Cisco Group Encrypted Transport VPN

Q. What is Cisco Group Encrypted Transport VPN?

A. Cisco Group Encrypted Transport is a next-generation WAN VPN solution that defines a new category of VPN, one that does not use traditional point-to-point tunnels. For the first time, it eliminates the need to make the compromise between network intelligence and data privacy. This new security model introduces the concept of “trusted” group member routers, which use a common security methodology that is independent of any point-to-point relationship. By eliminating point-to-point tunnels, Cisco Group Encrypted Transport VPNs can scale much higher while accommodating multicast applications and instantaneous branch-to-branch transactions.

Q. What are the key features of Cisco Group Encrypted Transport?

A. Cisco Group Encrypted Transport is a standards-based technology that integrates routing and security in the network fabric. The key features include:

- **Group Domain of Interpretation:** GDOI (RFC 3547) is the key management protocol that establishes security associations among authorized group member routers.
- **IP header preservation:** The original IP header inside the IPsec packet is preserved.
- **Centralized key and policy management:** A central key server pushes keys and re keyed messages as well as security policies to authorized group member routers. Policies supported include global policies—applicable to all members in a group—and local policies. Cooperative Key Server support enables high availability by synchronizing keys and the policy database with a secondary key server router.

Q. What benefits does Cisco Group Encrypted Transport VPN provide for an MPLS network?

A. Cisco Group Encrypted Transport VPN adds any-to-any encryption to an MPLS network without a tunnel overlay, maintaining the high scale, manageability, and routing intelligence of the existing MPLS network. It meets the requirements of security-conscious enterprises looking for a balance in network control since they may add encryption to the network themselves. In addition, it alleviates the complexity in adding any-to-any IPsec to large MPLS networks with requirements. Moreover, it addresses regulatory-compliance guidelines regarding encryption such as HIPAA and PCI.

Q. Who should use Cisco Group Encrypted Transport?

A. 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 Cisco Group Encrypted Transport to help ensure data privacy while maintaining the any-to-any connectivity intrinsic in their private WANs. In doing so, organizations attain a much-needed balance of control over security among their businesses and service providers while maintaining compliance with security regulations.

For enterprises deploying IPsec VPNs over the public Internet, Cisco Group Encrypted Transport provides additional value by enhancing Dynamic Multipoint VPN (DMVPN) and generic routing encapsulation (GRE)-based site-to-site VPNs. Specifically, these customers

can take advantage of almost instantaneous branch-to-branch connectivity, while improving the core meshing capability they already have.

Satellite multicast provides an efficient and cost-effective way to deliver bandwidth-rich content such as video, audio, and software upgrades to multiple sites. Using Cisco® Group Encrypted Transport in conjunction with the Cisco IP VSAT Satellite WAN Module and the Cisco Enterprise CDN (Content Delivery Network) solution, enterprise customers can (skn: efficiently protect their multicast traffic while creating a highly secure, reliable, and scalable content delivery system for their branch offices worldwide.)

Details of Cisco Group Encrypted Transport VPN topologies and configurations can be found at http://www.cisco.com/go/getvpn.

Q. Is Cisco Group Encrypted Transport applicable only for MPLS VPNs?

A. No, Cisco Group Encrypted Transport is WAN-agnostic. It can be deployed on an MPLS, IP, Frame Relay, or ATM network. For deployment with internet based environments, Cisco Group Encrypted Transport must be deployed with DMVPN.

Q. What are the technical benefits of Cisco Group Encrypted Transport VPN?

A. Table 1 lists the technical benefits of Cisco Group Encrypted Transport VPN.

Table 1. Technical Benefits of Cisco Group Encrypted Transport VPN

Previous Limitation	New Feature	Benefit
Encrypting multicast traffic was not scalable and it was difficult to troubleshoot.	Encryption is supported for native multicast and unicast traffic with Group Encrypted Transport's GDOI protocol.	Allows for higher scale and simplifies troubleshooting
Overlay VPN networks created overlay routing, lack of advanced QoS, and suboptimal multicast replication.	The original IP header is preserved, so no overlay network is required.	Achieves optimal routing and maintains network intelligence such as efficient multicast and advanced QoS

Q. What are the advantages of Cisco Group Encrypted Transport VPN vs traditional point-to-point IPsec?

A. Cisco Group Encrypted Transport has the following advantages:

Traditional Point-to-Point IPSec Tunnels	GET VPN
Scalability—an issue (N^2 problem). IKE/IPsec tunnels between each pair of peers	Scalable architecture. Single SA and key pair used for entire any-to-any group.
Any-to-any instant connectivity can't be done to scale	Any-to-any instant connectivity to high-scale
Overlay routing	No overlays—native routing
New IP Header added to original packed results in Limited advanced QoS	IP header preservation keeps original IP header on Ipsec packet, preserves advanced QoS
Multicast replication inefficient due to tunnel overlay	IP header preservation and lack of tunnel overlay results in efficient multicast replication

Q. What are the differences between DMVPN and Cisco Group Encrypted Transport?

A. DMVPN and Cisco Group Encrypted Transport are complementary. When used in a DMVPN environment, Cisco Group Encrypted Transport can aid in the deployments of voice and video over a VPN:

- DMVPN provides spoke-to-hub and spoke-to-spoke connectivity solutions using multipoint GRE (mGRE) and Next Hop Resolution Protocol (NHRP) functions. For spoke-to-spoke connectivity, the originating spoke must send an NHRP resolution request to the hub in order to establish a tunnel with the requested spoke. Until the dynamic tunnel is built, traffic continues to pass through the hub. To receive the response from the destination spoke, the same procedure is initiated by the destination spoke.

- By using Cisco Group Encrypted Transport, the delay caused by IPsec tunnel negotiation—which is the major contributor to the overall delay—is eliminated as connections are static. It is important to note that when group keying is applied to the tunnel in a DMVPN context, all tunnel traffic is encrypted with the group key.

Q. When should Cisco Group Encrypted Transport be deployed?

A. Consider deploying Cisco Group Encrypted Transport when interested in a VPN installation that involves:

- Securing private WAN connections
- Encrypting data over MPLS networks
- Securing multicast traffic
- Deploying voice or similar collaborative applications requiring any-to-any encryption
- Encrypting IP packets over satellite links

Q. When should customers be interested in a Cisco VPN solution other than Cisco Group Encrypted Transport?

A. Customers interested in a VPN for hub-and-spoke connectivity can deploy “vanilla” IPsec point-to-point tunnels, Cisco Enhanced Easy VPN with virtual tunnel interfaces (VTIs) or Cisco Dynamic Multipoint VPN (DMVPN) Customers needing partial-mesh spoke-to-spoke VPNs should deploy DMVPN or DMVPN with Cisco Group Encrypted Transport VPN. Customers interested in multicast and routing protocols over the Internet should deploy DMVPN with Cisco Group Encrypted Transport. Customers interested in encryption while supporting multicast applications and dynamic routing, and customers deploying voice over a classic WAN should deploy Cisco Group Encrypted Transport.

Q. What is GDOI?

A. GDOI is the ISAKMP Domain of Interpretation (DOI) for group key management. In this trusted group model, the GDOI protocol operates between each group member and the group controller, or key server, to establish security associations between authorized group member routers.

Q. Can Cisco Group Encrypted Transport be deployed in Internet-based environments?

A. For enterprise IPsec VPNs that traverse the public Internet, Group Encrypted Transport enhances Dynamic Multipoint VPN (DMVPN) and GRE-based site-to-site VPNs by providing manageable, highly scalable network meshing cost-effectively by using the group shared key. In this way, Group Encrypted Transport simplifies key management in large network deployments. Cisco Group Encrypted Transport requires DMVPN for Internet-based deployments because it requires IP public addresses.

Q. How is voice supported in a Cisco Group Encrypted Transport network?

A. The voice-over-IP (VoIP) application is very sensitive to end-to-end delay. Cisco Group Encrypted Transport provides security to voice applications with an optimized path across the network. Call setup time is reduced because there is a direct path between the group members. In a DMVPN scenario, the addition of Cisco Group Encrypted Transport reduces latency during spoke-to-spoke tunnel setup and enhances the quality of voice calls over a VPN network.

Q. What platforms are supported with Cisco Group Encrypted Transport?

A. Cisco Group Encrypted Transport is supported on the Cisco 800, 1800, 2800, and 3800 Series Integrated Services Routers as well as on the Cisco 7301 and 7200 Series routers and the Cisco ASR 1000 Series routers.

Q. What software release is required to use Cisco Group Encrypted Transport?

A. The Cisco 800 through Cisco 7200 Series and Cisco 7301 Routers must use Cisco IOS® Software Release 12.4(11) T Advanced Security image or later. The Cisco ASR 1000 Series Routers must use the Advanced Enterprise Services or Advanced IP Services image options of the Cisco IOS XE Software Release 2.3.0 or later. Note that the Cisco ASR 1000 Series Routers can support only the Group Member role and do not support VRF-lite application currently.

Q. Can Key Servers be deployed in different geographic locations in the network?

A. Yes

Q. What is the Max number of Key Servers that can be deployed in a Cisco Group Encrypted VPN?

A. The current maximum number of key servers that can be deployed is 8.

Q. Can individual group member connections be monitored at the key server?

A. Yes, several command-line interface (CLI) commands are available to monitor group members. One example is show crypto group.

Q. What routing protocols are supported with Cisco Group Encrypted Transport?

A. Because Cisco Group Encrypted Transport does not introduce an overlay routing model, all routing protocols are supported. Cisco Group Encrypted Transport supports Layer 3 Enhanced Interior Gateway Routing Protocol (EIGRP), On-Demand Routing (ODR), and Open Shortest Fast Path (OSPF).

Intermediate System-to-Intermediate System (IS-IS) is not supported because it does not use IP as its network or transport protocol. Border Gateway Protocol (BGP) is supported, but requires specification of all the neighbors individually in the configuration.

Q. Does Cisco Group Encrypted Transport support resiliency and failover features?

A. Cisco Group Encrypted Transport provides failover between key servers with a feature called Cooperative Key Server. Cooperative key servers ensure that the keying data, such as group policy, active group members, and tunnel encryption key, is shared and kept synchronized between key servers. One primary key server is designated per group. The role of primary key server is determined by priority or by highest IP address.

For More Information

Q. Where can I get more information?

A. For more information, go to http://www.cisco.com/go/getvpn or contact your account team for more information.

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 C67-376506-03 03/09