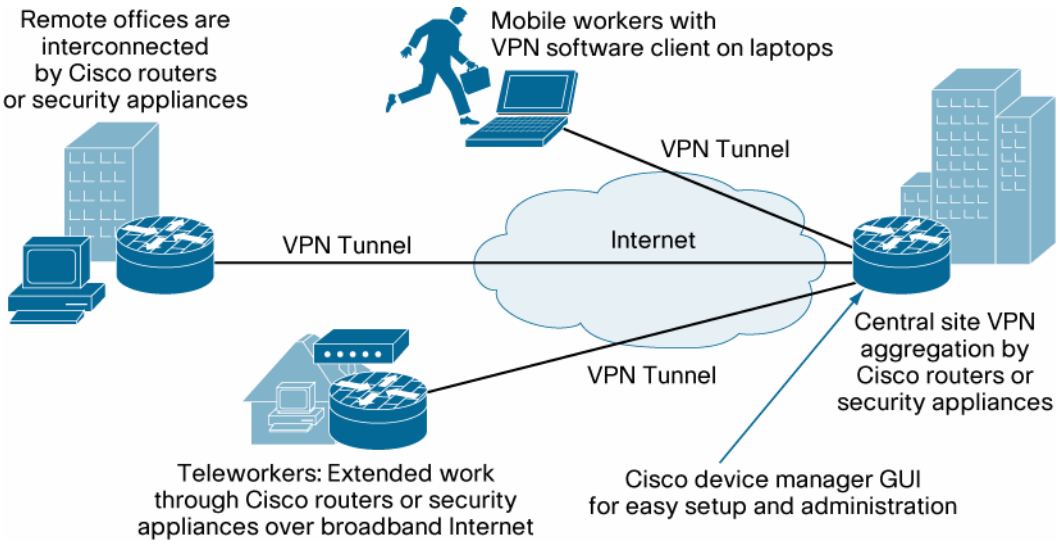
Cisco Easy VPN on Cisco IOS Software-Based Routers

Cisco Easy VPN Solution Overview

The Cisco® Easy VPN solution (Figure 1) offers flexibility, scalability, and ease of use for site-to-site and remote-access VPNs:

- Makes it easier than ever for customers of all sizes to deploy VPNs into locations with limited technical staff—such as small branch offices, teleworkers, and mobile workers
- Offers unprecedented flexibility in choice and support of VPN devices, enabling Cisco routers, security appliances, and software VPN clients to be integrated into a single deployment
- Reduces the management complexity of large-scale VPN deployments by centralizing VPN management with a consistent policy and key management method across all Cisco VPN devices

Figure 1. Cisco Easy VPN Solution Overview



Applications: Small Office Deployment

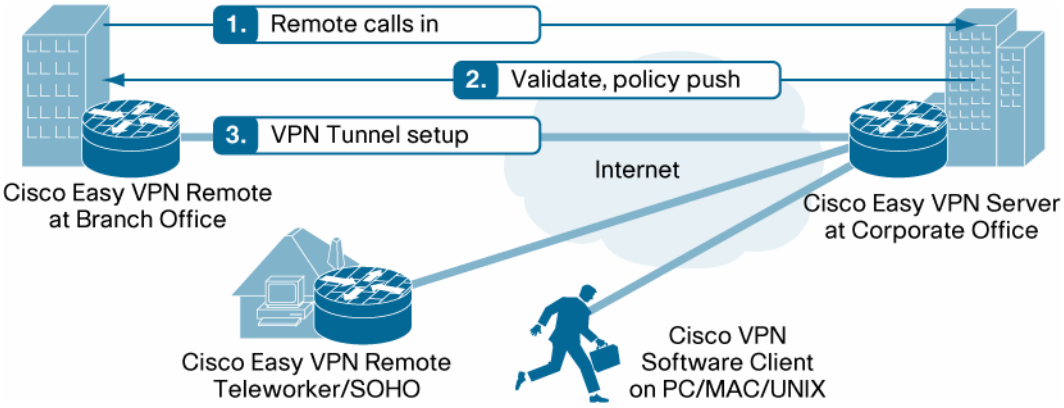
For mobile workers and telecommuters, it's not enough to have a high-performance connection to the Internet. To be truly effective, these users need complete, secure access to electronic resources at the home office, which means establishing a VPN connection with a high level of authentication and the ability to encrypt data. The Cisco Easy VPN solution allows remote workers and telecommuters from small offices or enterprise branch offices to establish VPN connections across the public Internet directly to their home office—making the high-speed network resources they need to do their jobs available to them at a fraction of the cost of alternative secure connections.

Previously, providing secure access to remote workers often entailed using Point-to-Point Tunneling Protocol (PPTP) to connect to a home office. Although this method allows users to terminate a secure connection to their home office, a PPTP tunnel does not provide user authentication, which can lower the overall security threshold of the connection. Alternative methods of establishing a secure connection were limited because they did not support all platforms across the network.

Solution Components

The Cisco Easy VPN solution consists primarily of two operational components: Cisco Easy VPN Remote and Cisco Easy VPN Server (Figure 2).

Figure 2. Cisco Easy VPN Solution



Cisco Easy VPN Remote represents the branch or remote user side of the VPN connection. A variety of devices can participate as Easy VPN Remotes, including Cisco IOS® Software-based routers, Cisco ASA security appliances, and PCs running Cisco VPN Client software.

Cisco Easy VPN Server is the headend side of the VPN tunnel. Cisco IOS Software-based routers, Cisco Catalyst® switches, and Cisco ASA security appliances can act as Easy VPN aggregation points for thousands of Easy VPN Remote devices, including devices at branch office, teleworker, and mobile worker sites.

Cisco Easy VPN Servers use centralized policy push to send predefined security policies and configuration parameters automatically to Easy VPN Remote devices. For example, configuration parameters such as internal IP addresses, internal subnet masks, DHCP server addresses, WINS server addresses, and split-tunneling flags can be pushed to the remote device. This simplifies management, making it ideal for remote offices with little IT support, or large-scale customer premises equipment (CPE) deployments where it is impractical to individually configure multiple remote devices.

Features and Benefits

The Cisco Easy VPN solution provides numerous features and benefits, including:

- **Network integration:** Cisco IOS Software delivers advanced VPN solutions that work across multiple topologies and use cases. The key to this is network integration—the ways in which VPN and IP services are integrated within the device as well as across multiple devices on the network.
- **Ease of management:** The Cisco Easy VPN solution offers ease of ongoing management, with features such as centralized policy push and an Enhanced Easy VPN architecture (virtual tunnel interface integration).
- **Authentication:** Cisco Easy VPN supports a two stage process for authenticating the remote client and user using both group and xauth level authentication.
- **Scalability and high availability:** Cisco Easy VPN Servers are able to aggregate thousands of remote devices, enabling highly scalable deployments. In these scenarios, high availability is a prime consideration. Several mechanisms are built into the Cisco Easy VPN solution to help ensure that large numbers of sites are not taken out by device or connectivity failures.
- **Reduced cost of ownership:** Combining security and VPN on a single device—especially a mandatory branch router—results in initial cost savings as well as investment protection in the form of the scalability and modularity of the routers as business needs expand. And with only one management solution to learn,

training needs are minimized and ongoing operations are simplified. Cisco IOS Software-based routers deliver the best all-in-one, scalable solution for multiprotocol routing, perimeter security, intrusion detection, and advanced VPN, along with industry-leading device management and manageability.

Network Integration

Table 1 lists the major network integration features and benefits of the Cisco Easy VPN solution.

Table 1. Network Integration Features and Benefits

Feature	Description and Benefit
New Enhanced Easy VPN Virtual Tunnel Interface (VTI) Integration	• The Enhanced Easy VPN architecture features new virtual interfaces that can be configured directly with IP Security (IPsec) without needing to encapsulate IPsec inside protocols such as generic routing encapsulation (GRE). Network integration benefits include: • Per-user attributes such as quality of service (QoS)—VTI allows painless configuration of policies on a per-user basis; enabling administrators to be proactive in delivering the desired application performance and keeping users productive and motivated • Tunnel-specific features—VTI allows each branch VPN tunnel to be configured with its own set of parameters, providing flexibility to customize configuration and security based on site-specific needs
Virtual Route Forwarding (VRF) Integration	VRF integration with VTI allows multiple VRF instances to be terminated in multiple interfaces, facilitating large-scale service provider and enterprise Multiprotocol Label Switching (MPLS) deployments.
TCP-Based Firewall Traversal	IPsec TCP packets can be tunneled through third-party firewall devices, enabling a secure connection where standard Encapsulating Security Payload (ESP) or User Datagram Protocol (UDP) port 500 is not accepted or permitted.
Network Address Translation (NAT) Integration	NAT integration addresses and resolves known incompatibilities between IPsec and NAT by supporting NAT transparency under UDP port 500 (RFC 3947)
SafeNet Client	SafeNet clients bind to a client configuration group by using a specific Internet Security Association and Key Management Protocol (ISAKMP) local address. Different customers can use the same peer identities and ISAKMP keys by using different local termination addresses.

Some of the major ease-of-use capabilities in Cisco Easy VPN include:

- **Dynamic policy updates:** Allows network operators or service providers to change equipment and network configurations as needed, without touching end-user devices. Easy VPN Servers push down the latest security policies as and when required, minimizing manual configuration and operator errors, thereby reducing additional service calls.
- **Enhanced Easy VPN architecture (VTI integration):** Greatly simplifies configuration requirements at the headend as well as the remote branches. IP services can be configured using virtual-template interfaces (or downloaded from authentication, authorization, and accounting [AAA] servers), and at connection time, VTI instances are cloned dynamically from these templates. There is no need to manually create similar sets of configuration commands for each remote site. Enhanced Easy VPN does not support routing protocols; however, it works well with Reverse Route Injection (RRI) for distributing the reachability information for various subnets.
- **Hardware VPN client:** Allows the VPN router or security appliance to act as a VPN client, processing encryption on behalf of PC users on the LAN. This eliminates the need for end users to purchase and configure external VPN devices.
- **Cisco Easy VPN and Cisco Unity® framework:** Reduces interoperability problems between the different PC-based software VPN clients, external hardware-based VPN solutions, and other VPN applications.

The dynamic (i.e., on-demand and automated) nature of Cisco Easy VPN's policy push feature is central to significantly simplifying VPN rollouts to small office, teleworker, and remote/branch-office environments. Table 2 below lists the major policy push features and benefits.

Table 2. Centralized Policy Push Features and Benefits

Feature	Description and Benefit
Browser Proxy Configuration	This feature allows the Easy VPN server to automatically push the proxy server to the remote device without manual intervention. Original proxy settings on remote are also automatically reverted upon disconnection.
Include-Local-LAN	LAN connectivity can be retained in a non-split-tunnel connection. This allows local resources such as printers and servers to remain reachable when a secure connection is established.
Login Banner (for Hardware Clients)	Easy VPN Server pushes a banner to the remote device, where the banner can be used during Extended Authentication (Xauth) and Web-based activation. Personalized messages can be displayed on the remote device the first time the Easy VPN tunnel is brought up.
Auto Upgrade (for Software Clients)	Easy VPN Server can be configured to provide an automated mechanism for software upgrades to Easy VPN clients.
Auto Configuration Update	Easy VPN Server can be configured to provide an automated mechanism for software and firmware upgrades on an Easy VPN remote client. Any configuration change can be pushed to any number of clients, without needing to touch them.
Central Policy Push for Integrated Client Firewall	This feature allows Cisco IOS Software-based Easy VPN Servers to configure personal firewalls on client machines, allowing for improved security against split tunneling. EasyVPN Servers can choose not to allow clients that do not have the latest firewall configuration policies to join the VPN.
DHCP Client Proxy and Distributed DNS	The Easy VPN Server acts as a proxy DHCP client, acquires an IP address from the DHCP server, and pushes the IP address to the client. With this feature, the Cisco Easy VPN Server is able to assign an IP address to a client from the corporate DHCP server, making IP address allocation management centralized.
Split Tunneling	Split tunneling allows Internet-destined traffic to be sent unencrypted directly to the Internet. Without this feature, all traffic is sent to the headend device and then routed to destination resources (eliminating the corporate network from the path for Web access). Split tunneling provides a more efficient use of corporate IT resources, freeing bandwidth for those who access mission-critical data and applications from remote locations.
Split DNS Support	Split-DNS enables the 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.

Authentication

Table 3 lists the major authentication features and benefits of the Cisco Easy VPN solution.

Table 3. Authentication Features and Benefits

Feature	Description and Benefit
AAA Services	Acts as a RADIUS client, performs user authentication through RADIUS, performing local authentication and authorization, and supporting accounting session information.
Digital Certificates	Supports digital certificates for authentication of tunnel endpoints.
Encrypted Secrets	Improves encryption scheme to obfuscate passwords in Cisco IOS Software by using a stronger cipher.
Tunnel Activate on Interesting Traffic (ACL Trigger)	Secure tunnels can be built based on interesting traffic defined in an access control list (ACL). The ability to control, on a granular level, which traffic is encrypted reduces potential bandwidth waste.
Web Intercept for Xauth	Provides an HTTP interface for entering Xauth credentials to the Cisco IOS Software-based hardware client. This eliminates the need use the CLI to log in, and allows users to authenticate the entire device rather than just a single port.
Xauth Bypass	Provides the option to bypass the tunnel, allowing unencrypted Internet access for household members.
Password Expiry Using AAA	VPN client users can enter new passwords once old passwords expire.

Scalability and High Availability

Table 4 lists the major high-availability and scalability features and benefits of the Cisco Easy VPN solution.

Table 4. Scalability and High-Availability Features and Benefits

Feature	Description and Benefit
Reverse Route Injection (RRI)	For VPNs requiring either high availability or load balancing, RRI simplifies network designs. RRI creates routes for each remote network or host on the headend device to allow for dynamic route propagation.
Dead Peer Detection (DPD) and Keepalives	DPD is ideal for environments in which customers want failover between concentrators on different subnets. The router queries its IKE peer at regular intervals, allowing earlier detection of dead peers.
Hot Standby Router Protocol (HSRP)	HSRP provides high network availability by routing IP traffic from hosts on Ethernet networks without relying on the availability of any single router. When used together, RRI and HSRP provide a more reliable network design for VPNs and reduce complexity in configuring remote peers.

Feature	Description and Benefit
IPsec Stateful Failover	Stateful failover enables a router to continue processing and forwarding IPsec packets after a planned or unplanned outage occurs.
Invalid Security Parameter Index (SPI) Recovery	Receipt of an invalid SPI message automatically triggers the receiver to initiate a new key exchange. For IKE peers that do not support keepalives or DPD, invalid SPI recovery helps resynchronize peers after failover.
Multiple Backup Peers	This feature enables support for multiple peer configurations locally on the router.
Primary Peer Reactivation	If the primary VPN tunnel connection is lost, the Easy VPN client will continue to reattempt a connection with the primary peer after failover occurs. Once the primary peer becomes available, the connection is reestablished and the connection to the backup dropped.
Remote Dual Tunnels	This feature allows you to configure multiple Easy VPN tunnels that share common inside and outside interfaces to connect two peers to two different VPN servers simultaneously.
IPsec Single Security Association	This feature sets up a single IPsec tunnel, regardless of the number of multiple subnets that are supported and the size of the split-include list. The resource usage on the VPN routers is reduced, enhancing their ability to scale.
Server Load Balancing	Cisco IOS Software chooses a server based on a configured load-balancing algorithm. If one of the servers fails, all incoming requests are dynamically rerouted to the remaining servers.

Reduced Total Cost of Ownership

The Cisco Easy VPN solution helps businesses reduce their total cost of ownership in several ways:

- Reduced capital expenditure: An integrated Cisco IOS Software-based solution reduces the initial procurement costs when compared with deploying separate appliances. VPN client software is included with the solution, providing support for remote-access users without requiring additional feature licenses.
- Reduced training costs: Cisco Easy VPN features can be configured with the standard Cisco IOS CLI, allowing network operators to set up and troubleshoot the solution easily and intuitively without extensive training; there is no need to learn new hardware and software.
- Lower operations costs: Large deployments benefit from centralized policy push capabilities that minimize human intervention during ongoing changes to remote hardware and software. For smaller deployments, Cisco Easy VPN can be configured with the included device management application, Cisco Router and Security Device Manager (SDM). Easy-to-use Cisco SDM wizards allow configuration of routing, QoS, VPN, and security features (e.g., Cisco TAC-approved default firewall policies), as well as real-time monitoring of firewall logs.
- Lower support and maintenance costs: A single integrated device means a single support contract, further reducing the ongoing costs associated with multiple devices. In addition, managing a single vendor is much simpler than managing multiple relationships.

Table 5 lists the number of Cisco Easy VPN tunnels supported based on Cisco platform.

Table 5. Number of Tunnels Supported per Platform

Platform	Maximum Number of Easy VPN Tunnels
Cisco 800 Series Integrated Services Routers	10
Cisco 1800 (ALL 18xx except 1841)Integrated Services Routers	50
Cisco 1841 Integrated Services Routers with Advanced Integration Module 1 (AIM-VPN/SSL-1)	800
Cisco 1941 Integrated Services Routers with On-board crypto module	800
Cisco 2800 Series Integrated Services Routers with AIM-VPN/SSL-2	1500
Cisco 2900 Series Integrated Services Routers with On-board crypto	1500
Cisco 3825 Integrated Services Routers with AIM-SSL-3	2000
Cisco 3925 Integrated Services Routers with SPE-100	2000
Cisco 3845 Integrated Services Routers with AIM-SSL-3	2500
Cisco 3945 Integrated Services Routers with SPE-150	2500
Cisco ASR 1000 Series Router	2,000

Platform	Maximum Number of Easy VPN Tunnels
Cisco 7200 Series Routers with VPN Acceleration Module 2+ (VAM2+)	5000
Cisco 7201/7301 Routers with VAM2+	5000
Cisco 7200VXR Routers with VPN Services Adapter (VSA)	5000
Cisco 7600 Series Routers with IPsec VPN Shared Port Adapter (SPA)	8,000
Cisco Catalyst 6500 Series Switches with IPsec VPN SPA or VSPA	8,000

System Requirements

Table 6 lists the system requirements for Cisco Easy VPN software on Cisco routers and switches running Cisco IOS Software.

Table 6. System Requirements

Feature	Description
Hardware	• Easy VPN Remote: • Cisco 800, 1800, 1900, 2800 and 2900 Series Integrated Service Routers • Cisco ASA 5505 Series Adaptive Security Appliances • Easy VPN Server: • Cisco 1800, 1900, 2800, 2900, 3800 and 3900 Series Integrated Service Routers • Cisco ASA 5500 Series Adaptive Security Appliances • Cisco 7200 Series Routers, Cisco 7301 Routers, and Cisco Catalyst 6500 Series Switches • Cisco ASR 1000 Series Routers
Software Compatibility	• Cisco IOS Software Release 12.4T

Ordering Information

All Cisco router security bundles include support for Cisco Easy VPN. For a list of router security bundles, visit http://www.cisco.com/go/securitybundles.

To place an order, visit the Cisco Ordering Home Page. To download software, visit the Cisco Software Center http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml.

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

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 C78-457320-01 10/09