Cisco Group Encrypted Transport VPN: Tunnel-less VPN Delivering Encryption and Authentication for the WAN

Product Overview

Today's networked applications such as voice and video are accelerating the need for instantaneous, branch-interconnected, and quality of service (QoS)-enabled WANs. And the distributed nature of these applications results in increased demands for scale. At the same time, enterprise WAN technologies force businesses to make a tradeoff between QoS-enabled branch interconnectivity and transport security. As network security risks increase and regulatory compliance becomes essential, Cisco® Group Encrypted Transport VPN, a next-generation WAN encryption technology, eliminates the need to compromise between network intelligence and data privacy.

With the introduction of Group Encrypted Transport, Cisco now delivers a new category of Virtual Private Network (VPN) that eliminates the need for tunnels. By removing the need for point to point tunnels, distributed branch networks are able to scale higher while maintaining network-intelligence features critical to voice and video quality, such as QoS, routing, and multicast. Group Encrypted Transport offers a new standards-based IP Security (IPsec) security model that is based on the concept of "trusted" group members. Trusted member routers use a common security methodology that is independent of any point-to-point IPsec tunnel relationship.

Group Encrypted Transport-based networks can be used in a variety of WAN environments, including IP and Multiprotocol Label Switching (MPLS). MPLS VPNs that use this encryption technology are highly scalable, manageable, and cost-effective, and meet regulatory-mandated encryption requirements. The flexible nature of Group Encrypted Transport allows security-conscious enterprises to manage their own network security over a service provider WAN service or to offload encryption services to their providers. Group Encrypted Transport simplifies securing large Layer 2 or MPLS networks requiring partial or full-mesh connectivity.

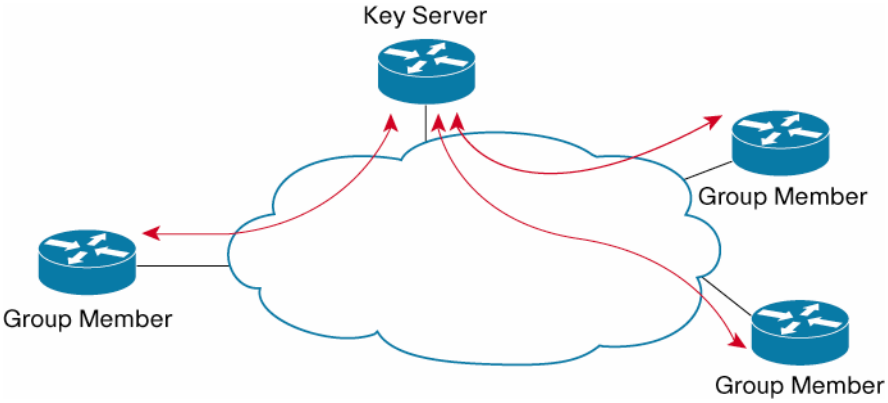
Product Architecture

Group Encrypted Transport is built on standards-based technologies and easily integrates routing and security together in the network fabric. Secure group members are managed through an IETF standard, Group Domain of Interpretation (GDOI).

Simplifying the Security Policy Distribution

GDOI alleviates the need to configure tunnel endpoints. A key server distributes keys and policies to all registered and authenticated member routers (Figure 1).

Figure 1. Key and Policy Distribution with GDOI

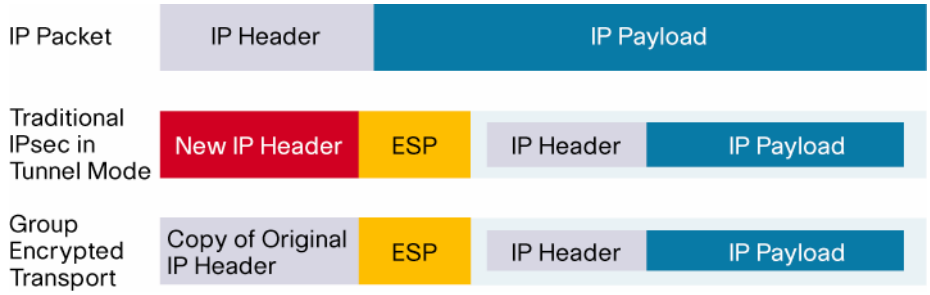


By distributing policies from a centralized point and by sharing the same group security association with authenticated group members, key distribution and management are greatly simplified.

IP Routing Preservation

A Group Encrypted Transport-enabled security model uses the existing routing infrastructure rather than using the traditional IPsec overlay. Data packets maintain their original IP source and destination addresses (Figure 2). By preserving the original IP header in IPsec packets, Group Encrypted Transport enables organizations to rely on the existing Layer 3 routing information, thus providing the ability to address multicast replication inefficiencies and improving network performance.

Figure 2. IP Routing Comparison Between IPsec and Group Encrypted Transport



Additionally, Group Encrypted Transport helps ensure low latency and jitter for voice, video, and other latency-sensitive traffic by enabling direct, always-on communication between all sites without traversing a central hub site. Furthermore, it reduces traffic loads for multicast traffic across IP Layer 3 VPNs by eliminating the broadcast traffic replication usually required on IPsec-encrypted networks.

Applications

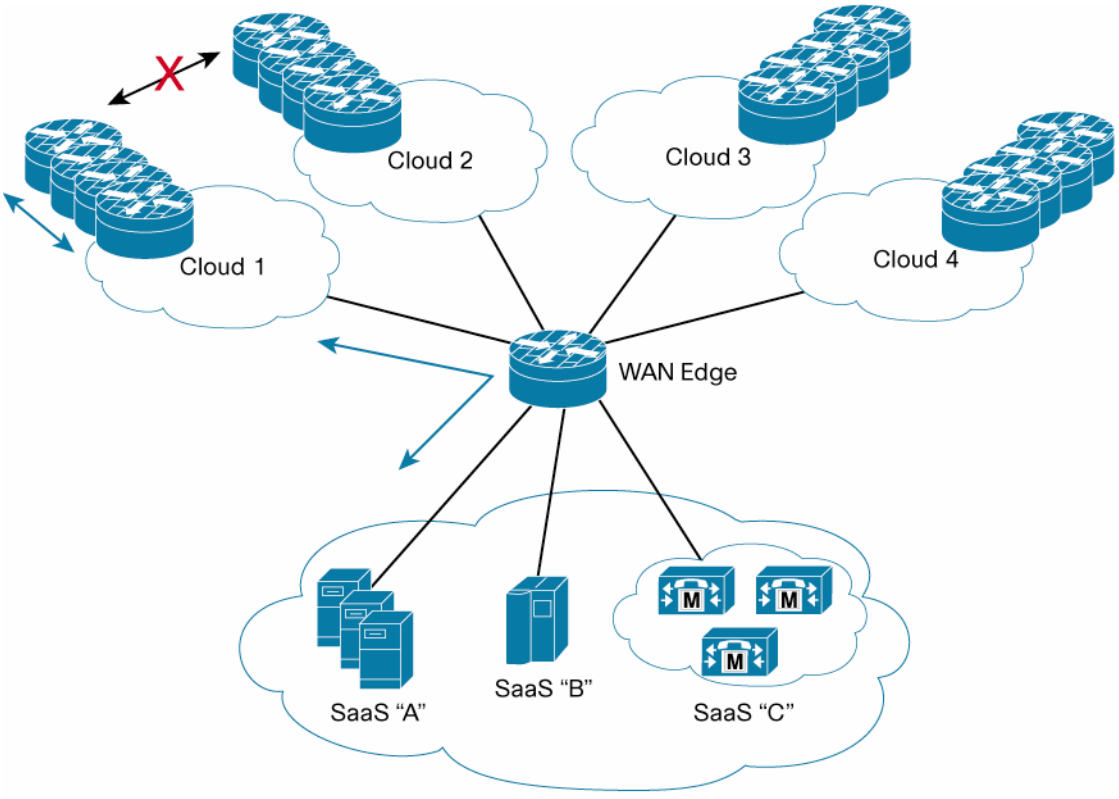
Private WAN (IP/MPLS) Encryption

Increased network security risks and regulatory compliances have driven the need for WAN transport security. Enterprise organizations that are either self-managing their own MPLS network or have purchased MPLS or private WAN services from a service provider can self-employ Group Encrypted Transport to help ensure data privacy while maintaining the any-to-any connectivity intrinsic in many private WANs. In doing so, organizations attain a much needed balance of control over security between their businesses and service providers while maintaining compliance with security regulations.

Private Secure Cloud Computing

The move towards data center virtualization and cloud computing is creating unique requirements for securing the data in transit.

Figure 3. Secure Cloud Computing—Example of Requirements



For example, in the diagram above:

- Each cloud represents a user community that must be given selective access to virtualized Software-as-a-Service entities in the data center: Cloud 1 users can access SaaS "A" only; Cloud 2 users require access to SaaS "A" and "C", etc.
- All members within a cloud are permitted to communicate to each other.
- Each cloud may represent a different organization and so inter-cloud communications may need to be denied. For example, each cloud could be an Enterprise department or a Government agency accessing a shared data center; or Enterprise customers—such as bank consortia or healthcare providers—accessing applications hosted in a Service Provider's data center.

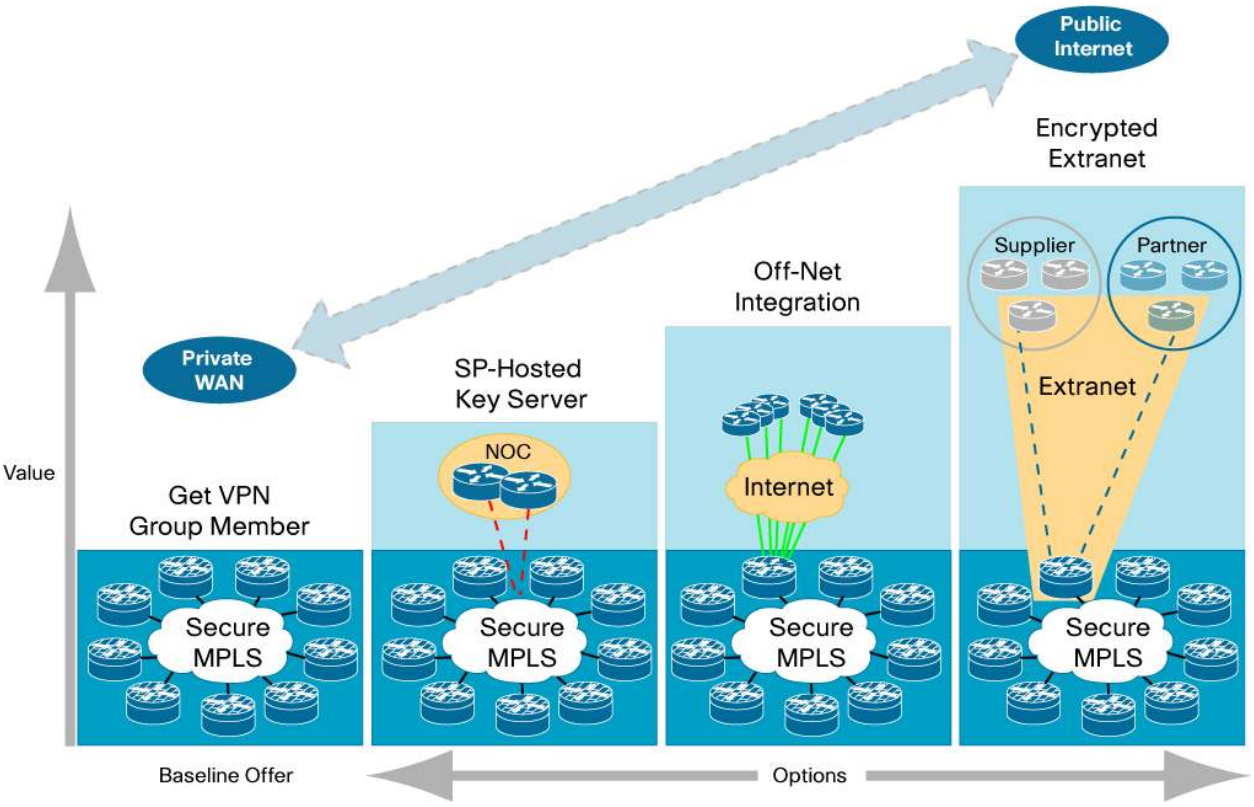
GET VPN can be deployed to implement such applications. Inter-cloud communications can be denied or permitted as required.

Managed Secure MPLS

GET VPN has been designed to add encryption seamlessly into MPLS networks. Service Providers are utilizing this to offer value-added encrypted MPLS services that strengths the security of MPLS networks while maintaining network intelligence that is critical to voice and video quality—including quality of service (QoS), natural routing path, and multicast. The primary driver for these services has been regulatory compliance.

A choice of deployment models allows the Key Servers and security policy distribution to remain under Enterprise control or be managed by the Service Provider as well.

Figure 4. Managed Secure MPLS Services Offers



Public Internet Environments

For enterprise IPsec VPNs that traverse the public Internet (including the off-net integration and encrypted extranet options above), tunneling technologies such as Dynamic Multipoint VPN (DMVPN) or GRE-based IPsec VPN are required. Group Encrypted Transport can be used to enhance these technologies through group shared keys, which simplifies key management in large network deployments.

For a comparison of Cisco IPsec site-to-site solutions available for either tunnel-less or tunnel-based environments, view the Cisco Site-to-Site At a Glance document.

Features and Benefits

Table 1 summarizes the key Group Encrypted Transport VPN features and benefits.

Table 1. Cisco GET VPN Features and Benefits

Feature	Description and Benefit
Group Keys	Standards-based (RFC 3547) GDOI key management protocol establishes security associations among authorized group member routers. Group Members share a single Group Key versus separate encryption keys with every peer. This has multiple benefits: • Scalable Tunnel-less Full Mesh: Each remote site can communicate with every other site without requiring to configure inordinate numbers of point-to-point tunnels. • Group Member Size and Cost: The same security association serves to connect with all members of a group. This allows even the smallest VPN routers to participate in the full mesh.
IP Header Preservation	By virtue of preserving the original IP headers while transporting the encrypted packet, GET VPN delivers several benefits including: • Optimal Routing and Redundancy: Maintains the natural routing path instead of traditional IPsec tunneling. If a path to a destination LAN fails (e.g. VPN gateway fails), packets can be routed through alternate VPN gateway without loss of connectivity or black holing. • QoS: All QoS features within the IP header are preserved end-to-end. • IP Multicast: Where the WAN core supports IP Multicast, GET VPN optimizes the replication and encryption process such that encryption occurs once per packet rather than multiple times for every destination as is common in traditional IPsec tunneling.
Key Services	Key Servers are responsible for ensuring that keys are granted to authenticated and authorized devices only. They maintain the freshness of the key material, pushing re-key messages as well as security policies on a regular basis. The chief characteristics include: • Key Servers can be located centrally, granting easy control over membership. • Key Servers are not in the "line of fire" – encrypted application traffic flows directly between VPN end points without a bottleneck or an additional point of failure. • Supports both local and global policies, applicable to all members in a group – such as "Permit any any", a policy to encrypt all traffic. • Supports IP Multicast to distribute and manage keys, for improved efficiency; Unicast is also supported where IP Multicast is not possible.
Reliability	• GM-Initiated Registration: GMs initiate the process by attempting to register; if a Key Server is unreachable, the GM can try multiple alternate Key Servers sequentially. • Periodic Rekeys: The Key Server sends out rekey messages containing replacement keys before the current keys expire. • Key Server High Availability: Set of cooperative Key Servers synchronize keys and the policy database, allowing seamless failover. Key Servers can be located in different geographies for optimal disaster recovery designs • Re-registration: Group Members detect missed rekey in time, and attempt to re-register with Key Servers in a pre-determined order or priority. • Script-based Fail Open: For deployments where connectivity SLAs are paramount, EEM scripts detect lost Key Server connectivity and provide roll back to clear text.
Scalability and Throughput	• The solution scales to thousands of sites fully meshed in a single group. • Tiered designs allow for further expansion to tens of thousands of sites. For example the first tier could represent regions fully meshed to one or more data centers; the data centers serviced by a pool of high performance Group Members and shared Key Servers. • Up to 7 Gbps throughput is available in a single device. • Additional performance can be obtained by load balancing a number of VPN routers behind the edge router. For example, placing 11 ASR 1000 Series Routers behind the load balancer scales up to 70 Gbps throughput – while allowing for N+1 redundancy. • The full mesh nature of the solution allows devices to communicate directly with each other, without requiring transport through a central hub; this minimizes extra encrypts and decrypts at the hub router; it also helps minimize latency and jitter. • Efficient handling of IP Multicast traffic by using the core network for replication can boost effective throughput further.
Security	Provides data security and transport authentication, helping to meet security compliance and internal regulation by encrypting all WAN traffic • Packet Confidentiality: Supports Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), and DES; AES is recommended. • Packet Integrity: Supports HMAC-SHA and SHA-MD5. • Replay Protection: Cisco Time-Based Anti-Replay (TBAR) protects against man-in-the-middle attacks. • Control Plane Security: GDOI Registration and Rekey protected by RFC 3547 mechanisms including digital certificates and signatures, access lists, AES/3DES, cookies, message ID, nonces, hashes, etc. • Fail Close: For deployments that do not tolerate the flow of any non-encrypted packets, Fail Close ensures that traffic will cease in the event of encryption failure.

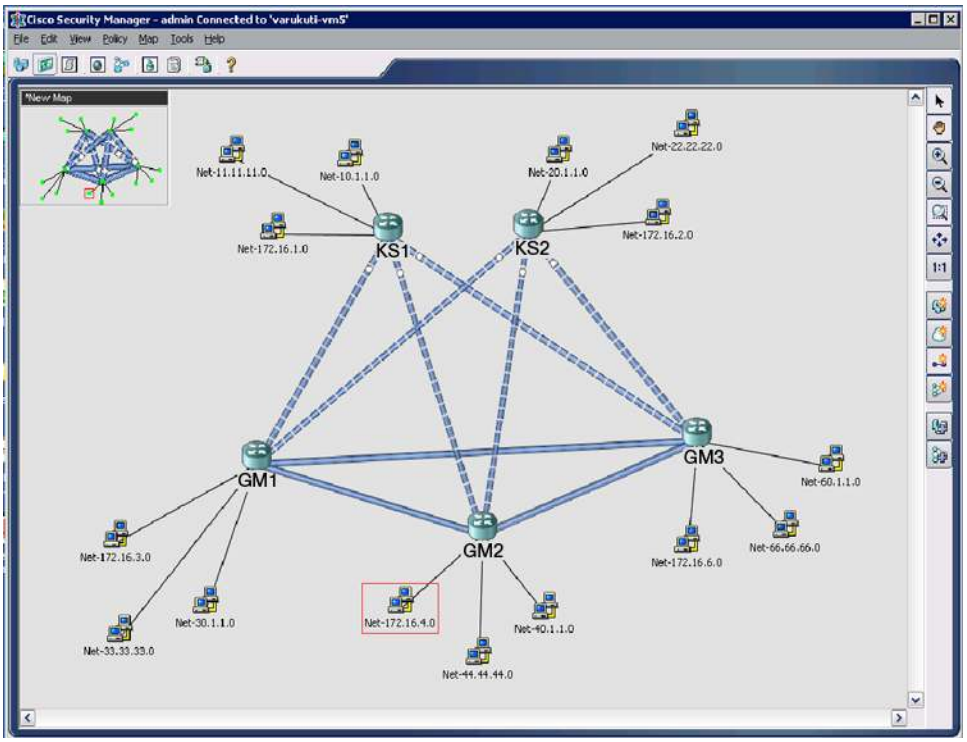
Feature	Description and Benefit
VRF Awareness	GET VPN allows virtualization through the use of Virtual Route Forwarding (VRF). Group Members configured with multiple VRFs can be used to carry traffic belonging to separate entities within an organization (e.g. Government agencies). The Key Server is to be treated as a server rather than a router – it does not participate in routing. As such, it is not VRF aware, and can be placed in a location that has access to all the VRFs (similar to the Root CA Server). • VRF-Lite: Group Members support data plane separation via VRF-Lite. Further isolation can be achieved by placing the VRFs in separate groups. • VRF-Aware GDOI: Group Members can be configured with a separate VRF for the control plane traffic ie: registrations and rekeys.

Management

Cisco Security Manager is an enterprise-class management application designed to configure VPN, firewall, and intrusion prevention system (IPS) security services on Cisco network and security devices. Version 3.3 adds GET VPN support including the following features:

- GET VPN Configuration wizard with pre-populated default values.
- Discovery and provisioning of Group Members and Key Servers.
- Adding a new Group Member at a new site or a new Key Server made simple in just 3 steps: clone existing Group Member or Key Server, modify, and deploy.
- Parameters that can be configured include: Group IPSec SA, KEK, TEK, Unicast and Multicast rekey distribution, and Anti replay on Key Server; and Local Security Policy on Group Members.
- Cooperative Key Servers configuration for both high availability and load sharing.
- Easy migration of clear-text and IPsec VPNs to GET VPN.

Figure 5. Configuring GET VPN with Cisco Security Manager



Cisco® Configuration Professional is a GUI device management tool for Cisco IOS® Software-based access routers, including Cisco integrated services routers, Cisco 7200 Series Routers, and the Cisco 7301 Router. Version 1.4 adds GET VPN support, simplifying configuration through GUI-based easy-to-use wizards. The application is available as a free download from Cisco.com for all supported platforms.

Cisco Group Encrypted Transport supports Easy Secure Device Deployment for secure device provisioning in PKI deployments.

Monitoring and debugging for GET VPN is provided through syslogs.

System Requirements

Hardware IPsec acceleration is recommended, and helps ensure optimal performance of the GET VPN network. IPsec acceleration is supported with the onboard processors within the Cisco Integrated Services Routers and ASR 1000 Series Routers; further acceleration is supported on some models using optional acceleration modules. For IPsec acceleration on the Cisco 7200 Series Routers and the Cisco 7301 Routers, VPN modules are mandatory, as listed below.

Tables 2 and 3 list the hardware and software requirements to install and use Cisco GET VPN.

Table 2. Cisco Hardware Platforms That Support Cisco GET VPN

Feature	Platform	Cisco VPN Acceleration
GET VPN Group Member	Cisco 870, 880, 890, 1800, 1900, 2800, 2900, 3800, and 3900 Series Integrated Series Routers	On-board IPsec Acceleration
	Cisco 1841, 2800, and 3800 Series Integrated Series Routers	AIM-VPN/SSL-1, AIM-VPN/SSL-2, AIM-VPN/SSL-3*
	Cisco 7200 Series Routers	VPN Acceleration Module 2+ (VAM2+), VPN Services Adapter (VSA) with NPE-G2
	Cisco 7301 Routers	VAM2+
	Cisco ASR 1000 Series Routers**	Onboard IPsec Acceleration with ESP-2.5G, ESP-5G, ESP-10G, and ESP-20G
GET VPN Key Server	Cisco 1841; Cisco 1900, 2800, 2900, 3800, and 3900 Series Integrated Services Routers	On-board IPsec Acceleration
	Cisco 1841, 2800, and 3800 Series Integrated Series Routers	AIM-VPN/SSL-1, AIM-VPN/SSL-2, AIM-VPN/SSL-3*
	Cisco 7200 Series Routers	VAM2+, VSA with NPE-G2
	Cisco 7301 Routers	VAM2+

* Cisco ISRs with Cisco AIM-VPN-HPII-PLUS, Cisco AIM-VPN-EPII-PLUS, Cisco AIM-VPN-BPII-PLUS are supported; however they do not accelerate the GDOI RFC 3547 functionality (control plane)
** Cisco ASR 1000 Series routers do not support GET VPN VRF-Lite or VRF-aware GDOI features

Table 3. Cisco GET VPN Software Requirements

Platform	Feature Set and License	Recommended Release
Cisco 870, 880, 890, 1800, 2800, and 3800 Series Integrated Services Routers	Requires SEC, VSEC or HVSEC bundle or equivalent.	Cisco IOS Software Release 12.4(15)T8
Cisco 1900, 2900, and 3900 Series Integrated Services Routers	Requires SEC Technology Package License.	Cisco IOS Software Release 15.0
Cisco 7200 Series and 7301 Routers	Requires Advanced Security feature set or higher.	Cisco IOS Software Release 12.4(15)T8
Cisco ASR 1000 Series Routers	Requires Advanced Enterprise Services or Advanced IP Services feature sets, along with VPN License.	Cisco IOS Software XE Release 2.3.2

To Download the Software

Visit the Cisco Software Center to download Cisco IOS Software.

Cisco and Partner Services for the Branch

Services from Cisco and our certified partners can help you transform the branch experience and accelerate business innovation and growth in the Borderless Network. We have the depth and breadth of expertise to create a clear, replicable, optimized branch footprint across technologies. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help improve operational efficiency, save money, and mitigate risk. Optimization services are designed to continuously improve performance and help your team succeed with new technologies. For more information, visit http://www.cisco.com/go/services.

For More Information

For more information about Cisco Group Encrypted Transport, visit http://www.cisco.com/go/getvpn or contact your local account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-373601-05 11/09