Cisco Site-to-Site VPN Technologies Comparison

At-A-Glance

Cisco Systems® provides the most feature-rich and flexible site-to-site VPN solutions in the industry. Cisco® site-to-site VPN solutions integrate advanced network intelligence and routing to deliver reliable transport for complex mission-critical traffic, such as voice and client-server applications, without compromising communications quality. These solutions are built on five underlying VPN technologies: Dynamic Multipoint VPN (DMVPN), Easy VPN, GRE tunneling, standard IP Security (IPsec), and the new Group Encrypted Transport VPN (GET-VPN). Each technology has it benefits and is customized to meet specific deployment requirements. Following is a comparison of the technologies and guidance on when to use them.

	Cisco GET-VPN	Cisco DMVPN	Cisco GRE-Based VPN	Cisco Easy VPN	Standard IPsec VPN
	Tunnel-less VPN	Tunnel-based VPN			
Customer Benefits	▪ Simplifies encryption integration on IP and Multiprotocol Label Switching (MPLS) WANs ▪ Simplifies encryption management through use of "group keying" instead of point-to-point key pairs ▪ Enables scalable and manageable any-to-any connectivity between sites ▪ Supports quality of service (QoS), multicast, and routing	▪ Simplifies encryption configuration and management for point-to-point GRE tunnels ▪ Provides on-demand spoke-to-spoke tunnels ▪ Supports QoS, multicast, and routing	▪ Enables transport of multicast and routing traffic across an IPsec VPN ▪ Supports non-IP protocols ▪ Supports QoS	▪ Simplifies IPsec and remote-site device management through dynamic configuration policy-push ▪ Supports QoS	▪ Provides encryption between sites ▪ Supports QoS
When to use	▪ Adds encryption to MPLS or IP WANs while preserving any-to-any connectivity and ▪ networking features ▪ Offers scalable, full-time meshing for IPsec VPNs ▪ Enables participation of smaller routers in meshed networks ▪ Simplifies encryption key management while supporting routing, QoS, and multicast	▪ Simplifies configuration for hub-and-spoke VPNs while supporting routing, QoS, and multicast ▪ Provides low-scale, on-demand meshing	▪ Use when routing must be supported across the VPN ▪ Use for same functions as hub-and-spoke DMVPN, but it requires more detailed configuration	▪ Use when simplifying overall VPN ▪ configuration and management is ▪ the primary goal, but only limited networking features are required ▪ Use to provide simple, unified configuration framework for mix of Cisco VPN products	▪ Use when multivendor interoperability is required
Product interoperability	Cisco routers only	Cisco routers only	Cisco routers only	Cisco, ASA 5500 Series, Cisco VPN 3000 Series, and Cisco PIX® Firewall	Multivendor
Scale	Thousands	Thousands hub and spoke; hundreds partially meshed spoke-to-spoke connections	Thousands	Thousands	Thousands
Provisioning and management	CLI, Cisco Security Manager	Cisco Security Manager and Cisco Router and Security Device Manager	Cisco Security Manager and Cisco Router and Security Device Manager	Configuration automatically pushed to remote sites from headend; headend policies defined in Cisco Security Manager or Cisco Router and Security Device Manager	Cisco Security Manager and Cisco Router and Security Device Manager
Topology	Hub and spoke; any-to-any	Hub and spoke; on-demand spoke-to-spoke partial mesh; spoke-to-spoke connections automatically terminated when no traffic present	Hub and spoke; small-scale meshing as manageability allows	Hub and spoke	Hub and spoke; small-scale meshing as manageability allows
Routing	Supported; Cisco GET-VPN any-to-any connectivity capability can also be used to provide secure routing across an entire router backbone	Supported	Supported	Not supported	Not supported
QoS	Supported	Supported	Supported	Supported, but QoS policy is not dynamically pushed to the remote sites	Supported
Multicast	Natively supported across MPLS and private IP networks; tunneled across Internet-based WANs	Tunneled	Tunneled	Not supported	Not supported
Non-IP Protocols	Not supported	Not supported	Supported	Not supported	Not supported
Private IP addressing	Requires use of GRE or DMVPN with Cisco GET-VPN to support private addressesacross public Internet backbones	Supported	Supported	Supported	Supported
High availability	Routing	Routing	Routing	Stateless failover	Stateless failover

C45-376503-00 11/06