in enterprise branch offices for connecting remote offices, mobile users, partner extranets, or service provider managed-services customer premises equipment (CPE), the Cisco 1700, 2600, 3600, and 3700 Series VPN Module delivers a rich integrated package of routing, firewall, intrusion-detection, and VPN functions. As an integral component of Cisco VPN solutions, Cisco 1700, 2600, 3600, and 3700 Series VPN Module provides industry-standard encryption IP Security (IPSec), application-aware quality of service (QoS) and bandwidth management, together with robust perimeter security options. Figure 1 shows the VPN modules.

Figure 1:
Cisco 1700, 2600, 3600, and 3700 Series VPN Modules

AIM-VPN/ BP

MOD1700-VPN



NM-VPN/MP

AIM-VPN/ (EP II&HPII)

Table 1 shows the VPN module hardware availability.

Table 1 Cisco VPN Module Hardware Availability

VPN Module	Cisco 1700 Router	Cisco 2610 & 2611 Routers	Cisco 2620 & 2621 Routers	Cisco 2650 & 2651 Routers	Cisco 2600XM Router	Cisco 2691 Router	Cisco 3620 & 3640 Routers	Cisco 3660 Router	Cisco 3725 Router	Cisco 3745 Router
MOD1700-VPN	X									
AIM-VPN/BP		X	X	X	X	X				
AIM-VPN/EP				X	X	X			X	
AIM-VPN/HP								X		X
AIM-VPN/EP II						X			X	
AIM-VPN/HP II								X		X
NM-VPN/MP							X			

- *MOD1700-VPN*—This VPN module fits in all Cisco 1700 Series routers, including the Cisco 1710, 1720, 1721, 1750, 1751, and 1760 models. It fits in a slot inside the Cisco 1700 chassis, and encrypts data using the Data Encryption Standard (DES) and Triple DES (3DES) algorithms at speeds suitable for a full-duplex T1/E1 serial connection. (Up to 8 Mbps of 3DES performance. The maximum is based on a 1400-byte packet size.)
- *AIM-VPN/Base Performance (BP)*—This advanced interface module (AIM) can be added to all current Cisco 2600 Series routers, including Cisco 2600, 2600XM, and 2691 routers. It provides hardware-based encryption services with up to 10-Mbps of 3DES performance for Cisco 2600 and 2600XM. (The maximum is based on a 1400-byte packet size.)
- *AIM-VPN/Enhanced Performance (EP)*— This AIM VPN module can be added to all current Cisco 2600, 2600XM, and 2691 routers as well as the Cisco 3725. This module takes advantage of the Cisco 2650, 2651, 2600XM, 2691, and 3725 router speeds, and is not recommended for Cisco 2610, 2611, 2620, and 2621 routers. It provides hardware-based encryption services with up to 14 Mbps of 3DES performance in the Cisco 2650 and 2651, and up to 15 Mbps of 3DES performance on Cisco 2600XMs. (The maximum is based on a 1400-byte packet size.)
- *VPN/Mid Performance (MP)*—This network module is supported on all current Cisco 3620 and 3640 platforms to provide hardware-based encryption services with up to 18 Mbps of 3DES performance. (The maximum is based on a 1400-byte packet size.)
- *AIM-VPN/High Performance (HP)*—This AIM VPN module can be added to the Cisco 3660 and Cisco 3745 models to provide hardware-based encryption services with up to 42 Mbps of 3DES performance. (The maximum is based on a 1400-byte packet size.)
- *AIM-VPN/Enhanced Performance (EP II)*— This AIM VPN module can be added to Cisco 2691 and 3725 routers. This module offers DES, 3DES, and the new Advanced Encryption Standard (AES) from the National Institute for Standards (http://csrc.nist.gov/encryption/aes/). It supports hardware-assisted compression services, where bandwidth conservation may lower network connection costs. This module can provide hardware-based encryption services up to 80 Mbps 3DES performance in Cisco 2691 routers and 150 Mbps in Cisco 3725. (The maximum is based on a 1400-byte packet size.)

- *AIM-VPN/High Performance (HP II)*— This AIM VPN module can be added to Cisco 3745 and 3660 routers. This module also offers DES, 3DES, and AES. It supports hardware-assisted compression services where bandwidth conservation may lower network connection costs. This model can provide hardware-based encryption services up to 180 Mbps 3DES performance in Cisco 2691 routers. (The maximum is based on 1400-byte packet size.)

In addition to encryption processing, the Cisco 1700, 2600, 3600, and 3700 Series VPN Module handles numerous other IPSec-related tasks, including hashing, key exchange, and storage of security associations—freeing the main processor and memory to perform other router, voice, firewall, and intrusion-detection functions. Tables 2 and 3 list the features of the VPN module.

Table 2 Feature Support

Feature	Description
Physical	Network module, AIM, and encryption slot, and (Cisco 1700) form factors
Platform Support	Cisco 1700, 2600, 3600, and 3700 Series Routers
Hardware Prerequisites	Available encryption slot for Cisco 1700; available AIM slot for Cisco 2600, 2600XM, 2691, 3660, and 3700 series; available network-module slot for Cisco 3620 and 3640
Encryption Supported	All support IPSec DES, 3DES, Authentication: Rivest, Shamir Aldeman algorithm (RSA) and Diffie Hellman, Data integrity: SHA-1 and MD5 Only new AIM-VPN/EPII and HPII support IPSec with AES in Hardware
Hardware-Based DES and 3DES Encryption	Increases overall encryption performance over software encryption methods, supported on all VPN Modules
Hardware-Based AES, with 128, 192, and 256 Keys	New AES standard. Keys supported: 128, 192, and 256. Supported on EPII and HPII, hardware is optimized for 128
IPSec Hardware-based Compression	Layer 3 IPPCP LZS AIM-VPN/EP II and AIM-VPN/HPII Only
IPSec Software-based Compression	Software-based Layer 3 IPPCP is now enabled to use with current VPN modules. This allows IPPCP to run on the Router CPU (requires 12.2(13)T or later)
Software Prerequisites	Cisco IOS® Software with the IPSec feature
Throughput	Up to 8 Mbps for Cisco 1700; up to 10 Mbps for Cisco 2600; up to 14 Mbps for Cisco 2600XMs; up to 18 Mbps for Cisco 3620 and 3640; up to 40 Mbps for Cisco 3660 (with 1400-byte packets). With AIM-VPN/EPII and AIM-VPN/HPII: Up to 80 Mbps for Cisco 2691; up to 150 Mbps for Cisco 3725; up to 180 Mbps for Cisco 3745 (optimized for 3DES and AES).
Number of Encryption Modules per Router	One
Minimum Cisco IOS Version Required	MOD1700-VPN: Supported on Releases 12.1(1)XC, 12.1(2)T, and later on the Cisco 1700 Series AIM-VPN/BP, NM-VPN/MP, and AIM-VPN/HP: Supported on Releases 12.1(5)T or later on the Cisco 2600 and 3600 Series AIM-VPN/EP Supported on Releases 12.2(2)T or later on the Cisco 2600 Series AIM-VPN EPII and HPII: Supported on Releases 12.2(13)T or later on the Cisco 2691 and 3700 Series

Table 2 Feature Support

Feature	Description
Maximum Number of Encrypted Tunnels	Up to 100 encrypted tunnels on Cisco 1700; up to 300 on Cisco 2600; up to 800 on Cisco 2650 with AIM-VPN/ EP; up to 800 on Cisco 2600XMs, 2691, and 3725; up to 800 on Cisco 3620 and 3640, and up to 2,000 tunnels on Cisco 3660 and 3745
Standards Supported	IPSec/Internet Key Exchange (IKE): RFCs 2401-2411, 2451

Table 3 Features and Benefits of the Cisco VPN Module

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	The IPSec MIBs allow Cisco IPSec configuration monitoring and can be integrated in a variety of VPN management solutions.
Certificate Support Enables Automatic Authentication using Digital Certificates	Scales encryption use for large networks requiring secure connections between multiple sites
VPN modules Easily Integrated into New and Existing Cisco 1700, 2600, 3600, and 3700 Series Routers	Significantly reduces the system costs, management complexity, and deployment effort over multiple box solutions
Management	CiscoWorks VPN/Security Management Solution (VMS) is a comprehensive management tool for mid- to large-scale VPN deployments; can configure both IPSec tunnels and firewall rules VPNSC (VPN Solution Center 2.0 is a service-provider MPLS/IPSec management tool)
IPSec Provides Confidentiality, Data Integrity, and Data Origin Authentication	Enables the secure use of public-switched networks and the Internet for WANs

Features

Cisco fully supports the entire set of RFCs describing IPSec and related protocols—RFCs 2401-2410. In particular, Cisco supports the following features:

- *AES*—The National Institute of Standards and Technology (NIST) created AES as a new Federal Information Processing Standard (FIPS) publication. AES has a variable key length—the algorithm can specify a 128-bit key (default), a 192-bit key, or a 256-bit key. The new AIM-VPN/EPII and HPII are the only modules that support AES in hardware. Visit: http://csrc.nist.gov/encryption/aes/ for details.
- *IPSec*—This feature 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.
- *IKE*—This feature provides security association management. IKE authenticates each peer in an IPSec transaction, negotiates security policy, and handles the exchange of session keys. It is based on the Internet Security Association Key Management Protocol (ISAKMP/Oakley).

- *Certificate management*—Cisco fully supports the X509.V3 certificate system for device authentication and the Cisco Simple Certificate Enrollment Protocol (SCEP), a protocol for communicating with certificate authorities. Several vendors, including Verisign, Entrust Technologies, and Microsoft support Cisco SCEP and are interoperable with Cisco devices.
- *DES, 3DES, and AES*— DES, 3DES, and AES encryption is required for all packets destined for an IPSec tunnel. The Cisco 1700, 2600, 3600, and 3700 Series VPN Module encrypts data with DES or 3DES, freeing the main processor for other tasks. AIM-VPN/EPII and HPII can also support AES.
- *RSA signatures and Diffie-Hellman*—These are used every time an IPSec tunnel is established to authenticate the IKE signature authority. Diffie-Hellman is used to derive the shared secret encryption key for the protection of data across the IKE signature authority, including the negotiation of the IPSec policy to be used.
- *Enhanced security*—Hardware-based cryptography offers several security advantages over software-based solutions, including enhanced protection of keys.

Certifications

Cisco recognizes that certifications and evaluations are important to our customers, and we continue to be a leader in providing certified and evaluated products to the marketplace. Cisco continues to work with international security standards bodies to help shape the future of certified and evaluated products, and to accelerate certification and evaluation processes. Certification and evaluation are considered at the earliest part of the product development cycle; Cisco continues to position its security products to ensure that customers have the certified and evaluated products they need.

FIPS

The Cisco 1700, 2600, and 3600 Series VPN Modules meet FIPS 140-1 Level 2 security. Currently only the Cisco 2611, 2651, 3640, and 3660 have FIPS 140-1 Level 2. The NIST has upgraded FIPS 140-1 to FIPS 140-2. Cisco will now be submitting a number of our routers for FIPS 140-2, Level 2. For the current status of Cisco products certified for FIPS, visit: http://www.cisco.com/warp/public/779/largeent/issues/security/secvpncert.html.
And visit: http://csrc.nist.gov/cryptval/

ICSA IPSec

ICSA is a commercial security certification body that offers ICSA IPSec and ICSA Firewall Certification for various types of security products. Cisco participates in ICSA's IPSec program and its Firewall program. For the current status of Cisco products certified for ICSA, visit:

http://www.cisco.com/warp/public/779/largeent/issues/security/secvpncert.html.

Common Criteria

Common Criteria is an international standard for evaluating IT security. It was developed by a consortium of countries to replace a number of existing country-specific security assessment processes, and was intended to establish a single standard for international use. Currently, fourteen countries officially recognize the Common Criteria. Several versions of Cisco IOS IPsec software and Cisco routers have now been evaluated under the Australasian Information Security Evaluation Program (AISEP) against the ITSEC or the Common Criteria.

For the current status of Cisco products certified for Common Criteria, visit: http://www.cisco.com/warp/public/779/largeent/issues/security/secvpncert.html.

And visit: http://www.dsd.gov.au/infosec/aisep/EPL/ns.html - ciscoipsec

Cisco Management Software for IPSec VPNs

Management Tools for Enterprise-Based VPNs

CiscoWorks VPN/Security Management Solution

CiscoWorks VPN/Security Management Solution (VMS), an integral part of the SAFE Blueprint for network security, combines Web-based tools for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network- and host-based intrusion detection systems (IDSs). CiscoWorks VMS delivers the industry's first robust and scalable foundation and feature set that addresses the needs of small- and large-scale VPN and security deployments.

CiscoWorks VMS v2.1 includes management centers for Cisco VPN routers, Cisco PIX® Firewalls, IDS sensors, and a monitoring center for security.

CiscoWorks VMS v2.1 features:

- Management centers for VPN routing
- Monitoring center for security
- New and consistent user interface, workflow, and roles definition
- Smart Rules Hierarchy and flexible grouping for rapid policy replication
- Comprehensive change-control and auditing features
- Centralized role-based access control (RBAC) support

The CiscoWorks Router Management Center, a component of CiscoWorks VMS, provides scalable security management for the configuration and deployment of VPN connections. The CiscoWorks Router Management Center provides a powerful, flexible, and intuitive way to configure and deploy large-scale and site-to-site VPN connections. It provides administrative user-approval controls, enabling large enterprises to define multiple administrative and operational roles. In addition, the CiscoWorks Router Management Center provides an intuitive GUI interface for simplified policy definitions, a hierarchical inheritance model, flexible deployment options and enhanced reporting capabilities.

CiscoWorks VPN Monitor is a Web-based management tool that allows network administrators to collect, store, and view information on IPSec VPN connections for remote-access or site-to-site VPN terminations. Multiple devices can be viewed from an easy-to-use dashboard that is configured using a Web browser. CiscoWorks VPN Monitor uses the IPSec Management Information Base (MIB) supported by all Cisco VPN modules

CiscoWorks VMS provides one integrated management solution to configure, monitor, and troubleshoot firewalls, VPNs, and network- and host-based IDSs. CiscoWorks VMS uniquely offers multi-faceted scalability features, including Auto Update and Smart Rules Hierarchy, to enable customers to easily deploy large-scale security infrastructures.

Management Tools for Service-Provider VPN Networks

Cisco VPN Solution Center v2.2

With Cisco VPN Solutions Center (VPNSC) Release 2.2 a provider can now manage both IPSec and MPLS-based IP VPNs with one tool. Cisco VPNSC offers a suite of service management solutions that enable service providers to effectively plan, provision, operate, and bill for VPN services.

As service providers build VPNs that include WAN switches, routers, firewalls, VPN concentrators, and Cisco IOS Software, they must be able to seamlessly manage these devices across the network infrastructure and provide service-level agreements (SLAs) to their customers. They also need to enable business customers to personalize their access to network services and applications. Cisco VPNSC offers the first cost effective, carrier-class VPN service management solution allowing service providers to rapidly deploy outsourced VPN services that businesses want today. The portfolio combines robust IPSec VPN services with all the features of Cisco IOS Software on platforms for every site, from the small office to corporate headquarters, and includes:

- Support of Multi-VRFs in a single customer edge router, extending limited MPLS functionality to customer edge routers (see Cisco Product Bulletin, No. 1575)
- IPSec VPN provisioning; configures an IKE and IPSec tunnel between all Cisco IOS Software devices
- Comprehensive hub-and-spoke, full-mesh, and partial-mesh VPN topology views
- Arbitrary VPN topologies; formed by adding multiple sites to the VPN, including extranet and intranet VPNs
- Service provisioning and auditing for site-to-site IPSec
- SLA monitoring for IPSec and MPLS
- Task manager
- Events APIs including TIBCO event bus and Common Object Request Broker Architecture (CORBA) event API
- Extensible Markup Language (XML) interface for easy import and export of data to the Cisco VPNSC repository

Cisco VPNSC v2.2 supports the Cisco 1700 and 2600 Series routers as both MPLS CPE and as IPSec devices. This allows the provider to manage both IPSec and MPLS-based IP VPNs. The Cisco 2691 model is being tested to offer provider-edge support in a future Cisco IOS Software release, but this feature is not currently supported.

Cisco VPNSC v2.2 also supports the Cisco 3600 and 3700 Series routers as both MPLS CPE and as IPSec devices. In addition, Cisco 3640, 3660, and 3700 Series routers can be supported as provider-edge devices with Cisco VPNSC v2.2.

Cisco 1700, 2600, 3600, and 3700 Series VPN Module Software

The Cisco 1700 Series VPN Module is supported on Cisco IOS Software Releases 12.1(1)XC, 12.1(2)T, and later. The Cisco 2600, 3600, and 3700 Series VPN Module is supported on Cisco IOS 12.1(5)T and later. The Cisco 2600XMs, 2691, and 3700 Series require Cisco IOS Software Releases 12.2(8)T and later. Cisco IOS Software IP Firewall plus IPSec 3DES software contain all the IPSec, firewall, and plus features of Cisco IOS Software, and support both 3DES and DES (56-bit) encryption, while the IPSec 56 release supports DES (56-bit) encryption.

A Cisco 1700, 2600, 3600, or 3700 Series router with a VPN module will run with any Cisco IOS Software feature set, but the VPN module is used only with IPSec feature sets. For example, Cisco IOS IP-only Software Release 12.1(5)T will run on a Cisco 1700, 2600, or 3600 Series router with the VPN module installed, but it will not be enabled for IPSec and will not exploit the features of the VPN module. Table 3 lists the software memory requirements for the VPN module.

Table 4 Cisco 1700, 2600, 3600, and 3700 Series IPSec Software Memory Requirements with Cisco IOS Software Release 12.2(13)T

Product Name2600/ 3600/3660/ 3700	Image Name	Software Image	Required Flash Memory 2600/3620/ 3640/3660/ 3700	Required DRAM Memory 2600/ 3620/3640/ 3660/3700	Runs From
S26/36AL	Enterprise Plus IPSec 56 (DES)	C2600/3620/3640/3660-jk8s-mz	16/32/32/32/NA	64/64/96/96/NA	RAM
S26/36AK2	Enterprise Plus IPSec 3DES	C2600/3620/3640/3660-jk9s-mz	16/32/32/32/NA	64/64/96/96/NA	RAM
S26/36AHL	Enterprise IP/FW/IDS Plus IPSec 56	C2600/3620/3640/3660-jk8o3s-mz	16/32/32/32/NA	64/64/96/96/NA	RAM
S26/36/37AHK2	Enterprise IP/FW/IDS Plus IPSec 3DES	C2600/3620/3640/3660-jk9o3s-mz	16/32/32/32/32	64/64/96/96/128	RAM
S26/36AR1L	ENTERPRISE/SNASW PLUS IPSEC 56	C2600/3620/3640/3660-a3jk8o3s-mz	16/32/32/32/NA	64/64/96/96/NA	RAM
S26/36AR1K2	ENTERPRISE/SNASW PLUS IPSEC 3DES	C2600/3620/3640/3660-a3jk9s-mz	16/32/32/32/NA	64/64/96/96/NA	RAM
S26/36/37CL	IP Plus IPSec 56 (DES)	C2600/3620/3640/3660/3700-ik8s-mz	16/16/16/32/NA	64/64/64/64/NA	RAM
S26/36/37CK2	IP PLUS IPSEC 3DES	C2600/3620/3640/3660/3700-ik9s-mz	16/16/16/32/32	64/64/64/64/128	RAM
S26/36CHL	IP/FW/IDS Plus IPSec 56 DES	C2600/3620/3640/3660-ik8o3s-mz	16/16/16/32/NA	64/64/64/64/NA	RAM
S26/36/37CHK2	IP/FW/IDS Plus IPSec 3DES	C2600/3620/3640/3660/3700-ik9o3s-mz	16/16/16/32/32	64/64/64/64/128	RAM
S17C7HK8	Cisco 1700 IOS IP/ ADSL/FW/IDS PLUS IPSEC 56	C1700-k8o3sy7-mz	8	48	RAM
S17C7HK9	Cisco 1700 IOS IP/ ADSL/FW/IDS PLUS IPSEC 3DES	C1700-k9o3sy7-mz	8	48	RAM

Table 4 Cisco 1700, 2600, 3600, and 3700 Series IPSec Software Memory Requirements with Cisco IOS Software Release 12.2(13)T

Product Name2600/ 3600/3660/ 3700	Image Name	Software Image	Required Flash Memory 2600/3620/ 3640/3660/ 3700	Required DRAM Memory 2600/ 3620/3640/ 3660/3700	Runs From
S17C7V8K8	Cisco 1700 IOS IP/ ADSL/VOX/FW/IDS PLUS IPSEC 56	C1700-k8o3sv8y7-mz	16	64	RAM
S17C7V8K9	Cisco 1700 IOS IP/ ADSL/VOX/FW/IDS PLUS IPSEC 3DES	C1700-k9o3sv8y7-mz	16	64	RAM
S17C7K8	Cisco 1700 IOS IP/ ADSL PLUS IPSEC 56	C1700-k8sy7-mz	8	48	RAM
S17C7K9	Cisco 1700 IOS IP/ ADSL PLUS IPSEC 3DES	C1700-k9sy7-mz	8	48	RAM
S17CV8K8	Cisco 1700 IOS IP/ ADSL/VOX PLUS IPSEC 56	C1700-k8sv8y7-mz	16	64	RAM
S17CV8K9	Cisco 1700 IOS IP/ ADSL/VOX PLUS IPSEC 3DES	C1700-k9sv8y7-mz	16	64	RAM
S17Q7HK8	Cisco 1700 IOS IP/ ADSL/IPX/AT/IBM/FW/ IDS PLUS IPSEC 56	C1700-bk8no3r2sy7-mz	16	64	RAM
S17Q7HK9	Cisco 1700 IOS IP/ ADSL/IPX/AT/IBM/FW/ IDS PLUS IPSEC 3DES	C1700-bk9no3r2sy7-mz	16	64	RAM
S17Q7V8K8	Cisco 1700 IOS IP/ ADSL/IPX/AT/IBM/ VOX/FW/IDS PLUS IPSEC 56	C1700-bk8no3r2sv8y7-mz	32	96	RAM
S17Q7V8K9	Cisco 1700 IOS IP/ ADSL/IPX/AT/IBM/ VOX/FW/IDS PLUS IPSEC 3DES	C1700-bk9no3r2sv8y7-mz	32	96	RAM

Export Regulations on the VPN Module

DES, 3DES, and AES software for the Cisco VPN Module is controlled by U.S. export regulations on encryption products. The module itself is 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 and 3DES software enforces these requirements. For more details, visit http://www.cisco.com/wwl/export/crypto/.

Specifications

Product Number and Description

- MOD1700-VPN: DES/3DES VPN Module 1700
- AIM-VPN/BP: DES/3DES VPN Encryption AIM—Base Performance
- AIM-VPN/EP-DES/3DES VPN Encryption AIM—Enhanced Performance
- NM-VPN/MP-DES/3DES VPN Encryption NM—Mid Performance
- AIM-VPN/HP-DES/3DES VPN Encryption AIM—High Performance
- AIM-VPN/EPII-DES/3DES/AES and Compression VPN Encryption AIM—Enhanced Performance
- AIM-VPN/HPII-DES/3DES/AES and Compression VPN Encryption AIM—High Performance

Standards (Cisco IOS Software IPSec)

- IPSec (RFCs 2401-2410)
- IPSec ESP using DES/3DES (RFC 2406)
- IPSec authentication header using MD5 or SHA (RFCs 2403-2404)
- IKE (RFCs 2407-2409)

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

Dimensions and Weight

Module	MOD1700-VPN	AIM-VPN/BP	AIM-VPN/EP	NM-VPN/MP	AIM-VPN/HP
Width	2.25 in. (5.72 cm)	5.25 in. (13.34 cm)	5.25 in. (13.34 cm)	7.10 in. (18.03 cm)	5.25 in. (13.34 cm)
Height	0.70 in. (1.78 cm)	.95 in. (2.41 cm)	.95 in. (2.41 cm)	1.65 in. (4.19 cm)	.95 in. (2.41 cm)
Depth	3.75 in. (9.53 cm)	3.25 in. (8.26 cm)	3.25 in. (8.26 cm)	7.20 in. (18.29 cm)	3.25 in. (8.26 cm)
Weight	0.078 lb (35.5g)	.60 lb. (.27 kg)	.60 lb. (.27 kg)	1.1 lb. (.5 kg)	.6 lb. (.27 kg)

Regulatory Compliance, Safety, EMC, Telecom, Network Homologation

When installed in a Cisco 1700, 2600, 3600, or 3700 Series router, the VPN module does not change the standards (Regulatory Compliance, Safety, EMC, Telecom, Network Homologation) of the router itself. See data sheets for the Cisco 1700, 2600, 3600, and 3700 Series routers.

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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 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 Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia 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

LW3851 11/02