Data Sheet

Cisco 1700, 2600, 3600, and 3700 Series VPN Security Router Bundles

Overview

The Cisco VPN security router bundles are based on the Cisco 1700, 2600XM, 2691, 3600, and 3700 modular multiservice router platforms. These virtual private network (VPN) bundles allow customers to use a single part number when ordering a Cisco router with all the necessary VPN and security components at a reduced price compared to ordering each component separately. Each VPN bundle can have optional modules added as needed. All bundles include the selected router platform, a VPN hardware card, additional memory, and the Cisco IOS® Software to run IP Security (IPSec) Triple Digital Encryption Standard (3DES) encryption, and Cisco IOS firewall with an intrusion detection system (IDS).

These bundles offer customers the ability to deploy proven security features such as secure VPNs, IDSs, and firewalls, as well as high-speed Internet access and the ability to create extranets or demilitarized zones (DMZs). These VPN bundles can also support intranet, extranet, and remote access VPN deployments.

For remote access, the VPN bundles include the Cisco VPN Client 3.0. Cisco VPN security router bundles are also ideal for site-to-site VPNs. They deliver a rich, integrated package of routing, firewall, dial, and packet voice gateway functionality, and VPN functions for multiservice VPN applications. The Cisco 1700, 2600, 3600, and 3700 series together with the VPN module are the perfect IPSec VPN solution for connecting small, medium, and large offices to other remote locations, corporate headquarters, central-office intranets, or partner extranets.

VPNs help companies reap benefits such as dramatically lowered WAN costs, improved global connectivity, and better reliability, while enabling capabilities such as secure extranet communications. Remote dial, Internet, intranet, and extranet access can all be consolidated over a single WAN connection to the Internet. See Table 2 for a complete list of Bundle Part numbers.

VPN Security Bundle Features and Benefits

Voice and Video-Enabled IPSec VPN

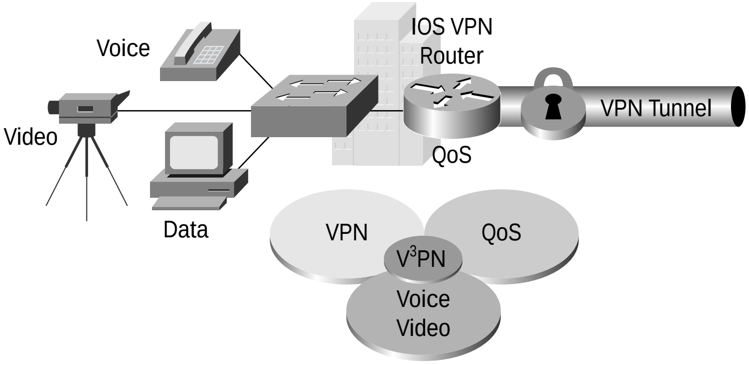
The Cisco VPN security router bundles are all voice and video-enabled IPSec VPN ready. Cisco offers a VPN infrastructure capable of transporting converged voice, video, and data traffic across a secure IPSec network. Unlike many VPN devices on the market, Cisco VPN platforms accommodate the diverse network topologies and traffic types characteristic of multiservice IPSec VPNs, and ensure that the VPN infrastructure does not break multiservice applications deployed now or in the future.

With the VPN security router bundles, Cisco provides products for all aspects of multiservice VPNs. The network architecture of the Cisco Voice and

Video-Enabled IPSec VPN (V^3PN) Solution takes advantage of Cisco VPN routers with Cisco IOS Software, Cisco CallManager, and IP phones. Furthermore, Cisco provides an overall deployment model for these products through Cisco AVVID (Architecture for Voice, Video and Integrated Data) for converged networking and the SAFE Blueprint for VPNs. These deployment models ensure a secure, interoperable, reliable network solution with end-to-end product support (refer to Figure 1).

Figure 1

Cisco Voice and Video-Enabled IPSec VPN

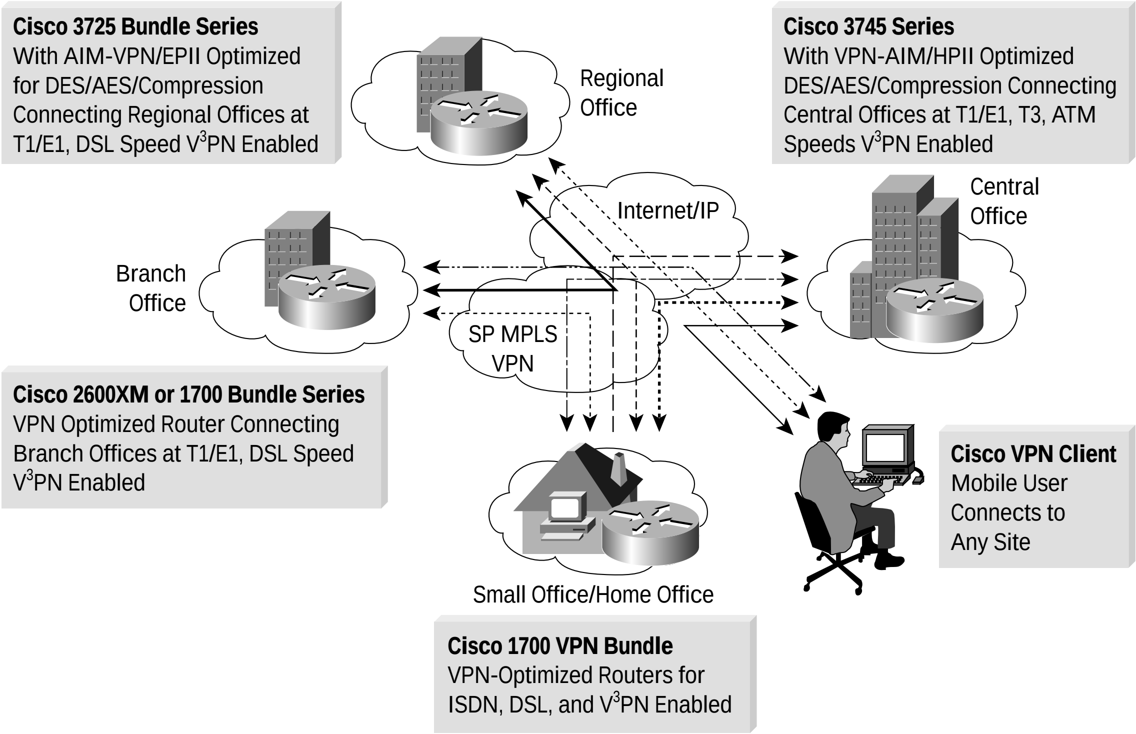


Dynamic Multipoint for IPSec

In Cisco IOS Version 12.2(13)T, Cisco will introduce Dynamic Multipoint for IPSec. Currently in a mesh network, *all* point-to-point IPSec (or IPSec + generic routing encapsulation [GRE] tunnels) must be configured on *all* the devices, even if some or most of these tunnels are not running or needed at all times. With Dynamic Multipoint VPN feature for Cisco routers, one router is designated the “hub,” and all the other routers (“spokes”) are configured with tunnels to the hub. The spoke-to-hub tunnels are up continuously. However, the spokes do not have, nor do they need, configuration for tunnels to any of the other spokes. Instead, when a spoke wants to transmit a packet to another spoke (that is, the subnet behind another spoke), it uses Next Hop Resolution Protocol (NHRP) to dynamically determine the required destination address of the target spoke. The hub router acts as the NHRP server and handles this request for the source spoke. The two spokes then dynamically create an IPSec tunnel between them (via the single mGRE interface) and data can be directly transferred. A timeout function automatically tears down the tunnel after a period of inactivity (refer to Figure 2).

Figure 2

Dynamic Multipoint VPN


Cisco 3725 Bundle Series
With AIM-VPN/EPII Optimized for DES/AES/Compression Connecting Regional Offices at T1/E1, DSL Speed V^{3}PN Enabled
Regional Office
Cisco 3745 Series
With VPN-AIM/HPII Optimized DES/AES/Compression Connecting Central Offices at T1/E1, T3, ATM Speeds V^{3}PN Enabled
Central Office
Internet/IP
Branch Office
SP MPLS VPN
Cisco 2600XM or 1700 Bundle Series
VPN Optimized Router Connecting Branch Offices at T1/E1, DSL Speed V^{3}PN Enabled
Cisco VPN Client
Mobile User Connects to Any Site
Small Office/Home Office
Cisco 1700 VPN Bundle
VPN-Optimized Routers for ISDN, DSL, and V^{3}PN Enabled

Cisco Easy VPN

Cisco Easy VPN is a software enhancement for Cisco routers and security appliances that greatly simplifies VPN deployment for remote offices and teleworkers. Cisco Easy VPN takes advantage of Cisco's Unified Client Framework and centralizes all key and policy management, reducing the complexity of VPN deployments.

Cisco Easy VPN has two components: Cisco Easy VPN Remote and Cisco Easy VPN Server. Cisco Easy VPN Remote enables Cisco routers and security appliances to automatically establish and maintain a VPN tunnel to a Cisco Easy VPN Server-enabled device without complex remote configuration. Cisco Easy VPN Server accepts incoming calls from Cisco Easy VPN Remote-enabled devices or VPN software clients and ensures that those connections have up-to-date policies in place before the connection is established.

Cisco Easy VPN provides a consistent connection and policy and key management method, allowing a choice of VPN remotes—Cisco routers, appliances, or software clients—within a single deployment to any Cisco Easy VPN Server-enabled device.

Advanced Encryption Standard

Cisco supports DES, 3DES, and Advanced Encryption Standard (AES) with IPSec in Cisco IOS Version 12.2(13)T with Cisco IOS IPSec. The feature adds support for the new encryption standard AES, with Cipher Block Chaining (CBC) mode.

AES has a variable key length—the algorithm can specify a 128-bit key (default), a 192-bit key, or a 256-bit key. All Cisco VPN bundles support AES in software and the Cisco 2691, 3725, and 3745 routers offer hardware-based AES acceleration.

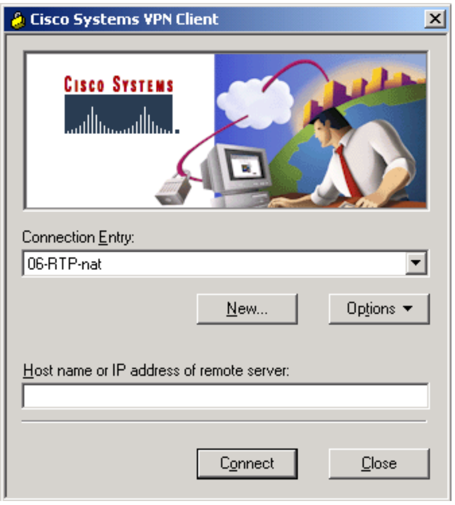
The National Institute of Standards and Technology (NIST) created AES as a new Federal Information Processing Standard (FIPS) publication. Refer to the NIST Web site for more details on AES:

http://csrc.nist.gov/encryption/aes/.

Cisco VPN Client (Supports Easy VPN Remote)

Simple to deploy and operate, the Cisco VPN Client enables customers to establish secure, end-to-end encrypted tunnels to any Cisco VPN server. This thin-design, IPSec implementation is available via Cisco.com, and a CD is included with every VPN router bundle. The client can be preconfigured for mass deployments, and initial logins require very little user intervention. VPN access policies and configurations are downloaded from the central gateway and pushed to the client when a connection is established, allowing simple deployment and management, as well as high scalability. The Cisco VPN Client provides support for Windows 95(OSR2+), 98, ME, NT 4.0, 2000, and XP; Linux (Intel); Solaris (UltraSPARC—32 and 64 bit); and MacOS X 10.1 and 10.2 (Jaguar). See Figure 3.

Figure 3
Cisco VPN Client



Cisco Systems VPN Client

Connection Entry: 06-RTP-nat

Host name or IP address of remote server:

VPN Modules for Cisco 1700, 2600XM, 3600, 3700 Series Routers

The VPN modules included with the Cisco VPN router bundles encrypt data using the DES and 3DES algorithms at speeds suitable for multiple full-duplex T1/E1 serial connections. The VPN encryption modules handle a variety of IPSec-related tasks, including encryption, hashing, key exchange, and storage of security associations—all of which free the main processor and memory to perform other router, voice, and firewall functions.

The Cisco 2691, 3725, and 3745 VPN bundles include VPN modules that now offer AES and hardware-assisted compression in addition to DES and 3DES.

Cisco IOS Firewall with Intrusion Detection

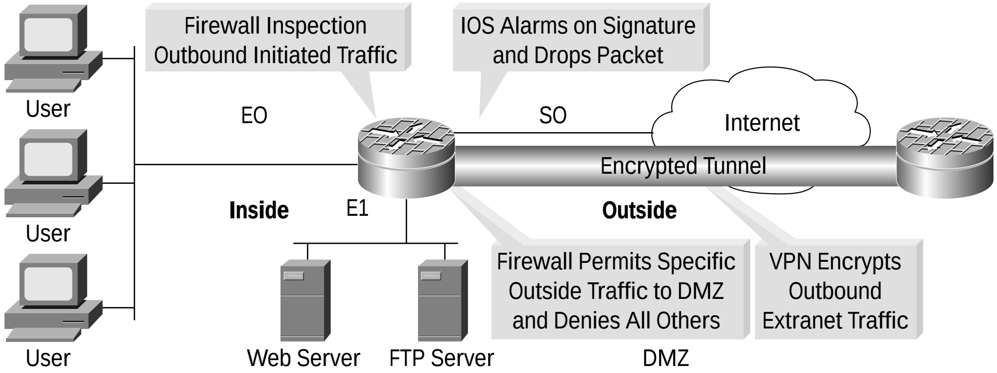
The Cisco IOS Firewall (with IDS included in the bundle) protects the LAN from network attacks (see Figure 4).

Context-Based Access Control (CBAC) provides dynamic or stateful filtering on a per-application basis, permitting legitimate traffic to enter the LAN only while a session is active. CBAC capability is considered essential for effective firewall functionality. The Cisco IOS Firewall also supports other key features such as Java blocking, denial-of-service detection and prevention, audit trail, and real-time alerts.

The Cisco IOS Firewall authentication, authorization, and accounting (AAA) features provide authentication of remote users, authorize access to specific network resources, and account for this activity. The Cisco IOS Firewall IDS identifies 59 of the most common attacks using signatures to detect patterns of misuse in network traffic.

The intrusion-detection signatures included in the new release of the Cisco IOS Firewall were chosen from a broad cross-section of intrusion-detection signatures. The signatures represent severe breaches of security and the most common network attacks and information-gathering scans.

Figure 4
Cisco IOS Firewall with Intrusion Detection


Firewall Inspection Outbound Initiated Traffic
IOS Alarms on Signature and Drops Packet
User
EO
SO
Internet
Encrypted Tunnel
User
Inside
E1
Outside
Firewall Permits Specific Outside Traffic to DMZ and Denies All Others
VPN Encrypts Outbound Extranet Traffic
User
Web Server
FTP Server
DMZ

Tunneling and Encryption

IPSec provides the following network security services:

- Privacy—IPSec can encrypt packets before transmitting them across a network.
- Integrity—IPSec authenticates packets at the destination peer to ensure that the data has not been altered during transmission.
- Authentication—IPSec peers authenticate the source of all IPSec-protected packets.
- Anti-replay protection—IPSec prevents capture and replay of packets, and helps protect against denial-of-service attacks.
- Encrypted tunnels—IPSec protects data from being intercepted and viewed by unauthorized entities and also performs multiprotocol encapsulation.

The Cisco IOS IPSec feature sets support both DES (56 bit) and 3DES (168 bit) encryption. In Cisco IOS Version 12.2(13)T, Cisco IOS IPSec feature sets will also support AES. The algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key. All Cisco VPN bundles support AES in software, and certain bundles support AES in hardware (Cisco 2691, 3725, and 3745).

GRE with IPSec is a unique solution from Cisco that enables routing updates to be sent over the VPN, thus delivering greater network resiliency than IPSec-only solutions. Aside from providing a failover mechanism, GRE tunnels provide the ability to encrypt multicast and broadcast packets and non-IP protocols. Thus by using GRE with IPSec, Cisco can support AppleTalk and Novell Internetwork Packet Exchange (IPX) with its site-to-site VPN solution.

Cisco Tunnel Endpoint Discovery, a feature in Cisco IOS software, facilitates tunnel scalability and survivability critical to fully meshed site-to-site VPN environments by enabling tunneled connections to dynamically self-configure according to network security policy, thus mitigating the need to manually configure every point-to-point tunnel on the VPN.

Dynamic Multipoint for IPSec, a feature in Cisco IOS Software that facilitates VPN spoke connections, allows any router to set up a dynamic connection to any other router using NHRP to dynamically determine connection.

Certifications

Cisco is committed to maintaining an active product certification and evaluation program for customers worldwide. Recognizing that certifications and evaluations are important to its customers, Cisco continues 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 will work to accelerate certification and evaluation processes. Certification and evaluation are considered at the earliest part of the company's product development cycle, and Cisco will continue to position its security products to ensure that customers have a variety of certified and evaluated products to meet their needs.

FIPS

The Cisco 1700, 2600, 3600, and 3700 series routers and Cisco VPN modules have been designed to meet the FIPS 140-1 level 2 security standard. Currently, only the Cisco 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 be submitting numerous 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 as well as 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 numerous existing country-specific security assessment processes, and was intended to establish a single standard for international use. Currently, 14 countries officially recognize the Common Criteria. Several versions of Cisco IOS IPSec 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

Management Tools for Enterprise-Based VPN Networks

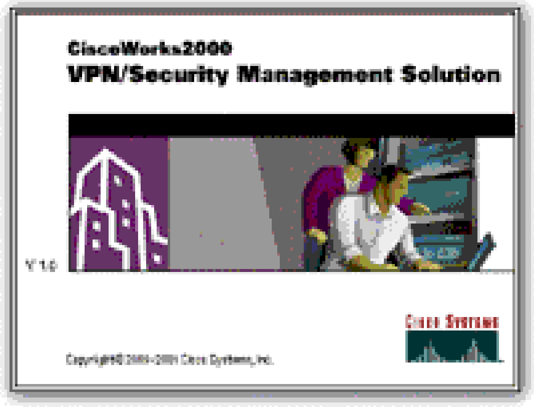
CiscoWorks VPN/Security Management Solution

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 IDSs. CiscoWorks VMS (Figure 5) 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 VPN routers, Cisco PIX® firewalls, IDS sensors, and a monitoring center for security.

Figure 5

CiscoWorks VPN/Security Management Solution



Features

- Management centers for VPN routing and 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 the CiscoWorks VMS, provides scalable security management for the configuration and deployment of VPN connections. The 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 for control over individual user and deployment permissions, enabling large enterprises to define multiple administrative and operational roles. In addition, the router management center provides an intuitive graphical user interface (GUI) interface for simplified policy definitions, a hierarchical inheritance model, flexible deployment options, and enhanced reporting capabilities.

CiscoWorks VPN Monitor

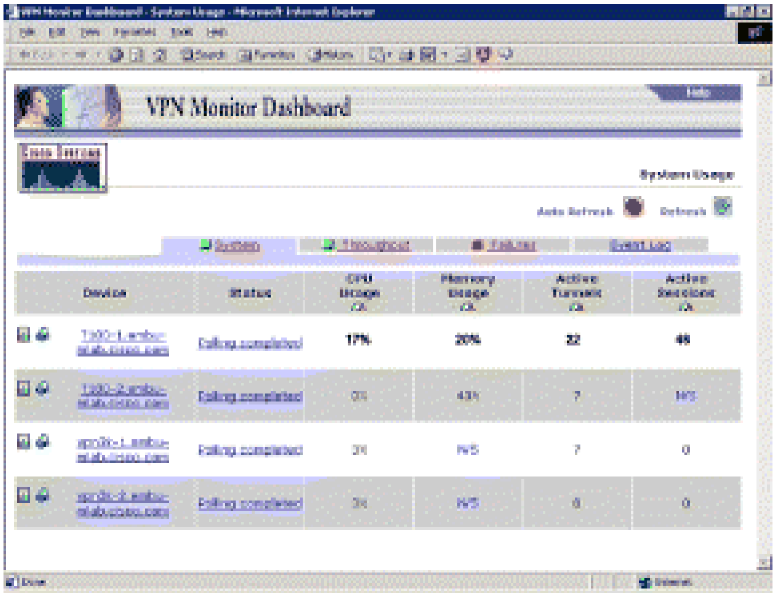
CiscoWorks VPN Monitor is a Web-based management tool that allows network administrators to collect, store, and view information on IPSec VPN connections for remote-access or site-to-site VPN terminations. Multiple devices can be viewed from an easy-to-use dashboard that is configured using a Web browser (Figure 6). CiscoWorks VPN Monitor uses the IPSec Management Information Base (MIB) supported by all Cisco router VPN modules.

When a VPN is deployed, network administrators must be able to monitor the health of the tunnels and VPN devices to ensure optimal VPN services. They need the following information:

- Number of operational tunnels
- Throughput of individual tunnels
- Status of security negotiations and sessions
- VPN device performance status
- Performance threshold violations

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

Figure 6
CiscoWorks VPN Monitor



VPN Monitor Dashboard

	Device	Status	CPU Usage	Memory Usage	Active Tunnels	Active Sessions
	7100-1.ambu-rlab.cisco.com	Polling completed	17%	20%	22	48
	7100-2.ambu-rlab.cisco.com	Polling completed	0%	43%	7	N/S
	vpn3k-1.ambu-rlab.cisco.com	Polling completed	3%	N/S	7	0
	vpn3k-2.ambu-rlab.cisco.com	Polling completed	3%	N/S	0	0

Cisco VPN Solution Center 2.2 (optional)

With Cisco VPN Solution Center (VPNSC) Release 2.2, a service provider can now manage both IPSec and Multiprotocol Label Switching (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 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. Cisco VPNSC offers:

- The ability to provision IPSec IP VPNs by configuring an IKE and IPSec tunnel between the Cisco devices—all Cisco IOS devices
- Comprehensive hub-and-spoke, full-mesh, and partial-mesh VPN topology views
- The ability to 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 application programming interfaces (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

Cisco VPNSC 2.2 supports the Cisco 1700 and 2600 series routers as both MPLS customer premises equipment (CPE) and as IPSec devices, allowing the provider to manage both IPSec and MPLS-based IP VPNs. The Cisco 2691 model is currently being tested to provide provider edge support at a future Cisco IOS release date, but is not currently supported.

Cisco VPNSC 2.2 also supports the Cisco 3600 and 3700 series routers as both MPLS CPE and IPSec devices. In addition, the Cisco 3640, 3660, and 3700 can be supported as provider edge devices with Cisco VPNSC 2.2.

Technical Details and Performance

The performance test was performed via full-duplex Fast Ethernet and Ethernet to a Spirent Communications SmartBits SMB2000, which functions as a full-duplex traffic generator and counter. Internet Control Message Protocol (ICMP) packets are generated from SmartBits via Ethernet into a device under test. The SmartBits test tool by default supports a mixed-packet definition called the IMIX pattern. IMIX traffic is defined as the following streams set up in the Smart Windows application:

- Seven data streams of 64-byte packets
- Four data streams of 570-byte packets
- One data stream of 1518-byte packet

See Table 1 for details, Table 2 for ordering information, and Table 3 for a summary of chassis features.

Table 1 Cisco VPN Bundles

Bundle	Firewall with IDS	GRE and IPSec	*IP Payload Compression Protocol (IPPCP)	**High Availability or Failover	*** MPLS VPN	VPN QoS	AES in Hardware	Max. Tunnel	IMIX 3DES packet	3DES Mbps Packet 1400
Cisco 1700 bundles	Yes	Yes	Software	Yes	CPE	Yes	No	100	3.5	8
Cisco 2600XM bundles	Yes	Yes	Software	Yes	CPE	Yes	No	800	4	14
Cisco 2691 VPN	Yes	Yes	Hardware	Yes	CPE	Yes	Yes	800	25	80
Cisco 3640A VPN	Yes	Yes	Software	Yes	PE	Yes	No	1000	5	18
Cisco 3662 VPN	Yes	Yes	Software	Yes	PE	Yes	Yes	1800	9	40
Cisco 3725 VPN	Yes	Yes	Hardware	Yes	PE	Yes	No	2000	47	150
Cisco 3745 VPN	Yes	Yes	Hardware	Yes	PE	Yes	Yes	2000	75	180

Note: Mbps 3DES speeds are based on a back-to-back Fast Ethernet router tests; your numbers may vary based on WAN speed, memory, and other applications that may be running in Cisco IOS Software.

* Software-based Layer 3 IPPCP is now enabled to use with current VPN modules. This allows IPPCP to run on the router CPU (requires Cisco IOS Version 12.2(13) T or later).

** High availability or failover: Cisco IOS support for Reverse Route Injection (RRI) and Hot Standby Router Protocol (HSRP) with IPSec.

*** MPLS: All VPN security router bundles support MPLS extensions for customer edge routers. A multi-VPN routing and forwarding (VRF) customer edge extends limited provider edge functionality to a customer edge router in an MPLS-VPN model. Customer edge routers now have the ability to maintain separate VRF tables.

Table 2 gives ordering information for the Cisco VPN router bundles.

Table 2 VPN Router Bundle Ordering Information

Cisco Part Number	Description	Optional WAN Interface Cards (WICs) Available	Optional Network Modules Available	Optional Dial-Backup ISDN or Analog
CISCO1721-VPN/K9	Cisco 1721 VPN Bundle with VPN module, 64-MB DRAM, IP Plus/FW/3DES	Yes	No	Yes
CISCO1721-VPN/K9-A	Cisco 1721 VPN Bundle with asymmetric DSL (ADSL) WIC, VPN module, 64-MB DRAM, IP+/FW/3DES	Yes	No	Yes
CISCO1751-VPN/K9	Cisco 1751 VPN Bundle with VPN module, 64-MB DRAM, IP Plus/FW/3DES	Yes	No	Yes
CISCO1751-VPN/K9-A	Cisco 1751 VPN Bundle with ADSL WIC, VPN module, 64-MB DRAM, IP+/FW/3DES	Yes	No	Yes
CISCO1760-VPN/K9	Cisco 1760 VPN Bundle with VPN module, 64-MB DRAM, IP Plus/FW/3DES	Yes	No	Yes
CISCO1760-VPN/K9-A	Cisco 1760 VPN Bundle with ADSL WIC, VPN module, 64-MB DRAM, IP+/FW/3DES	Yes	No	Yes
CISCO1760-V3PN/K9	Cisco 1760 V^{3}PN Bundle with ADSL WIC, VPN module, 32-MB Flash, 96-MB DRAM, 4-channel digital signal processor (DSP), IP Plus/ ADSL/VOX/FW/IDS/3DES	Yes	No	Yes
C2611XM-2FE/VPN/K9	Cisco 2611XM VPN Bundle, AIM-VPN/EP/2FE/IOS FW/ IPSec 3DES, 96-MB DRAM	Yes	Yes	Yes
C2621XM-2FE/VPN/K9	Cisco 2621XM VPN Bundle, AIM-VPN/EP/2FE/IOS FW/ IPSec 3DES, 96-MB DRAM	Yes	Yes	Yes
C2651XM-2FE/VPN/K9	Cisco 2651XM VPN Bundle, AIM-VPN/EP/2FE/IOS FW/ IPSec 3DES, 96-MB DRAM	Yes	Yes	Yes
C2691-VPN/K9	Cisco 2691 VPN Bundle, AIM-VPN/EPII, Plus FW/IPSec 3DES, 128-MB DRAM	Yes	Yes	Yes
C3640A-2FE/VPN/K9	Cisco 3640 VPN Bundle, NM-VPN/MP, 2xFE, Cisco IOS FW/IPSec 3DES, 2WAN, 64DRAM	Yes	Yes	Yes

Table 2 VPN Router Bundle Ordering Information

Cisco Part Number	Description	Optional WAN Interface Cards (WICs) Available	Optional Network Modules Available	Optional Dial-Backup ISDN or Analog
C3662-2FE/VPN/K9	Cisco 3662 VPN Bundle, AIM-VPN/HP, 2xFE, Cisco IOS FW/IPSEC 3DES, 96-MB DRAM	Yes	Yes	Yes
C3725-VPN/K9	Cisco 3725 VPN Bundle, AIM-VPN/EPII, Plus Cisco IOS FW/IPSec 3DES, 128-MB DRAM	Yes	Yes	Yes
C3745-VPN/K9	Cisco 3745 VPN Bundle, AIM-VPN/HPII, Plus Cisco IOS FW/IPSec 3DES, 128-MB DRAM	Yes	Yes	Yes

Note: In all cases, bundles will ship with most current Cisco IOS IPSec image set available for that platform.

Summary

Built on Cisco IOS Software, Cisco VPN routers take advantage of best-in-market wide-area networking services to set the standard in site-to-site VPN solutions.

- *Support for diverse networking environments*—IPSec is a unicast, IP-only protocol. Cisco VPN routers, utilizing Cisco IOS Software features, accommodate multicast and multiprotocol traffic, as well as routing across the VPN, thus delivering flexible solutions for the most diverse VPN environments.
- *Timely, reliable delivery of latency-sensitive traffic*—Bandwidth management features of Cisco VPN routers enable traffic to be prioritized up to the application layer, thereby facilitating differentiated quality-of-service (QoS) policies by true application type, not just TCP port number.
- *V^3PN*—V^3PN provides a VPN infrastructure capable of converged voice, video, and data across a secure IPSec network.
- *Site-specific VPN scalability*—Cisco provides the broadest range of VPN devices ranging from dedicated headend VPN routers to single-box remote office VPN router solutions complete with WAN interfaces and stateful firewall.

Cisco 1700, 2600, 3600, and 3700 series secure VPN bundles allow both enterprise and service providers to easily deploy Cisco routers as VPNs, thus taking advantage of new and powerful services. These bundles are a great complement to the Cisco 7100 and 7200 VPN bundles also available from Cisco, and they extend the range, functionality, and price points available to the VPN buyer.

Table 3 Chassis Features Summary

VPN Router Bundle	Fast Ethernet Ports	Combination Slot WIC or Voice WIC (VWIC)	Combination Slot Voice Interface Card (VIC) or WIC or VWIC Slots	VIC-Only Slots	Network Module Slots	Cisco IOS Software	Flash Memory (MB)*	DRAM Memory (MB)*	VPN Card	Other Modules
c1721-VPN/K9	1	2	–	–	–	IP Plus/FW/IDS/3DES	16	64	MOD1700-VPN	Optional
c1721-VPN/K9-A	1	2	–	–	–	IP Plus/FW/IDS/3DES	16	64	MOD1700-VPN	WIC-1 ADSL included
c1751-VPN/K9	1	–	2	1	–	IP Plus/FW/IDS/3DES	16	64	MOD1700-VPN	Optional
c1751-VPN/K9-A	1	–	2	1	–	IP Plus/FW/IDS/3DES	16	64	MOD1700-VPN	WIC-1 ADSL included
c1760-VPN/K9	1	–	2	2	–	IP Plus/FW/IDS/3DES	16	64	MOD1700-VPN	Optional
c1760-VPN/K9-A	1	–	2	2	–	IP Plus/FW/IDS/3DES	16	64	MOD1700-VPN	WIC-1 ADSL included
C1760-V3PN/K9	1	–	2	2	–	IP Plus/ADSL/VOX/FW/IDS/3DES	32	96	MOD1700-VPN	4-channel DSP included
c2611XM-VPN/K9 **c2621XM-VPN/K9** **c2651XM-VPN/K9**	2	2	–	–	1	IP Plus/FW/IDS/3DES	32	96	AIM-VPN/EP	Optional
c2691-VPN/K9	2	3	–	–	1	IP Plus/FW/IDS/3DES	32	128	AIM-VPN/EPII**	Optional
3640A-VPN/K9	2	2	–	–	4	IP Plus/FW/IDS/3DES	16	64	AIM-VPN/MP	Optional
3662-VPN/K9	2	2	–	–	6	IP Plus/FW/IDS/3DES	32	96	AIM-VPN/HP	Optional
3725-VPN/K9	2	3	–	–	2	IP Plus/FW/IDS/3DES	32	128	AIM-VPN/EPII**	Optional
3745-VPN/K9	2	3	–	–	4	IP Plus/FW/IDS/3DES	32	128	AIM-VPN/HPII**	Optional

* All Cisco 1700, 2600, and 3600 bundles include upgraded Flash and DRAM memory.

** Cisco 2691, 3725, and 3745 VPN modules support DES, 3DES, AES, and compression.

CISCO SYSTEMS

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