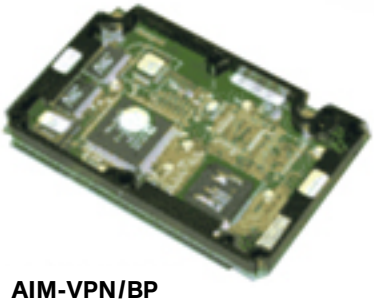
Data Sheet

Virtual Private Network Modules for the Cisco 1700, 2600, 3600, and 3700 Series

The Cisco 1700, 2600, 3600, and 3700 Series Router Virtual Private Network Modules (VPN Modules) optimize the platforms for virtual private networks (VPNs).

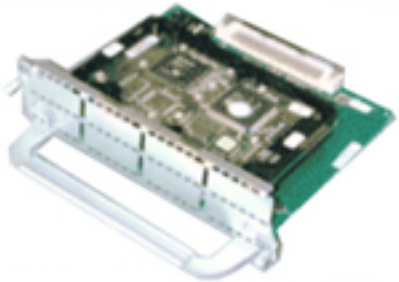
The Cisco 1700, 2600, 3600, and 3700 Series VPN Modules provide up to 10 times the performance over software-only encryption by offloading the encryption processing from the router central processing unit (CPU). Ideal for use in enterprise branch offices for connecting remote offices, mobile users, and partner extranets or service provider managed-services customer premises equipment (CPE), the Cisco 1700, 2600, 3600, and 3700 Series VPN Modules delivers a rich integrated package of routing, firewall, intrusion-detection, and VPN functions. As an integral component of Cisco VPN solutions, the Cisco 1700, 2600, 3600, and 3700 Series VPN Modules provide industry-standard encryption (IPSec), application-aware quality of service (QoS) and bandwidth management, together with robust perimeter security options.

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



AIM-VPN/BP

MOD1700-VPN



NM-VPN/BP

VPN/(BPII, EPII, HPII) and AIM-VPN/(BPII-PLUS, EPII-PLUS, HPII-PLUS)

The VPN module hardware is available in these forms:

	1700	2610/11	2620/21	2650/51	2600XM	2691	3620/40	3660	3725	3745
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/BPII					X					
AIM-VPN/EP II						X			X	
AIM-VPN/HP II								X		X
NM-VPN/MP							X			
AIM-VPN/ BPII-PLUS					X					
AIM-VPN/ EPII-PLUS						X			X	
AIM-VPN/ HPII-PLUS								X		X

- *MOD1700-VPN*—This VPN module fits in ALL 1700 Series Routers, which includes the Cisco 1710, 1720, 1721, 1750, 1751, and 1760 models. This VPN Module fits in a slot inside the Cisco 1700 chassis, encrypts data using the Data Encryption Standard (DES) and 3DES algorithms at speeds suitable for a full-duplex T1/E1 serial connection (up to 8-Mbps triple Data Encryption Standard (3DES). (max based on 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 the Cisco 2600s, 2600XMs and 2691) to provide hardware-based encryption services with up to 10-Mbps triple Data Encryption Standard (3DES) performance for the Cisco 2600s and 2600XMs (max based on 1400 byte packet size).
- *AIM-VPN/Enhanced Performance (EP)*—This advanced interface module (AIM) VPN Module can be added to all current Cisco 2600, 2600XM, and 2691 as well as the Cisco 3725. This AIM is designed to take advantage of the Cisco 2650/51, 2600XMs, 2691 and 3725's speed and is not recommended for the Cisco 2610/11 and 2620/21. This model can provide hardware-based encryption services with up to 14-Mbps triple Data Encryption Standard (3DES) performance in the Cisco 2650/51, up to 15-Mbps 3DES performances on the Cisco 2600XMs. (max based on 1400 byte packet size).
- *Network module (NM)-VPN/Mid Performance (MP)*—This network module is supported on all current Cisco 3620 and Cisco 3640 platforms to provide hardware-based encryption services with up to 18-Mbps 3DES performance (max based on 1400 byte packet size).
- *AIM-VPN/High Performance (HP)*—This AIM can be added to the Cisco 3660 and Cisco 3745 models to provide hardware-based encryption services with up to 42-Mbps-3DES performance (max based on 1400 byte packet size).

- *AIM-VPN/Base Performance (BP II) combines DES/3DES/AES (optimized for AES128 only) and Layer 3 (IPPCP) compression for Cisco 2600XM*— This new advanced interface module (AIM) VPN Module can be added to current Cisco 2600XM. This VPN Module offers DES/3DES and new AES (Advanced Encryption standard) from the National Institute for Standards (http://csrc.nist.gov/encryption/aes/). This VPN module is optimized for AES128 key only and is ideal for network that require only AES128 encryption. In addition these VPN Modules support hardware-assisted Layer 3 (IPPCP) compression services where bandwidth conservation may lower network connection costs. This module can provide hardware-based encryption services up to 20-Mbps 3DES/AES128 performance in 2611 and up to 22 Mbps 3DES/AES128 performance on the Cisco 2651XM (max based on 1400 byte packet size).
- *AIM-VPN/Enhanced Performance (EP II) combines DES/3DES/AES (optimized for AES128 only) and Layer 3 (IPPCP) compression for Cisco 2691 and Cisco 3735*—This advanced interface module (AIM) VPN Module can be added to current Cisco 2691, and Cisco 3725. This Module offers DES/3DES and new AES (Advanced Encryption standard) from the National Institute for Standards (http://csrc.nist.gov/encryption/aes/). This VPN module is optimized for AES128 key only and is ideal for network that require only AES128 encryption. In addition these VPN Modules support hardware-assisted Layer 3 (IPPCP) compression services where bandwidth conservation may lower network connection costs. This module can provide hardware-based encryption services up to 80-Mbps 3DES/AES128 performance in Cisco 2691 and 150-Mbps 3DES/AES128 performance in Cisco 3725 (max based on 1400 byte packet size).
- *AIM-VPN/High Performance (HP II) combines DES/3DES/AES(optimized for AES128 only) and Layer 3 (IPPCP) compression for Cisco 3660 and Cisco 3745*— This advanced interface module (AIM) VPN Module can be added to current Cisco 3745, and Cisco 3660 platforms. This Module also offers DES/3DES and new AES from National Institute for Standards (Advanced Encryption standard) (http://csrc.nist.gov/encryption/aes/). This VPN module is optimized for AES128 key only and is ideal for networks that require only AES128 encryption. In addition these VPN Modules support hardware-assisted Layer 3 (IPPCP) compression services where bandwidth conservation may lower network connection costs. This model can provide hardware-based encryption services up to 180-Mbps 3DES/AES128 performance in the Cisco 3745 (max based on 1400 byte packet size).
- *AIM-VPN/Base Performance PLUS (BPII-PLUS) combines DES/3DES/AES (optimized for AES128, AES192, AES256) and Layer 3 (IPPCP) compression for Cisco 2600XM*—This new advanced interface module (AIM) VPN Module can be added to current Cisco 2600XM. This VPN Module offers DES/3DES and new AES (Advanced Encryption standard) from the National Institute for Standards (http://csrc.nist.gov/encryption/aes/). This VPN module is optimized for all AES key sizes (AES128, AES192, and AES256). In addition these VPN Modules support hardware-assisted Layer 3 (IPPCP) compression services where bandwidth conservation may lower network connection costs. This module can provide hardware-based encryption services up to 20-Mbps 3DES/AES(128,192,256) performance in 2611 and up to 22 Mbps 3DES/AES(128,192,256) performance on the Cisco 2651XM (max based on 1400 byte packet size).
- *AIM-VPN/Enhanced Performance PLUS (EP II-PLUS) combines DES/3DES/AES (optimized for AES128, AES192, AES256) and Layer 3 (IPPCP) compression for Cisco 2691 and Cisco 3735*—This advanced interface module (AIM) VPN Module can be added to current Cisco 2691, and Cisco 3725. This Module offers DES/3DES and new AES (Advanced Encryption standard) from the National Institute for Standards (http://csrc.nist.gov/encryption/aes/). This VPN module is optimized for all AES key sizes (AES128, AES192, and AES256). In addition these VPN Modules support hardware-assisted Layer 3 (IPPCP) compression services where

bandwidth conservation may lower network connection costs. This module can provide hardware-based encryption services up to 80-Mbps 3DES/AES (128, 192, 256) performance in Cisco 2691 and 150-Mbps 3DES/AES (128, 192, 256) performance in Cisco 3725 (max based on 1400 byte packet size).

- *AIM-VPN/High Performance PLUS (HP II-PLUS) combines DES/3DES/AES (optimized for AES128, AES192, AES256) and Layer 3 (IPPCP) compression for Cisco 3660 and Cisco 3745*—This advanced interface module (AIM) VPN Module can be added to current Cisco 3745, and Cisco 3660 platforms. This Module also offers DES/3DES and new AES from National Institute for Standards (Advanced Encryption standard) (http://csrc.nist.gov/encryption/aes/). This VPN module is optimized for all AES key sizes (AES128, AES192, and AES256). In addition these VPN Modules support hardware-assisted Layer 3 (IPPCP) compression services where bandwidth conservation may lower network connection costs. This model can provide hardware-based encryption services up to 180-Mbps 3DES/AES(128, 192, 256) performance in the Cisco 3745 (max based on 1400 byte packet size).

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

Table 1

Feature	Description
Physical	Network Module, AIM and Encryption Slot, and (1700) form factors
Platform Support	Cisco 1700, 2600, 3600 and 3700 Series
Hardware Prerequisites	Available Encryption slot for 1700, AIM slot for Cisco 2600, 2600XM, 2691, 3660, and 3700 series; available NM slot for Cisco 3620 and 3640
Encryption Supported	• All support IPSec DES,3DES, Authentication: RSA and Diffie Hellman, Data integrity: SHA-1 and MD5 • AIM-VPN/BPII, AIM-VPN/EPII and AIM-VPN/HPII support IPSec with AES in Hardware (optimized for AES128 only) • The new AIM-VPN/BPII-PLUS, AIM-VPN/EPII-PLUS and AIM-VPN/HPII-PLUS support IPSec with AES in Hardware (optimized for all 3 AES key sizes: AES128, AES192, and AES256)
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, HPII, and BPII. Hardware is optimized for AES128 only. The BPII-PLUS, EPII-PLUS and HPII-PLUS are optimized for all three key sizes (AES128, AES192, AES256)
IPSec Hardware-based Compression	Layer 3 IPPCP compression AIM-VPN/BPII, AIM-VPN/EP II, AIM-VPN/HPII and AIM-VPN/ BPII-PLUS, AIM-VPN/EPII-PLUS and AIM-VPN/HPII-PLUS
IPSec Software-based Compression	Software based Layer 3 IPPCP compression 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

Table 1 (Continued)

Feature	Description
Throughput	• Up to 8 Mbps for Cisco 1700, up to 10 Mbps for Cisco 2600, up to 22 Mbps for the Cisco 2600XMs, up to 18 Mbps for Cisco 3620 and 3640, and up to 40 Mbps for the 3660. (With 1400-byte packets) • With AIM-VPN/BPII, AIM-VPN/EPII and AIM-VPN/HPII up to 22 Mbps 2651XM, up to 80 Mbps for 2691, up to 150 Mbps for 3725, and up to 180 for the 3745 (optimized for 3DES and AES 128) • With AIM-VPN/BPII-PLUS, AIM-VPN/EPII-PLUS and AIM-VPN/HPII-PLUS up to 22 Mbps 2651XM, up to 80 Mbps for 2691, up to 150 Mbps for 3725 and up to 180 Mbps for the 3745 (DES/3DES/AES128/AES192/AES256)
Number of Encryption Modules per Router	1
Minimum Cisco IOS Version Required	• MOD1700-VPN: Supported on Releases 12.1(1) XC, 12.1(2) T, and later of the 1700 series • AIM-VPN/BP, NM-VPN/MP, and AIM-VPN/HP Supported on Releases 12.1(5) T or later 2600, and 3600 Series • AIM-VPN/EP Supported on 12.2(2) T or later 2600 Series • AIM-VPN/BPII for 2600XM Series 12.2(15)ZJ or later is required • AIM-VPN EPII and HPII for 2691 and 3700 Series 12.2(13) T or later is required • AIM-VPN/BPII-PLUS, EPII-PLUS and HPII-PLUS are all supported in 12.3(5c)/12.3(6) or later in mainline releases and 12.3(7)T or later in T-train releases
Maximum Number of Encrypted Tunnels	Up to 100 encrypted tunnel on a 1700, up to 300 tunnels on Cisco 2600, up to 800 for 2650, up to 800 tunnels for the Cisco 2600XMs, 2691, and 3725, up to 800 tunnels on Cisco 3620 and 3640, and up to 2,000 tunnels on Cisco 3660 and 3745.
Standards Supported	IPSec/IKE: RFCs 2401-2410, 2411, 2451

Table 2

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 SP 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 Request For Comments (RFCs) describing IPSec and related protocols, RFCs 2401-2410. In particular, Cisco supports the following features:

- *AES*—The Advanced Encryption Standard (AES). The National Institute of Standards and Technology (NIST) created AES, as a new Federal Information Processing Standard (FIPS) publication, and is privacy transforms for IPSec and Internet Key Exchange (IKE). 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/BPII, AIM-VPN/EPII and HPII are optimized for AES128 only in hardware. The new AIM-VPN/BPII-PLUS, AIM-VPN/EPII-PLUS and HPII-PLUS are optimized for all three AES key sizes: AES128, AES192, and AES256 in hardware. See for details on AES (http://csrc.nist.gov/encryption/aes/).
- *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.
- *IKE*—Based on the Internet Security Association Key Management Protocol, or ISAKMP/Oakley, provides security association management. IKE authenticates each peer in an IPSec transaction, negotiates security policy, and handles the exchange of session keys.
- *Certificate management*—Cisco fully supports the X509.V3 certificate system for device authentication and the 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, 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 while freeing the main processor for other tasks. AIM-VPN/BPII, AIM-VPN/EPII and HPII can also support AES.
- *RSA signatures and Diffie-Hellman*—Used every time an IPSec tunnel is established to authenticate the IKE SA. Diffie-Hellman is used to derive the shared secret encryption key for the protection of data across the IKE SA, 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 is committed to maintaining an active product certification and evaluation program for customer's worldwide. We recognize 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. We also will continue to work with international security standards bodies to help shape the future of certified and evaluated products, and will work to accelerate certification and evaluation processes. Certification and evaluation are considered at the earliest part of our product development cycle, and we will continue to position our security products to insure that customers have a variety of certified and evaluated products to meet their needs.

FIPS

The Cisco 1700, 2600 and 3600 Series and VPN modules have been designed to meet FIPS 140-1 Level 2 security. Currently only Specific model of the 2611, 2651, and 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. See Products by Certification for the current status of Cisco products certified for FIPS:

- http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking_solutions_audience_business_benefit0900aecd8009a16f.html
- 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 as well as their Firewall program. See Products by Certification for the current status of Cisco products certified for ICSA:

- http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking_solutions_audience_business_benefit0900aecd8009a16f.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 version of IOS IPsec and Cisco routers have now been evaluated under the Australasian Information Security Evaluation Program (AISEP) against the ITSEC or the Common Criteria.

See Products by Certification for the current status of Cisco products certified for Common Criteria:

- http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking_solutions_audience_business_benefit0900aecd8009a16f.html
- http://www.aisep.gov.au/infosec/evaluation_services/epl/network_security/Cisco_IPSec.html

Cisco Management Software for IPSec VPNs

Management Tools for Enterprise based VPN Networks

CiscoWorks VPN/Security Management Solution (VMS)

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 virtual private networks (VPNs), firewalls, and network and host-based intrusion detection systems (IDS). 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 2.1 includes Management Centers for Cisco Router Virtual Private Network (VPN) Routers, PIX Firewalls, Intrusion Detection (IDS) Sensors, and a Monitoring Center for Security.

Features:

- Management Centers for VPN Routing; and Monitoring Center for Security
- New and consistent user interface, workflow, and roles definition
- Includes 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 (Router MC), a component of the CiscoWorks VPN/Management Solution (VMS), provides scalable security management for the configuration and deployment of VPN connections. Router MC provides a powerful, flexible, and intuitive way to configure and deploy large-scale and site-to-site VPN connections. Router MC provides administrative user-approval controls for control over individual user and deployment permissions, enabling large enterprises to define multiple administrative and operational roles. In addition, Router MC 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. This dashboard provides the following capabilities. VPN Monitor uses the IPSec MIB supported by all Cisco Router VPN Modules

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

Management Tool for Service Provider VPN Network

VPN Solution Center 2.2

With the release of Cisco VPN Solutions Center (VPNSC) release 2.2 a provider can now manage both IPsec and MPLS-based IP VPNs with one tool. In addition, VPNSC offers a suite of service management solutions to 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 need 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. VPNSC now offers the first cost effective, carrier-class VPN service management for service providers to rapidly deploy outsourced VPN services that many businesses want today, the portfolio combines robust IPsec VPN services with all the other features of Cisco IOS software on platforms for every site, from the small office to corporate headquarters.

- Support of Multi-VRFs in a Single CE Extending Limited MPLS Functionality to CE Routers (see Product Bulletin, No. 1575)
- Provision IPSec IP VPNs by configuring an Internet Key Exchange (IKE) and IPSec tunnel between the Cisco devices—all Cisco IOS devices
- Comprehensive hub-and-spoke, full-mesh, and partial-mesh VPN topology views
- Form arbitrary VPN topologies 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 (scheduling)
- 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 VPN Solution Center repository

VPNSC 2.2 supports the Cisco 1700 and 2600 Series routers as both MPLS Customer Premise equipment (CPE) and as IPSec devices. This allows the provider to manage both IPsec and MPLS-based IP VPNs. The Cisco 2691 model is currently being tested to provide Provider Edge PE support at a future Cisco IOS release date but is not currently supported today.

VPNSC 2.2 also supports the Cisco 3600 and 3700 Series routers as both MPLS Customer Premise Equipment (CPE) and as IPSec devices. In addition, the Cisco 3640, 3660 and 3700 can be supported as Provider Edge PE devices with VPNSC 2.2.

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

The VPN module is supported on Releases 12.1(1) XC, 12.1(2) T, and later of the Cisco 1700 series The Cisco 2600, 3600, and 3700 Series VPN Module is supported on releases Cisco IOS 12.1(5) T and later of the Cisco IOS software. The Cisco 2600XMs, 2691 and 3700 Series require Cisco IOS 12.2(8)T and later. The Cisco 2600XMs with AIM-VPN/BPII require 12.2(15)ZJ Cisco IOS and later. The new AIM-VPN/BPII-PLUS, AIM-VPN/EPII-PLUS and AIM-VPN/HPII-PLUS require 12.3(5c)/12.3(6) Cisco IOS and later for mainline release and 12.3(7)T Cisco IOS and later for T-train releases. Cisco IOS IP firewall plus IPSec 3DES software contains all the IPSec, firewall and plus features of Cisco IOS software and supports both 3DES and DES (56-bit) encryption, while the IPSec 56 version software supports DES (56-bit) encryption.

A Cisco 1700, 2600, 3600, or 3700 Series router with a VPN module installed will run with any feature set for the Cisco IOS Software, but the module is utilized only with IPSec feature sets. For example, Cisco 1700, 2600 and 3600 Series Cisco IOS IP-only software for 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 Cisco 1700/ 2600/3600/3700 Series IPSec Software Part numbers

Product Name	Image Name	Software Image	Runs From
2600/3600/3660/3700			
S26/36AL	Enterprise Plus IPSec 56 (DES)	C2600/3620/3640/3660-jk8s-mz	RAM
S26/36AK2	Enterprise Plus IPSec 3DES	C2600/3620/3640/3660-jk9s-mz	RAM
S26/36AHL	Enterprise IP/FW/IDS Plus IPSec 56	C2600/3620/3640/3660-jk8o3s-mz	RAM
S26/36/37AHK2	Enterprise IP/FW/IDS Plus IPSec 3DES	C2600/3620/3640/3660-jk9o3s-mz	RAM
S26/36AR1L	ENTERPRISE/SNASW PLUS IPSEC 56	C2600/3620/3640/3660-a3jk8o3s-mz	RAM
S26/36AR1K2	ENTERPRISE/SNASW PLUS IPSEC 3DES	C2600/3620/3640/3660-a3jk9s-mz	RAM
S26/36/37CL	IP Plus IPSec 56 (DES)	C2600/3620/3640/3660/3700-ik8s-mz	RAM
S26/36/37CK2	IP PLUS IPSEC 3DES	C2600/3620/3640/3660/3700-ik9s-mz	RAM
S26/36CHL	IP/FW/IDS Plus IPSec 56 DES	C2600/3620/3640/3660-ik8o3s-mz	RAM

Table 3 Cisco 1700/ 2600/3600/3700 Series IPSec Software Part numbers (Continued)

Product Name	Image Name	Software Image	Runs From
S26/36/37CHK2	IP/FW/IDS Plus IPSec 3DES	C2600/3620/3640/3660 3700-ik9o3s-mz	RAM
S26/372/ 374AESK9	Advanced Enterprise Services	C2600/3700-adventerprisek9-mz	RAM
S26/372/ 274AISK9	Advanced IP Services	C2600/3700-advipservicesk9-mz	RAM
S26/372/374ASK9	Advanced Security	C2600/3700-advsecurityk9-mz	RAM
1700			
S17C7HK8	Cisco 1700 IOS IP/ADSL/FW/IDS PLUS IPSEC 56	C1700-k8o3sy7-mz	RAM
S17C7HK9	Cisco 1700 IOS IP/ADSL/FW/IDS PLUS IPSEC 3DES	C1700-k9o3sy7-mz	RAM
S17C7V8K8	Cisco 1700 IOS IP/ADSL/VOX/FW/IDS PLUS IPSEC 56	C1700-k8o3sv8y7-mz	RAM
S17C7V8K9	Cisco 1700 IOS IP/ADSL/VOX/FW/IDS PLUS IPSEC 3DES	C1700-k9o3sv8y7-mz	RAM
S17C7K8	Cisco 1700 IOS IP/ADSL PLUS IPSEC 56	C1700-k8sy7-mz	RAM
S17C7K9	Cisco 1700 IOS IP/ADSL PLUS IPSEC 3DES	C1700-k9sy7-mz	RAM
S17CV8K8	Cisco 1700 IOS IP/ADSL/VOX PLUS IPSEC 56	C1700-k8sv8y7-mz	RAM
S17CV8K9	Cisco 1700 IOS IP/ADSL/VOX PLUS IPSEC 3DES	C1700-k9sv8y7-mz	RAM
S17Q7HK8	Cisco 1700 IOS IP/ADSL/IPX/AT/IBM/FW/ IDS PLUS IPSEC 56	C1700-bk8no3r2sy7-mz	RAM
S17Q7HK9	Cisco 1700 IOS IP/ADSL/IPX/AT/IBM/FW/ IDS PLUS IPSEC 3DES	C1700-bk9no3r2sy7-mz	RAM
S17Q7V8K8	Cisco 1700 IOS IP/ADSL/IPX/AT/IBM/ VOX/FW/IDS PLUS IPSEC 56	C1700-bk8no3r2sv8y7-mz	RAM
S17Q7V8K9	Cisco 1700 IOS IP/ADSL/IPX/AT/IBM/ VOX/FW/IDS PLUS IPSEC 3DES	C1700-bk9no3r2sv8y7-mz	RAM
S17AESK9	Advanced Enterprise Services	C1700-adventerprisek9-mz	RAM
S17AISK9	Advanced IP Services	C1700-advipservicesk9-mz	RAM
S17ASK9	Advanced Security	C1700-advsecurityk9-mz	RAM

Export Regulations on the VPN Module

DES, 3DES and AES software for the 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, see: 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/BPII: DES/3DES/AES and Layer 3 (IPPCP) Compression VPN Encryption AIM—Base Performance
- AIM-VPN/EPII: DES/3DES/AES and Layer 3 (IPPCP) Compression VPN Encryption AIM—Enhanced Performance
- AIM-VPN/HPII: DES/3DES/AES and Layer 3 (IPPCP) Compression VPN Encryption AIM—High Performance
- AIM-VPN/BPII-PLUS: DES/3DES/AES and Layer 3 (IPPCP) Compression VPN Encryption AIM—Base Performance
- AIM-VPN/EPII-PLUS: DES/3DES/AES and Layer 3 (IPPCP) Compression VPN Encryption AIM—Enhanced Performance
- AIM-VPN/HPII-PLUS: DES/3DES/AES and Layer 3 (IPPCP) Compression VPN Encryption AIM—High Performance

Standards (Cisco IOS IPSec)

- IPSec (RFCs 2401-2410)
- IPSec Encapsulating Security Payload (ESP) Using DES/3DES (RFC 2406)
- IPSec Authentication Header (AH) using MD5 or SHA (RFCs 2403-2404)
- Internet Key Exchange (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 safety.

Dimensions and Weight

Module	MOD1700-VPN	AIM-VPN/ BP	AIM-VPN/ EP	NM-VPN/ MP	AIM-VPN/HP	AIM-VPN/ BPII AIM-VPN/ BPII-PLUS	AIM-VPN/ EPII AIM-VPN/ BPII-PLUS	AIM-VPN/ HPII AIM-VPN/ BPII-PLUS
Width	2.25 in. (5.72 cm)	5.25 in (13.3 cm)	5.25 in (13.cm)	7.10 in (18 cm)	5.25 in (13.3 cm)	5.25 in (13.3 cm)	5.25 in (13.3 cm)	5.25 in (13.3 cm)
Height	0.70 in (1.78 cm)	0.95 in (2.41 cm)	0.95 in (2.41 cm)	1.65 in (4.19 cm)	0.95 in (2.41 cm)	0.95 in (2.41 cm)	0.95 in (2.41 cm)	0.95 in (2.41 cm)
Depth	3.75 in (9.53)	3.25 in (8.26 cm)	3.25 in (8.26 cm)	7.20 in (18.3 cm)	3.25 in (8.26 cm)	3.25 in (8.26 cm)	3.25 in (8.26 cm)	3.25 in (8.26 cm)
Weight	0.078 lb (35.5 g)	0.60 lb (.27 kg)	0.60 lb (.27 kg)	1.1 lb 1.2 (.5 kg)	0.60 lb (.27 kg)	0.60 lb (.27 kg)	0.60 lb (.27 kg)	0.60 lb (.27 kg)

Regulatory Compliance, Safety, EMC, Telecom, Network Homologation

When installed in a Cisco 1700, 2600, 3600 and 3700 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 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.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 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 Website at www.cisco.com/go/offices

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

EC/LW6269 0504