Cisco Easy VPN

General Overview

Q. What is Cisco® Easy VPN?

A. Cisco Easy VPN is an IP Security (IPsec) virtual private network (VPN) solution supported by Cisco routers and security appliances. It greatly simplifies VPN deployment for remote offices and mobile workers. Cisco Easy VPN is based on the Cisco Unity® Client Framework, which centralizes VPN management across all Cisco VPN devices, thus reducing the management complexity of VPN deployments. There are three components of the Cisco Easy VPN solution: Easy VPN Client, Easy VPN Remote, and Easy VPN Server.

Q. What is Cisco Easy VPN Client?

A. The Cisco Easy VPN Client enables mobile workers to create a remote-access VPN connection to a Cisco Easy VPN Server. Cisco Easy VPN Client refers to the Cisco VPN Client, which is also commonly referred to as the Cisco Software VPN Client. For more information, please visit http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html.

Q. What is Cisco Easy VPN Remote?

A. The Cisco Easy VPN Remote enables Cisco routers and security appliances to establish a site-to-site VPN connection to a Cisco Easy VPN Server without complex remote-side configuration. Cisco Easy VPN Remote is also commonly referred to as a hardware client. For more information, please visit http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftezvpnr.html.

Q. What is Cisco Easy VPN Server?

A. The Cisco Easy VPN Server accepts connections from Cisco Easy VPN Client and Remote, ensures that those connections have up-to-date policies in place before the connections are established. All Cisco Easy VPN Servers are interoperable with all Cisco Easy VPN Client and Remote. For more information, please visit: http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_easy_vpn_srvr.html

Q. How does the Cisco Easy VPN solution reduce the management complexity in deploying IPsec VPNs?

A. The Cisco Easy VPN solution uses the Mode-Configuration (Mode-Config) mechanism within the Internet Key Exchange (IKE) to push policy (attributes) from the Easy VPN Server to the Easy VPN Client or Remote. Since this policy is pushed to the client or the remote every time a new tunnel is created, it makes it easier to propagate new policy changes. Mode-Config also enables the Client or the Remote to have minimal configuration in order to establish the tunnel.

Q. What types of attributes can be pushed to the Cisco Easy VPN Client or Remote through Mode-Config?

A. The attributes that can be pushed down through Mode-Config include: internal IP address, internal subnet mask, Domain Name Server (DNS) addresses, Windows Internet Name Service (WINS) addresses, backup server list, domain name, client firewall policy, Cisco IOS® Software configuration, login banner, and Split Tunneling Include List. For a complete list of Cisco Easy VPN attributes, refer to the appendix.

Q. Who can benefit from a Cisco Easy VPN solution?

A. Customers that need to deploy and manage large-scale site-to-site and remote-access VPNs should consider a Cisco Easy VPN solution because of its simplification of VPN management and configuration. Cisco Easy VPN supports quality of service (QoS) and multicast, but if there is a requirement to support dynamic routing protocols or direct spoke-to-spoke communications, Cisco recommends Dynamic Multipoint VPN (DMVPN) as the preferred site-to-site VPN solution. For more information on DMVPN, please visit http://www.cisco.com/go/dmvpn.

Q. What is Cisco Enhanced Easy VPN?

A. Cisco Enhanced Easy VPN is a new method for configuring Easy VPN using Dynamic Virtual Tunnel Interface (DVTI) instead of a crypto map, which is used by traditional Easy VPN. DVTI can be used on both the Easy VPN Server and Easy VPN Remote routers. DVTI relies on the virtual tunnel interface to create a virtual access interface for every new Easy VPN tunnel. The configuration of the virtual access interface is cloned from a virtual template configuration. The cloned configuration includes the IPsec configuration and any Cisco IOS Software feature configured on the virtual template interface, such as QoS, Network Address Translation (NAT), Context-Based Access Control (CBAC) firewall, NetFlow, or access control lists (ACLs). More details at: http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ipsec_virt_tunnl.html

Q. What benefits does DVTI bring to the Cisco Easy VPN solution?

A. Benefits are listed in Table 1.

Table 1. Benefits of DVTI

DVTI Features	Customer Benefits
Simplified VPN Configuration	
• Eliminates crypto maps, crypto ACLs, and generic routing encapsulation (GRE) • Requires minimal router configuration	• Ease of management • Allows rapid deployment of VPNs
Supports per-Session Features	
• Per-user attributes such as QoS	• Empowers the administrator to set proactive policies in delivering the desired application performance, which results in increased user satisfaction and productivity
Integrated with Cisco Easy VPN Solution	
• Hardware client has a separate interface context; tunnel-specific features can be applied • Cisco Easy VPN Server has DVTI; tunnel-specific features can be applied	• Integration of features and investment protection results in lower TCO • Flexibility to customize configuration and security based on site-specific needs
Virtual routing and Forwarding (VRF) Configured on the Interface	
• Multiple VRFs can be terminated in multiple interfaces	• Simplifies large-scale service provider and enterprise Multiprotocol Label Switching (MPLS) deployments

For more information on DVTI, please visit http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_ipsec_virt_tunnl_ps6350_TSD_Products_Configuration_Guide_Chapter.html#wp1078846.

Q. How does Cisco Enhanced Easy VPN improve scalability?

A. Based on DVTIs, Cisco Enhanced Easy VPN improves scaling by providing a single Security Association (SA) per remote site. This improves the overall scalability of deploying split tunneling and multiple routed subnet features under Cisco Easy VPN. Depending on the extent that these features were configured under Easy VPN based on crypto maps, the penalty on the available IPsec SA pool could be severe. This penalty is removed with Easy VPN based on DVTI, and platform tunnel limits are no longer reduced when customers deploy split tunneling and/or multiple routed subnet features.

Q. Is QoS supported with Cisco Enhanced Easy VPN?

A. Cisco Enhanced Easy VPN supports QoS per tunnel since 12.4(11)T2. QoS per tunnel can be turned on at the server and/or remote. At the Server, there are performance issues when enabling shaping or queuing with a large number of VTI tunnels (up to 100). Performance improvement is available since 12.4(15)T3. Other QoS policies, such as policing or marking, can be easily supported on both hub and spoke. Weighted Random Early Detection (WRED) is not supported.

Q. What is VRF-Aware IPsec? Does Cisco Easy VPN support this?

A. The VRF-Aware IPsec feature introduces IPsec tunnel mapping to MPLS VPNs. Using the VRF-Aware IPsec feature, you can map IPsec tunnels to VRF instances using a single public-facing address. VRF-Aware IPsec

was introduced to Cisco Easy VPN Server in Cisco IOS Software Release 12.2(15)T. Note: VRF is supported only on the server, not the remote. For generic VRF-Aware IPsec configuration information, please visit http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_vrf_aware_ipsec_external_docbase_0900e4b1805b06d8_4container_external_docbase_0900e4b1807b3707.html.

Q. Can I deploy standard Easy VPN and Enhanced Easy VPN on the same router?

A. Yes, Standard Easy VPN and Enhanced Easy VPN can coexist on the same router.

Availability

Q. Which Cisco products support Cisco Easy VPN Remote?

A. Cisco Easy VPN Remote is available on Cisco 800, 1800, 1900, and 2800 Series Integrated Service Routers and Cisco ASA 5505 Adaptive Security Appliances.

Q. Which Cisco products support Cisco Easy VPN Server?

A. Cisco Easy VPN Server is available on numerous Cisco IOS Software-based routers, including Cisco 1800, 1900, 2800, 2900, 3800, 3900, 7200 Series Routers and Cisco 7301 Router. It is also available on all Cisco ASA Adaptive Security Appliances.

Q. Which Cisco IOS Software release initially supports DVTI? Which Cisco products support DVTI?

A. DVTI is supported on Cisco IOS Software Release 12.4(4)T and higher; on Cisco 1800, 1900, 2800, 2900, 3800, 3900 and 7200 Series Routers; and on the Cisco 871/881/891 Integrated Services Router.

Q. What are the Cisco Easy VPN features in the Cisco IOS Software 12.4T release train?

A. The specific Easy VPN features are as follows:

Table 2. Easy VPN Features

Feature	Description
Easy VPN DVTI	12.4(2)T
Login Banner to Easy VPN Hardware	12.4(2)T
Auto Update for Software Clients	12.4(2)T
Browser Proxy Configuration	12.4(2)T
Auto Configuration Update	12.4(4)T
Dial Backup Reactivate Primary Peer	12.4(4)T
Easy VPN Remote Dual Tunnel Support	12.4(4)T
PKI AAA Integration	12.4(4)T
Easy VPN Password Aging via AAA	12.4(6)T
Easy VPN Firewall Policy Push	12.4(6)T
IPsec over TCP on Easy VPN Server	12.4(9)T
Firewall Traversal	12.4(9)T
NAT Transparency	12.4(9)T
DHCP Client Proxy and Dynamic DNS Registration	12.4(9)T
Split DNS	12.4(9)T
VTI Enhancements—per User Policy Taken from RADIUS	12.4(9)T
TI Manageability—Debug Show Commands	12.4(11)T
One-to-One NAT	12.4(11)T
QoS per tunnel on Enhanced Easy VPN	12.4(11)T
Easy VPN Remote Identical Addressing	12.4(15)T
Reverse Route INJECTION Enhancement	12.4(15)T
cTCP on Eas yVPN Remote	12.4(20)T

Q. What's the feature disparity between standard EasyVPN and Enhanced Easy VPN?

A. Table 3 lists the major feature disparity. For those features that are not listed in the table, they are supported on both.

Table 3. Standard Easy VPN and Enhanced Easy VPN Feature Disparity

Feature	Standard Easy VPN	Enhanced Easy VPN
Stateful Failover	Y	N
VRF-Aware IPsec	Y	Y
NAC Integration	Y	Y
Dynamic Routing	N	N
Auto Config Update	Y	Y
Dial Backup—Reactivate Primary Peer	Y	Y
Secure Multicast	N	Y
Qos per Tunnel	N	Y
Remote Dual Tunnel	Y	Y
Remote Identical IP Addressing	N	Y
RRI Distance Metric Enhancement	Y	Y

Q. Does Cisco Easy VPN Remote support Network Admission Control?

A. Yes. Network Admission Control (NAC) has worked with Cisco Easy VPN since Cisco IOS Software Release 12.3(8)T and with Cisco Enhanced Easy VPN since 12.4(4)T to query the client posture after the IPSec connection has been established. NAC uses Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) to query the Cisco Trust Agent on the PC, and allows a PC to access the network after it has passed the validation. For more information, please visit http://www.cisco.com/en/US/products/ps6635/products_white_paper0900aecd805092e0.shtml

Q. What is Cisco IOS Secure Multicast?

A. Cisco IOS Secure Multicast is a set of hardware and software features necessary to secure IP Multicast group traffic originating on or flowing through a Cisco IOS device. It combines the Group Domain of Interpretation (GDOI) with hardware-based IPsec encryption to provide users with an efficient way to secure IP Multicast group traffic. With Cisco IOS Secure Multicast, a router can apply encryption to IP Multicast traffic without having to configure tunnels.

Q. Does Cisco Easy VPN support Cisco IOS Secure Multicast?

A. No. Cisco Easy VPN does not support Cisco IOS Secure Multicast. Cisco Group Encrypted Transport VPN (GETVPN) solution supports Secure Multicast using Tunnel-less technology. For more GETVPN information, please visit: www.cisco.com/go/getvpn

Q. Does Cisco Easy VPN carry secure multicast traffic?

A. Cisco Enhanced Easy VPN carries secure multicast traffic.

Q. Where can I get more information about Easy VPN?

A. For more information about Cisco Easy VPN, visit http://www.cisco.com/go/easyvpn or send an e-mail to ask-stg-ios-pm@cisco.com

Positioning

Q. Are there any standard guidelines that customers can use when deciding on a Cisco Easy VPN solution?

A. Yes. Usually, customers meeting the following standards should choose Cisco Easy VPN.

1. A VPN connection from the corporate office to a branch office, extranet, reseller, or partner.
2. Capable of doing QoS and services (firewall/ACL) per tunnel if desired.
3. No non-IP traffic will be flowing.
4. Uses Route Injection to inject routes rather than running a dynamic routing protocol.
5. Able to push configuration changes to Easy VPN hardware clients; this can be done on a per-host level.

Q. When would customers be interested in an alternate Cisco VPN solution?

A. If a customer is interested in multicast and routing protocols, it is recommended to deploy:

- IPsec with GRE
- IPsec with Static VTI

If a customer is interested in multicast, routing, and direct spoke-to-spoke communication, DMVPN is recommended.

If a customer is interested in secure multicast, Dynamic Group VPN (DGVPN) is recommended.

If a customer requires clientless VPN, SSL VPN is recommended.

Q. What are the differences between Enhanced Easy VPN and DMVPN?

A. Please see table 4 for the comparison.

Table 4. Cisco Enhanced Easy VPN and DMVPN Comparison

Service/Feature Name	Enhanced Easy VPN	DMVPN
Scalability per Hub	Large number of spokes can be supported per hub	Depends on routing protocol chosen
Identical Configuration for All Spokes	Yes	No
Cross-Platform Support	Yes	No
Support for Software/Hardware Client	Yes	No software client support
Stateful Failover	No; but available with legacy Easy VPN	Depends on routing protocol for recovery
Always up Tunnel to Hub	Not required	Yes
Support for Multicast Traffic	Yes	Yes
Spoke-to-Spoke Direct Communication	No	Yes
Support for QoS	Yes	Yes
Support for Routing Protocols	No	Yes
Support for Certificates	Yes	Yes

Q. What are the differences between Easy VPN and other Site-to-Site VPN solutions?

A. Please refer to the following table 5 for the comparison.

Table 5. Cisco Site-to-Site VPN Solution Comparison

	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 laying" instead of point-to-point key pairs • Enables scalable and manageable any-to-any	• Simplifies encryption of configuration and management for point-to-point GRE tunnels • Supports QoS, multicast, and routing	• Enable transport of multicast and routing traffic across an IPsec VPN • Support 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

	Cisco GET-VPN	Cisco DMVPN	Cisco GRE-Based VPN	Cisco Easy VPN	Standard IPsec VPN
		Tunnel-less VPN		Tunnel-based VPN	
	connectivitiy between sites • Supports quality of services (QoS) multicase and routing				
When to Use	• Add encryption to MPLS or IP WANs while preserving any-to-any connectivity and networking features • Other 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	Mutlivendor
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 any 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 addresses across public Internet backbones	Supported	Supported	Supported	Supported
High Availability	Routing	Routing	Routing	Stateless failover	Stateless failover

Operation

Q. What operation modes does Cisco Easy VPN Remote support?

A. The Cisco Easy VPN Remote feature supports three modes of operation: Client, Network Extension, and Network Extension Plus.

- **Client mode**—Specifies that Network or Port Address Translation (NAT or PAT) be done so that the PCs and other hosts at the remote end of the VPN tunnel form a private network that does not use any IP addresses in the IP address space of the destination server. The server pushes down an IP address to the Easy VPN Client, and all traffic from the client will be internally translated to this address before being encrypted to the Cisco Easy VPN Server.
- **Network Extension mode**—Specifies that the PCs and other hosts at the client end of the VPN tunnel should be given IP addresses that are fully routable and reachable by the destination network over the tunneled network so that they form one logical network.
- **Network Extension Plus mode**—Identical to Network Extension mode with the additional capability of being able to request an IP address through Mode-Config and automatically assign it to an available loopback interface. This can typically be used for management purposes.

Q. How does load balancing work for Cisco Easy VPN Server?

A. Currently, the Cisco Easy VPN Server does not support load balancing. The load balancing of Easy VPN connections is done by inserting an external load balancer, such as the Content Services Module on the Cisco Catalyst® 6500 Series, or using the Cisco IOS Software server load balancing feature on the Cisco 7200 or 6500 Series, in front of Cisco Easy VPN Servers. For more information, please visit http://www.cisco.com/en/US/products/ps6635/products_white_paper0900aecd8045b552.shtml

Q. Is NAT transparency supported by Cisco Easy VPN Remote?

A. Yes. Cisco Easy VPN Remote supports NAT transparency under UDP port 4500 (RFC 3947). It is also called Cisco IOS/IPsec NAT traversal, and addresses the issue of known incompatibilities between IPsec and NAT. Cisco does not support the proprietary VPN 3000 Series-only method for NAT transparency.

Q. What is the IPsec Stateful Failover (HA) feature? Does Cisco Easy VPN support high availability?

A. IPsec Stateful Failover (HA) is a way of increasing IPsec VPN network uptime through redundancy. This feature was brought to Easy VPN in the Cisco IOS Software 12.3T release train, and enables the sharing of IPsec state information that cannot be reconstructed, on a standby device. However, IPsec Stateful Failover is not yet available with Cisco Enhanced Easy VPN.

Q. How many IPsec tunnels does Cisco Easy VPN Server support?

A. Cisco Easy VPN Server supports as many tunnels as are supported by the platform on which it is running. Table 6 shows some typical numbers tested with VPN and minimum other functions enabled.

Table 6. IPsec Tunnels Supported by Cisco Easy VPN Server

Cisco Router Platform	Maximum Number of IPsec Tunnels Supported
800 Series	20
1800 Series	Fixed Platform: 50 1841 (Modular Platform): 200
2800 Series	2801: 300 2811: 350 2821: 400 2851: 450
3800 Series (using AIM-SSL)	3825: 500 3845: 650

Cisco Router Platform	Maximum Number of IPsec Tunnels Supported
ASR-1000 Series	3000 per chassis
7200/7201/7301 Series (using VAM2+)	5000 per chassis
7200 Series (using the VSA)	5000 per chassis
6500 or 7600 Series (using VPN SPA)	8000 per chassis
6500 Series (using 8G+ VSPA)	8000 per chassis

For more information, please send e-mail to ask-stg-ios-pm@cisco.com.

Q. How many concurrent VPN tunnels does Cisco Easy VPN Remote support?

A. If using a virtual interface, Cisco Easy VPN Remote can support as many concurrent tunnels as are supported by the platform resource on which it is running. Cisco recommends using at most two tunnels, but Cisco Easy VPN Remote can support more.

Q. Which Cisco VPN clients does Cisco Easy VPN Server support?

A. Cisco Easy VPN Server supports Cisco Easy VPN Remote clients, Cisco VPN (software) Clients, Cisco ASA 5505 Adaptive Security Appliances and SafeNet IPSec VPN clients.

Q. What is dead-peer detection?

A. Dead-peer detection (DPD) is required for environments in which customers want failover between concentrators on different subnets. This feature allows you to configure your router to query the liveliness of its IKE peer at regular intervals. The benefit of this approach over IKE keepalives is improved performance on the router. With IKE keepalives, an encrypted Keepalive is sent at each interval, which adds to the processing overhead and reduces the data encryption throughput performance. DPDs are sent only if there is outbound traffic, but there has not been any inbound traffic for the DPD interval. Cisco Easy VPN Remote has supported this feature since Cisco IOS Software Release 12.3(7)T.

Q. Is human intervention required to establish the VPN tunnel once it is down?

A. If you configure Cisco Easy VPN Remote to connect to the server using Auto Connect mode, and a static password with “save password” is enabled, human intervention is not required. Otherwise, human intervention is required.

Q. Are certifications and pre-shared keys supported?

A. Yes. Cisco Easy VPN supports both pre-shared keys and Public Key Infrastructure (PKI) certificates.

Q. What authentication mechanism does Cisco Easy VPN provide?

A. The Cisco Easy VPN Remote feature supports a two-stage process for authenticating the remote router to the central concentrator. The first step is Group Level Authentication and is part of the control channel creation. In this first stage, two types of authentication credentials can be used: either pre-shared keys or digital certificates. The second authentication step is called Extended Authentication or Xauth. In this step, the remote side (in this case the Easy VPN router) submits a username and password to the central site router.

Q. What are the typical methods used to activate Xauth in Cisco Easy VPN?

A. There are four ways to activate Xauth in Cisco Easy VPN: automatic activation, traffic-triggered activation, Web-based activation, and console activation.

Automatic and traffic-triggered activation store the Xauth username and password in the configuration file of the router. This option is typically used if the router is shared between several PCs and the goal is to keep the VPN tunnel up all the time (automatic activation) or to have the router automatically bring up the tunnel whenever there is data to be sent (traffic-triggered activation).

Web-based activation does not store username and password data on the router. Instead, a PC user who is connected to the router is presented with a special Webpage that allows the user to manually enter the username and password.

The Xauth username and password can also be manually entered from the command-line interface (CLI) of the router. This method can be useful for network administrators during troubleshooting.

Q. Is user authentication supported with Cisco Easy VPN Remote?

A. Yes. Put the Cisco Easy VPN Remote in Automatic Activation mode to keep the tunnel “up” all the time and use Cisco IOS Authentication Proxy or 802.1x to authenticate the individual PCs. Because the tunnel is always up, Authentication Proxy or 802.1x can access a central site user database such as AAA/RADIUS to authenticate the individual user requests as they are submitted by PC users.

Q. Are IP phones supported through the Cisco Easy VPN Remote?

A. Yes. When the VPN tunnel is up, IP phones are supported. The IP phone is authenticated to the Cisco Unified CallManager at the central site, separately from the router or user authentication. Tighter integration of authentication for various logins is planned for the future.

Q. How does Reverse Route Injection (RRI) work with Cisco Easy VPN?

A. Reverse Route Injection (RRI) is a feature designed to simplify network design for VPNs when there is a requirement for redundancy and routing. RRI works with both dynamic and static crypto maps. When routes are created, they are injected into any dynamic routing protocol and distributed to surrounding devices. This causes traffic flows requiring IPsec to be directed to the appropriate headend VPN router for transport across the correct signature authorities.

Q. How does Dial Backup work with Cisco Easy VPN Remote?

A. The remote router uses reliable static routing to discover when the primary Cisco Easy VPN Server fails. Reliable static routing uses the IP Service Level Agreement (SLA) monitor feature to monitor a remote destination. The reliable static routing polls the Cisco Easy VPN Server availability every 10 seconds. When connectivity to the primary server fails, the reliable static routes are removed from the routing table and the remote router replaces the active crypto map with the backup crypto map. This enables a floating static route to become active and initiate a crypto session over the backup path. Once the primary Cisco Easy VPN Server is reachable again, the IP SLA monitor will reinstall the reliable static route in the routing table, replacing the floating static route, and will reactivate the primary crypto map. The backup path will be torn down after timeout. For more information, please visit http://www.cisco.com/en/US/products/ps6635/products_white_paper0900aecd80393720.shtml

Q. How does Auto Configuration Update work with Cisco Easy VPN?

A. During tunnel setup, Auto Configuration Update allows the Cisco Easy VPN Server to push configuration changes to any number of Cisco IOS Easy VPN hardware clients using Mode-Config. This feature allows the Easy VPN Server to automatically push any configuration update to the clients. This facilitates customized and “zero-touch” provisioning of clients for features such as voice over IP (VoIP) or routing. Auto Configuration Update can also be used to stop worms or attacks in real time by enabling the relevant IPS, firewall, QoS, and other security policies at the client.

Q. What is the Dial Backup Reactivate Primary Peer feature?

A. An existing Cisco Easy VPN Client configuration can be enhanced to use the CLI **peer a.b.c.d default**. The Easy VPN Client tries to set the tunnel up with any of the peers configured one-by-one, starting with the default/primary peer. When the primary peer is down, the client brings up the tunnel to the backup peer. In this case, the client thereafter tries to periodically check the connectivity with the primary peer. Anytime it detects that link is working and the IKE signature authority can be established, the client will tear down the existing connection, and bring the tunnel back up with the primary peer.

Q. Does Cisco Easy VPN Remote support Dual Tunnel?

A. Yes. Cisco Easy VPN Remote allows two tunnels to be built from one remote device connecting to different headend devices, which allows the segregation of application traffic such as voice and data to disparate locations. For more information, please visit http://www.cisco.com/en/US/products/ps6635/products_white_paper0900aecd8039e301.shtml

Q. How does Password Expiry work for Cisco Easy VPN?

A. Cisco Easy VPN environments currently initiate authentication by the software client/router connecting the end user. With Cisco Easy VPN Password Expiry via AAA, authentication servers can notify the client that the password has expired, while providing a generic way for the end user to change the password. This feature will work with the Cisco Secure Access Control System (ACS) and with the Microsoft Active Directory server (which calls for support of the MSCHAPv1/v2 authentication support). With this feature, users can change expired passwords without administrator intervention. For more information, please visit http://www.cisco.com/en/US/products/ps6635/products_white_paper0900aecd80478ad7.shtml

Q. How does Cisco Easy VPN work with personal firewalls?

A. A feature called Centralized Policy Push is introduced in Cisco Easy VPN through Cisco IOS Software Release 12.4(6)T. This feature enhances the Cisco Easy VPN Server, enabling it to push firewall policies to personal firewall products integrated with the Cisco Easy VPN Software Client running on the client's computer. This function has been tested with Cisco Security Agent, Cisco Integrated Client Firewall software, and Zone Labs ZoneAlarm firewalls.

The Cisco Easy VPN Client initially proposes the firewall function it supports to the Easy VPN Server. Based on the firewall policy configured on the server, it will either accept one of the policies proposed by the client and proceed with no client firewall support, or terminate the tunnel setup. This improves security, even with split tunneling. The firewall configuration policies are configured on the server, and these will be sent to the client. The client enforces firewall policies.

This feature is only supported on the Cisco VPN software client, not on the hardware client. For more information, please refer to the Cisco IOS Software Release 12.4T product bulletin, Section 3.1.7, at http://www.cisco.com/en/US/products/ps6441/prod_bulletin09186a00804a84ad.html.

Q. Does Cisco Easy VPN support Cisco Tunneling Control Protocol?

A. Yes. This feature was introduced in Cisco IOS Software Release 12.4.9(T). TCP tunneling of IPsec packets is often requested by traveling employees, who are operating out of hotels or airports, to pass through third-party firewall devices in their environments. To solve this problem without modifying the rules configured in the firewall, Cisco has come up with a protocol called Cisco Tunneling Control Protocol. When Cisco Tunneling Control Protocol is enabled on client and headend devices, IKE and Encapsulating Security Payload (ESP) traffic will be encapsulated in the TCP header, so that the firewalls in between the client and the headend device would simply permit this traffic, considering it as TCP traffic.

Currently, Cisco Tunneling Control Protocol (cTCP) is only supported on the Cisco Easy VPN Server with Cisco VPN software client and ASA5505. cTCP support on IOS based Easy VPN Remote is available starting 12.4(20)T and onwards.

Q. How does Split-DNS work in Cisco Easy VPN?

A. Split-DNS enables the Cisco Easy VPN Client to act as a "DNS proxy," directing Internet queries to the DNS server of the ISP and directing corporate DNS requests to the corporate DNS servers. Without Split-DNS, enterprises typically must point their customer premises equipment (CPE) to the corporate DNS servers for all DNS queries, because only their internal servers can resolve all their internal domains. This means that the internal servers will also have to carry the load of resolving or proxying all the queries for Internet URLs. This puts an unnecessary extra load on this important corporate resource. If Internet queries can be sent to the ISP, the load on the corporate DNS server will be reduced.

Q. How does DHCP Client Proxy Support work in Cisco Easy VPN?

A. This feature was introduced in Cisco IOS Software Release 12.4(9)T. It allows the Cisco Easy VPN Server to assign a DHCP address to a client from the corporate DHCP server rather than the local pool configured on the router or using the framed-IP-address attribute defined in the RADIUS server. Some VPN clients, such as the Windows VPN client, supply their hostname as part of a Mode-Config request that is forwarded to the DHCP server in the DHCP request. DHCP servers that support Dynamic DNS (DDNS) registration can then register the hostname with the IP address assigned with the DDNS server. This will allow anyone in the corporate network to reach the client by its DNS hostname rather than an IP address.

Q. Why a default route is pushed down to the Cisco Easy VPN Remote after the VPN tunnel is up?

A. With no split tunneling, all the traffic needs to be encrypted and sent over the tunnel. Since VTI uses routing to decide which traffic needs to be encrypted, a default route needs to be installed in the case of no-split tunneling. Cisco Easy VPN installs a default route that has a metric value of 1. Any configured default route on the Easy VPN Remote needs to have a metric value greater than 1, so the default route installed by the Cisco Easy VPN Server has precedence over the configured one.

Q. Does Easy VPN support overlapping IP addressing on the client side?

A. Yes. Easy VPN Remote has integrated Network Address Translation (NAT) to allow remote locations with overlapping internal IP addresses. Printers and servers hosted at remote locations are reachable from the hub as well as other spoke locations. You will need to enable Network Extension mode and Dynamic Virtual Tunnel Interface (DVTI) to use this feature.

Interoperability

Q. Which Cisco products support Cisco Easy VPN Remote or Server?

A.

Table 7.

Product	Easy VPN Server	Virtualization Support	Easy VPN Remote
Cisco 800 Router	No	VRF	Yes
Cisco 1800/1900/2800/2900 Router	Yes	VRF	Yes
Cisco 3800/3900 Router	Yes	VRF	No
Cisco 7200/7301 Router	Yes	VRF	No
ASR-100x Router	Yes	None (Roadmap)	No
Catalyst 6500/7600 with IPsec SPA	Yes	VRF	No
ASA5505	Yes	None	Yes
ASA55xx	Yes	FW only	No
VPN3000 Concentrator	Yes	None	No

Q. Can all the EasyVPN remotes work with all the EasyVPN servers?

A. No. Please refer to the following table 8 for the interoperability matrix.

Table 8.

Feature	IOS head-end (crypto-map)	IOS head-end (VTI)	ASA5500/PIX (crypto-map)
IOS Easy VPN Remote	Supported • Creates a single IPsec SA on the headend when a default policy is pushed. • Creates multiple SAs when a split-tunnel policy is pushed to the remote device.	Not supported • Cannot be used with split tunnels because the headend interface does not support multiple SAs on a single interface.	Supported • Creates a single IPsec SA on the headend when a default policy is pushed. • Creates multiple SAs for split tunnels

Feature	IOS head-end (crypto-map)	IOS head-end (VTI)	ASA5500/PIX (crypto-map)
IOS Easy VPN Remote (VTI)	Supported • Will create multiple SAs for a split tunnel. Because there is no interface on the headend, interface features cannot be Supported • Limited quality of service (QoS) is supported. With NEM only supports first ACL negotiated by remote.	Supported • Creates only a single SA in split and no-split tunnels. Route injection is accomplished on the server. • Routes are injected on the remote devices to direct traffic to the interface.	Supported • Creates multiple SAs for split tunnels.
ASA Easy VPN Remote	Supported • Always creates at least two IPsec SAs on the headend.	Not Supported • Cannot be used with split tunnels because the headend interface does not support multiple SAs on a single interface.	Supported • Always creates at least two IPsec SAs on the headend.

Troubleshooting

Q. How do I troubleshoot a VPN connection created using the Cisco Easy VPN Remote feature?

A. Typical troubleshooting methodologies involve the following techniques:

- Be aware of any changes to an active Cisco Easy VPN Remote configuration or IP address changes to the involved interfaces.
- Enable debugging of the Cisco Easy VPN Remote feature using the **debug crypto ipsec client ezvpn** command.
- Enable debugging of IKE events using the **debug crypto ipsec** and **debug crypto isakmp** commands.
- Display the active IPsec VPN connections using the **show crypto engine connections active** command.
- To reset the VPN connection, use the **clear crypto ipsec client ezvpn** command.

Q. How do the new show commands introduced in Cisco IOS Software Release 12.4(9)T enhance Cisco Easy VPN usability?

A. Benefits of the **show** command enhancements include:

- Provides filters to show crypto session commands.New *filters include username, isakmp-profile, group, local-address,* and *interface.*
- Provides *username, isakmp-profile, group, assigned-address, fvrf,* and *ivrf* in the output of “show crypto session” and “show crypto session detail”.
- “show crypto session detail” has another field, *uptime*, which signifies the time elapsed since the first IPsec session was created.
- Provides one-line session information using “brief” extension to “show crypto session” command or any of the other “show crypto session” command variants, such as “show crypto session isakmp group <group> brief”.

Q. What benefits do syslog enhancements bring to Cisco Easy VPN?

A. The greatest benefit of syslog enhancements is a transparent customer experience when debugging problems with Cisco Easy VPN Servers, Cisco VPN 3000 Series Concentrators, or Cisco ASA 5500 Series Adaptive Security Appliances. These enhancements help customers debug and understand Cisco Easy VPN across various platforms. Syslog messages are implemented on the Cisco Easy VPN Server side only.

Support is available for all Cisco IOS routers (except Cisco 6500 and 7600) with Cisco IOS Software Release 12.4(4)T and higher. For more information, please visit http://www.cisco.com/en/US/products/ps6635/products_white_paper0900aecd803fc77b.shtml.

Q. Does Cisco support SafeNet IPSec VPN client?

A. Support is available for all Cisco IOS routers (except Cisco 6500 and 7600) with Cisco IOS Software Release 12.3(14)T Advanced Security and higher. For more information, please visit http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_safenet_suppt_external_docbase_0900e4b1805b0679_4container_external_docbase_0900e4b1807b3707.html.

Appendix

Attributes that can be defined locally in Cisco IOS Software

Group Attributes

1. key—Group pre-shared key
2. dns—DNS servers
3. wins—WINS servers
4. domain—Domain name
5. pool—Address pool for assigning to clients. The pool itself must be configured locally.
6. acl—Split ACL for split-tunneling. The ACL itself must be configured locally.
7. access-restrict—To restrict connections from coming in on a particular interface.
8. group-lock—To restrict users belonging to one group from connecting to another group. This is only for pre-shared keys, not for certificates. This is group-based and cannot be used as a user-based attribute. The delimiters allowed for username@password are /,\.@,%.
9. save-password—To allow client to store username and password in memory for subsequent reconnections.
10. firewall—To verify if a firewall is running on the client. This is valid for software clients only.
11. include-local-lan—For clients to be able to reach the local LAN without going through the IPsec tunnel. This is only valid for software clients.
12. split-dns—Domain name for split tunneling.
13. pfs—Perfect forward secrecy so that key material is freshly derived each time.
14. backup-gateway—Alternate backup IPsec peers to be pushed down to clients.
15. max-users—Maximum number of users that can simultaneously connect within the same group.
16. max-logins—Maximum number of logins that a given user can have.
17. configuration url—URL to be pushed down to client so it can update its configuration.
18. configuration version—Version number of the configuration URL. Clients will get the configuration only if the version is newer than what they have previously downloaded.
19. banner—Banner to display when a client connects.
20. auto-update—URL of operating system binary to be pushed down to clients. This can be used to automatically update client's OS when they connect to the server, if the version they are running is older. This is currently only valid for software clients.
21. netmask—Mask to be applied to the pool IP address pushed down to clients. This is only valid for software clients.

User Attributes

No user attributes can be defined locally in Cisco IOS Software.

For more information about Cisco Easy VPN, visit http://www.cisco.com/go/easyvpn or send an e-mail to ask-stg-ios-pm@cisco.com.

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 C67-366306-10 12/09