

Cisco Easy VPN

Application Overview

When deploying VPNs for teleworkers and small branch offices, ease of deployment is critical when technical resources are not available for VPN configuration on remote site routers. It is now easier than ever to deploy VPNs as part of small/medium-business or large-enterprise networks with Cisco products. The Cisco Easy VPN Remote feature and the Cisco Easy VPN Server feature offer flexibility, scalability, and ease of use for site-to-site and remote-access VPNs.

The Cisco Easy VPN Remote feature allows Cisco routers running Cisco IOS Release 12.2(4)YA (or later releases), Cisco PIX firewalls, and Cisco hardware clients to act as remote VPN clients. The Cisco Easy VPN Remote feature is now available on Cisco800, uBR900, and 1700 series routers, as well as Cisco PIX 501 firewalls and the Cisco VPN 3002 hardware client. As such, these devices can receive predefined security policies and configuration parameters from the headquarters' VPN head-end, thus minimizing the VPN configuration required at the remote location. Parameters such as internal IP addresses, internal subnet masks, DHCP server addresses, WINS server addresses, and split-tunneling flags are all pushed to the remote device. This cost effective solution is ideal for remote offices with little IT support, or large CPE deployments where it is impractical to individually configure multiple remote devices. The Cisco Easy VPN Remote

feature simplifies VPN configuration and can help companies reduce costs as the need for local IT support is minimized. The Cisco Easy VPN Remote feature is now available on Cisco 800, Cisco 1700, and Cisco uBR900 series routers, as well as Cisco PIX 501 firewalls and the Cisco VPN 3002 hardware client.

The Cisco Easy VPN Server feature, available in Cisco IOS Release 12.2(8)T or later releases, increases compatibility of Cisco VPN products, and allows Cisco VPN concentrators, Cisco PIX firewalls, or Cisco routers to act as VPN head-end devices in site-to-site or remote-access VPNs. Using this feature, security policies defined at the head-end can be pushed to the remote office devices running the Cisco Easy VPN Remote feature. In addition, an Easy-VPN-Server-enabled device can terminate VPN tunnels initiated by mobile and remote workers running Cisco VPN client software on PCs. This flexibility makes it possible for mobile and remote workers, such as sales people on the road or teleworkers, to access their small business, branch office, or headquarters intranet where critical data and applications exist. The Cisco Easy VPN Server feature is available on numerous Cisco IOS routers including Cisco uBR900, 1700, 2600, 3600, 7100 and 7200 series routers running Cisco IOS Release 12.2(8)T, or later releases, Cisco VPN 3000 series VPN concentrators, and Cisco PIX firewalls.



Small/Medium Business Deployment

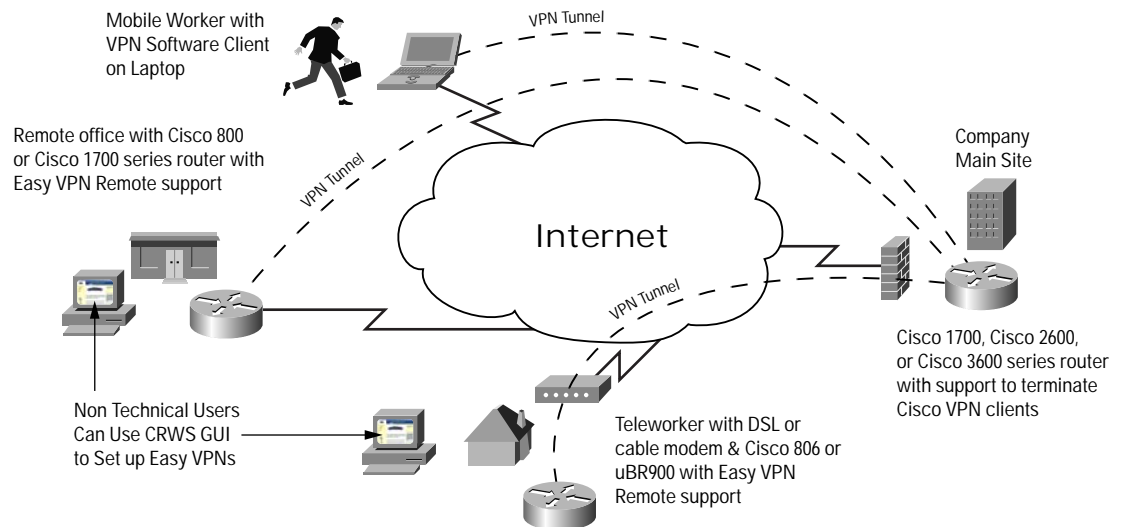
A small/medium business using a Cisco Easy-VPN-Server-enabled Cisco router or Cisco security appliance at the main site, or head-end, can securely connect small branch offices, teleworkers, and mobile workers. The head-end router must have security policies configured, determining which VPN parameters, such as encryption algorithms and authentication algorithms, will be used to communicate with remote devices.

When the head-end security policies have been defined, Cisco devices running the Cisco Easy VPN Remote feature can be deployed to small branch offices. During VPN initialization the head-end router is prompted to push the security policies to the small branch office devices, eliminating the need for remote users to do ongoing configuration updates. Once the VPNs are established, voice, video, and data can be safely exchanged over reliable secure connections, and individuals at the small branch offices no longer need to run VPN client software on their PCs.

Teleworkers using Cisco Easy-VPN-Remote-enabled Cisco routers or Cisco security appliances can also access the Cisco Easy-VPN-Server-enabled router at the head-end through secure VPN connections. As with the small branch office scenario, the head-end security policies are pushed to the remote devices with minimal configuration.

Mobile workers running VPN client software on PCs can easily establish VPN connections with the Cisco Easy-VPN-Server-enabled device through their ISP. This connectivity allows business travelers to securely access critical data and applications almost any time, from their ISP's points of presence (POPs).

Figure 1:
Small to Medium Business Deployment





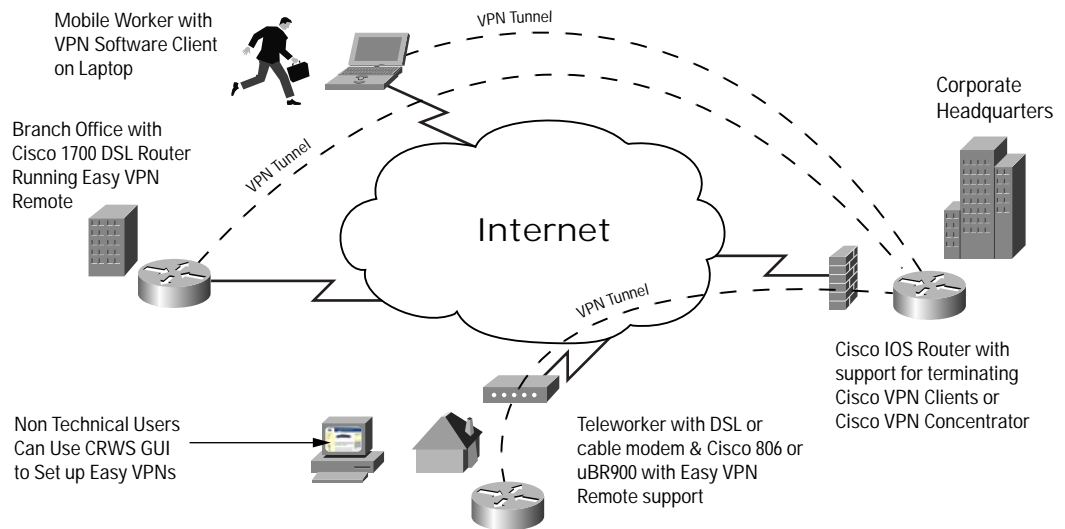
Large Enterprise Deployment

A large enterprise can connect branch offices, remote offices, and teleworkers to its network using a Cisco Easy-VPN-Server-enabled Cisco router or Cisco security appliance. The head-end router must have security policies configured, determining which VPN parameters, such as encryption algorithms and authentication algorithms, will be used to communicate with remote devices.

When the head-end security policies have been defined, branch offices can deploy Cisco Easy-VPN-Remote-enabled devices. During VPN initialization, the head-end device is prompted to push security policies to the small branch offices, eliminating the need for extensive local configuration. Voice, video, and data can be safely exchanged over reliable secure connections, and individuals at the branch offices no longer need to run VPN client software on their PCs.

Remote office workers and teleworkers using Easy-VPN-Remote-enabled devices can also access the Easy-VPN-Server-enabled enterprise head-end through secure VPN connections. As with the small branch office scenario, the head-end security policies are pushed to the remote devices with minimal configuration. Additionally, non technical users in remote sites can easily set up the VPN connections without the need for an on-site technician. The net effect is increased productivity, as remote workers spend less time configuring network devices.

Figure 2:
Enterprise Deployment





High Availability

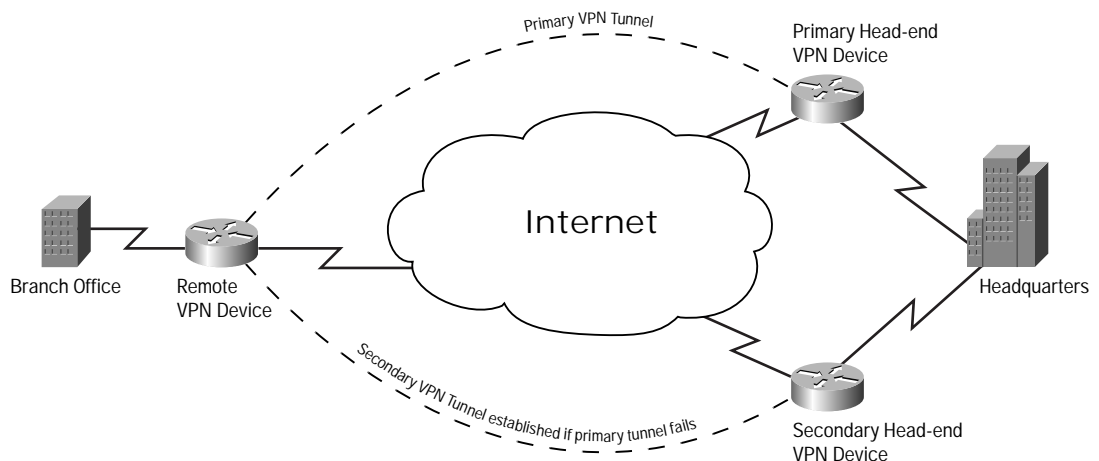
Cisco Easy VPN is compatible with Reverse Route Injection (RRI) and Hot Standby Router Protocol (HSRP) with IPsec. When used together, these two features provide a more reliable network design for VPNs and reduce configuration complexity on remote peers.

RRI is a feature designed to simplify network design for VPNs in which 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 head-end VPN router for transport across the correct SAs to avoid IPsec policy mismatches and possible packet loss.

HSRP is designed to provide high network availability by routing IP traffic from hosts on Ethernet networks without relying on the availability of any single router. IPsec can use the HSRP virtual IP address as the local IPsec identity, or local tunnel endpoint. Remote VPN gateways connect to the local VPN router via the virtual IP address that belongs to the active device in the HSRP group. In the event of failover, the standby device takes over ownership of the standby IP address and begins to service remote VPN peers.

RRI and HSRP are only relevant to the server side of the connection in a client-server VPN model, when redundant head-ended VPN devices are deployed. RRI may also be used on its own in the case where traffic destined to remote VPN devices must be routed to the VPN head-end device. If you have a single head-end gateway through which all traffic flows, then RRI and HSRP are not necessary. RRI is not recommended for use with GRE/IPsec.

Figure 3:
High availability

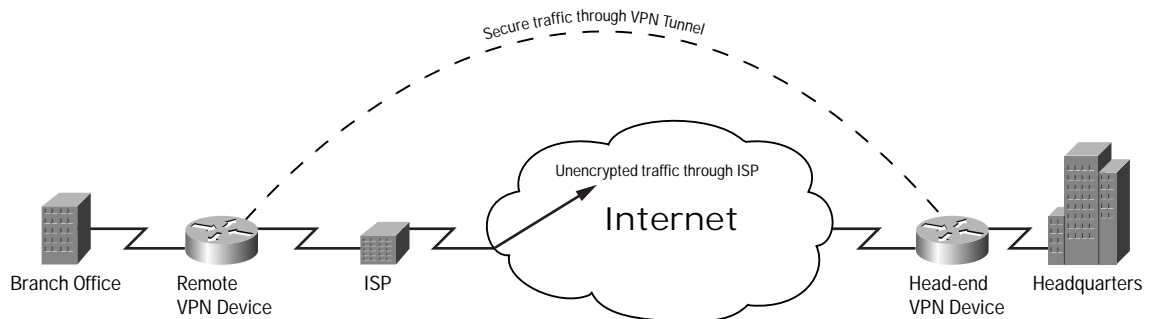




Split Tunneling

Cisco Easy VPN supports split tunneling which allows Internet destined traffic to be sent unencrypted directly to the Internet. Without split tunneling all traffic is sent to the head-end device and then routed to destination resources (eliminating the corporate network from the path for web access). This functionality provides a more efficient use of corporate IT resources, freeing bandwidth for those who access mission-critical data and applications from remote locations.

Figure 4:
Split Tunneling



Summary

The Cisco Easy VPN features provide ease-of-use, scalability and reduce the need for individual PC-based client applications. Branch office workers can now share connectivity through a Cisco Easy-VPN-Remote-enabled Cisco router or Cisco security appliance, making use of a single VPN tunnel from the remote site, allowing the head-end device to connect more users with fewer tunnels. The Cisco Easy VPN Server feature provides greater flexibility when deploying head-end devices to terminate remote VPN tunnels at branch offices or small businesses. Together, the Cisco Easy VPN features expand the critical role of Cisco products in any small/medium-business or large-enterprise VPN.

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France

www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912

www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARtnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0203R)