

# Cisco VPN Security Routers

## Setting the Standard in Site-to-Site VPN Solutions

Site-to-site virtual private networks (VPNs) are an alternative WAN infrastructure that replace or augment existing private networks using leased lines, Frame Relay, or ATM to connect remote and branch offices and central sites more cost-effectively and with increased flexibility. Interconnecting multiple sites requires a network manager to accommodate diverse traffic types and network topologies, ensure reachability and reliability of all devices in the network, provide a framework for managing numerous geographically dispersed devices and, of course, scale the network at the VPN aggregation hub site. Many of today's VPN devices lack the depth of networking features to accommodate these specific site-to-site VPN requirements.

Built on Cisco IOS<sup>®</sup> Software, Cisco VPN security routers take advantage of best-in-market wide-area networking services to set the standard in site-to-site VPN solutions. Important site-to-site VPN features of Cisco VPN security routers include:

- *Support for diverse networking environments*—IP security (IPSec) is a unicast, IP-only protocol. Cisco VPN security routers, using Cisco IOS Software features, accommodate multicast and multiprotocol traffic, as well as routing across the VPN, delivering flexible solutions for the most diverse VPN environments. Cisco

VPN security routers also support manageable and scalable meshed VPN topologies. The Cisco Dynamic Multipoint VPN (DMVPN) feature makes deployment of meshed VPNs easier by automating provisioning of connections between spoke sites. Furthermore, DMVPN dynamically sets up connections based on network traffic patterns, increasing scalability of meshed deployments.

- *Timely, reliable delivery of latency-sensitive traffic*—Bandwidth management features of Cisco VPN security routers enable traffic to be prioritized up to the application layer, facilitating differentiated quality-of-service (QoS) policies by true application type, not just TCP port number. The result is increased transmission reliability and better response time of business-critical applications running across the VPNs.

**Figure 1**  
Cisco IOS VPN Routers





- *Voice and Video-Enabled IPsec VPN (V3PN) Solution*—The Cisco V3PN solution combines advanced QoS, telephony, networking, and VPN features of Cisco IOS Software with purpose-built hardware platforms to deliver a VPN infrastructure capable of transporting converged data, voice, and video traffic across a secure IPsec network. Unlike many VPN devices on the market, Cisco VPN devices accommodate the diverse network topology and traffic requirements of multiservice IPsec VPNs, thereby ensuring the VPN infrastructure does not break productivity-enhancing multiservice applications deployed now or in the future.
- *Site-specific VPN scalability*—Cisco provides the broadest range of VPN devices, ranging from dedicated head-end VPN routers to single-unit, remote-office VPN router solutions, complete with WAN interfaces and stateful firewall. Cost-effective overlay broadband VPN devices for use behind carrier-provided DSL and cable devices are also an integral part of the Cisco VPN security router portfolio.
- *Comprehensive VPN features*—Cisco VPN security routers support all features essential to VPNs—IPsec data encryption, tunneling, broad certificate authority support for public key infrastructure (PKI)—and advanced features such as stateful VPN failover, certificate auto-enrollment, stateful firewall, intrusion detection, and service-level validation.
- *All-encompassing site-to-site VPN management framework*—Managing multiple VPN devices over multiple sites requires not only robust VPN configuration management and monitoring capabilities, but also device inventory and software version management features. Cisco delivers comprehensive enterprise-class VPN configuration and monitoring via CiscoWorks VPN/Security Management Solution (VMS). CiscoWorks VMS is an integral part of the Cisco SAFE Blueprint for network security. It combines Web-based tools for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network- and host-based intrusion detection systems (IDSs). For large enterprise and service provider deployments, Cisco VPN Solutions Center provides comprehensive VPN provisioning and management as well as integrated QoS and MPLS management.



**Table 1** Cisco VPN Security Router Portfolio

Site	Model	VPN Performance	Tunnels	Embedded Interfaces	Modular Interface Options
<b>Integrated Broadband SOHO</b>	Cisco 830	6 Mbps	<50	10BaseT + DSL -or- 10BaseT + ISDN	-none-
	Cisco 900	6 Mbps	<50	10BaseT + Cable	
<b>Overlay Broadband SOHO</b>	Cisco 830	6 Mbps	<50	Dual 10BaseT	-none-
	Cisco 1700	8 Mbps	100	Dual 10BaseT	
<b>Remote Office</b>	Cisco 1700	8 Mbps	100	10BaseT	Serial, DSL, ISDN, Ethernet, Voice
	Cisco 2600XM	14 Mbps	800	Single -or- Dual 10/100BaseT	Serial, DSL, ATM, ISDN, E/FE, Voice
<b>Branch Office</b>	Cisco 2691	80 Mbps	1000	Single -or- Dual 10/100BaseT	Serial, DSL, ATM, ISDN, E/FE, Voice
	Cisco 7400	120 Mbps	5000	Dual 10/100/1000BaseT	-none-
	Cisco 3725	150 Mbps	2000	None, Single, -or- Dual 10/100BaseT	Serial, DSL, ATM, ISDN, E/FE, Voice
<b>Central Hub Site</b>	Cisco 7400	120 Mbps	5000	Dual 10/100/1000BaseT	-none-
	Cisco 3745	180 Mbps	2000	None, Single, -or- Dual 10/100BaseT	Serial, DSL, ATM, ISDN, E/FE, Voice
	Cisco 7200	225 Mbps	5000	Dual 10/100/1000BaseT	Serial, POS, ATM, ISDN, E/FE/GE, Voice

"VPN Performance" is determined using IPSec Triple Data Encryption Standard (3DES) HMAC-SHA1 on 1400-byte packets

## Site-to-Site VPN Benefits and Applications

### Reduce WAN Costs, Increase WAN Flexibility

Using Internet transport, VPNs cut recurring WAN costs by 50 percent or more compared with traditional WAN technologies such as Frame Relay. And unlike Frame Relay, VPNs can be easily and quickly extended to new locations and extranet business partners.

### Deliver New, Revenue-Enhancing Applications via VPNs

VPNs enable secure use of cost-effective, high-speed links such as DSL to deliver revenue-generating applications such as in-store online catalogs and ordering and efficiency tools such as online training.

### Increase Data and Network Security

Traditional WANs using Frame Relay, leased lines, or ATM provide traffic segregation, not transport security. VPNs encrypt and authenticate traffic traversing the WAN to deliver true network security in an insecure, networked world.



## **Features**

### **VPN Tunneling**

- IPSec (RFC 2401-2411, 2451)
- GRE (RFC 1701-1702)
- L2TP (RFC 2661)
- PPTP (RFC 2637)

### **Encryption**

- ESP DES, 3DES, and AES (RFC 2406, 2451)
- MPPE RC4 (40/128 bit)

### **Authentication**

- X.509 digital certificates (RSA signatures)
- Shared secrets
- Simple Certificate Enrollment Protocol
- RADIUS (RFC 2138)
- TACACS+
- CHAP/PAP (RFC 1994)

### **Integrity**

- HMAC-MD5 & HMAC-SHA-1 (RFC 2403-2404)

### **Key Management**

- Internet Key Exchange (RFC 2407-2409)
- IKE-XAUTH
- IKE-CFG-MODEIP Compression
- IPPCP-LZS (RFC 2401-2402)

### **Certificate Authority Support**

- Entrust
- Verisign
- Microsoft
- iPlanet
- Baltimore Technologies



### **Bandwidth Management/QoS**

- Network-Based Application Recognition (NBAR) content-aware classification
- Class/Flow-based Weighted Fair Queuing (WFQ)
- Generic Traffic Shaping (GTS)
- Rate Limiting (Committed Access Rate [CAR])
- Congestion Avoidance (Weighted Random Early Detection [WRED])

### **Resiliency**

- Hot Standby Router Protocol (HSRP)
- IKE Keep-Alives
- Routing across IPSec
- Dynamic Multipoint for IPSec

### **Management Options**

- CiscoWorks VPN/Security Management Solution (VMS)
  - The CiscoWorks Router Management Center, a component of Cisco VMS, provides scalable security management for the configuration and deployment of VPN connections.
- Cisco VPN Solution Center for Service Provider Networks
- Secure command-line interface using secure shell (SSH) or kerberized telnet

### **Routing Protocols**

- BGP4
- RIP/RIP2
- OSPF
- EIGRP/IGRP
- NHRP
- IS-IS

### **Security**

- Context Based Access Control (CBAC) stateful firewall
- Java blocking
- Active audit intrusion detection
- Denial-of-service detection and prevention

### **Security Certifications**

- FIPS-140-1, level 2
- ICSA IPsec
- Common Criteria IPsec
- For more information, visit  
<http://www.cisco.com/warp/public/779/largeent/issues/security/secvpncert.html>

## CISCO SYSTEMS



### Corporate Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://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](http://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](http://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](http://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](http://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

All contents are Copyright © 1992-2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, Cisco IOS, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.  
(0208R) LW3851 11/02