



Cisco Virtual Private Network (VPN) solutions

A Virtual Private Network, or VPN, is a network that is deployed on a shared infrastructure instead of a dedicated, private infrastructure. A VPN provides the performance, functionality and benefits of a traditional Wide Area Network (WAN) such as leased lines, but does so at a lower cost and with greater flexibility. It is these characteristics that make VPN a compelling solution for small or medium businesses. A VPN can utilise the most widely used transport technologies, such as the public Internet, service provider IP backbones, or service provider Frame Relay and ATM networks. However, the functionality of the VPN is defined primarily by the equipment deployed at the edge of the network and the integration of features across the WAN, not by the WAN transport protocol itself. Cisco Systems® VPN solutions combine high levels of integration, flexibility and scalability with ease of deployment, straightforward management and rapid return on investment.

Definitions

Remote access VPN – connects remote workers such as telecommuters, mobile users, or branch offices to the business LAN and corporate computing resources over a secured connection.

Intranet VPN – Enterprise network extension to connect remote workers, mobile users, or branch offices to the business LAN and corporate computing resources within an enterprise WAN over a secured connection.

Extranet VPN – extends the limited access of enterprise computing resources to business partners, such as suppliers or customers, enabling access to shared information.

Tunnels – encrypted “channels” established to provide logical, point-to-point connections across a connectionless IP network, enabling the deployment of advanced security features. Encryption is applied to the tunneled connection to scramble data, thus making data legible only to authorised senders and receivers.

How to identify a sales opportunity

Any growing business with more than one site, or with people working remotely, can gain substantial benefits from a VPN deployment. The following questions will help you to establish how a VPN can address the needs and opportunities facing your customers.

- 1 Does the business already operate some form of Wide Area Network? This may be anything from an infrastructure running on a dedicated service provider leased line, to a facility for remote workers or branch office staff to dial-in over a telephone line to access resources on the main business network. The lower cost, higher security and greater flexibility of a VPN solution will benefit any organisation operating any form of WAN.
- 2 If there is no specific WAN infrastructure, does the customer still have staff working remotely? Even communication by e-mail using a dial-up line is a form of Wide Area Networking. Customers who have staff on the road, or working from home, will achieve significantly enhanced productivity through a VPN deployment, by giving them faster, secure access to the resources and data they need to work effectively.
- 3 Does the business have branch offices, or multiple operational sites? VPN solutions deliver major benefits to businesses operating more than one site. The customer may well have considered deploying a WAN to try to reduce communication costs between sites, but been put off by the high cost of deployment and maintenance. For an SMB, a VPN delivers all the benefits of a WAN at a much lower cost. As well as generally speeding up and improving communication between sites, a Cisco VPN solution can enable the deployment of voice services over the network infrastructure, helping to cut telephone charges dramatically.



VPN Solution elements

A Cisco VPN solution can employ IP Security, Point-to-Point Tunneling Protocol, Layer 2 Tunneling Protocol, Layer 2 Forwarding, and generic routing encapsulation for tunnel support, as well as the strongest standard encryption technologies: Data Encryption Standard, Triple DES, and Advanced Encryption Standard.

Security acronyms

- IP Security (IPSec),
- Point-to-Point Tunneling Protocol (PPTP),
- Layer 2 Tunneling Protocol (L2TP),
- Layer 2 Forwarding (L2F),
- Generic Routing Encapsulation (GRE)
- Data Encryption Standard (DES),
- Triple DES (3DES)
- Advanced Encryption Standard (AES).

- 4 Is the customer concerned about network security? VPN is actually a solution driven by security technologies (see Definitions for the principal technologies and their acronyms). Very high levels of encryption are used to secure the tunnels across the shared network; it is likely that a Cisco VPN will provide a higher level of security than any other area of the customer's network, unless the whole infrastructure is also based on Cisco solutions.
- 5 Is the customer concerned about return on investment? In comparison with a private WAN, the total cost of ownership for a VPN is reduced through the lower costs of transport bandwidth, backbone equipment and network operations. Infonetics, a networking management consulting firm, quotes reductions in cost of 20 to 40 percent for LAN-to-LAN connectivity, with cost reductions for remote access of between 60 to 80 percent. On this basis, return on investment can be quoted in months, not years.
- 6 Is the customer network managed in-house? There are significant overheads associated with owning and operating a private infrastructure. With a VPN, your customer can outsource some or all of their WAN functions to a service provider, enabling them to focus on core business objectives.

Key Features and Benefits of Cisco VPN Solutions

Cisco VPN solutions encompass all segments of the networking infrastructure: platforms, security, network services, network appliances, and management. They provide the broadest set of VPN service offerings across many different network architectures.

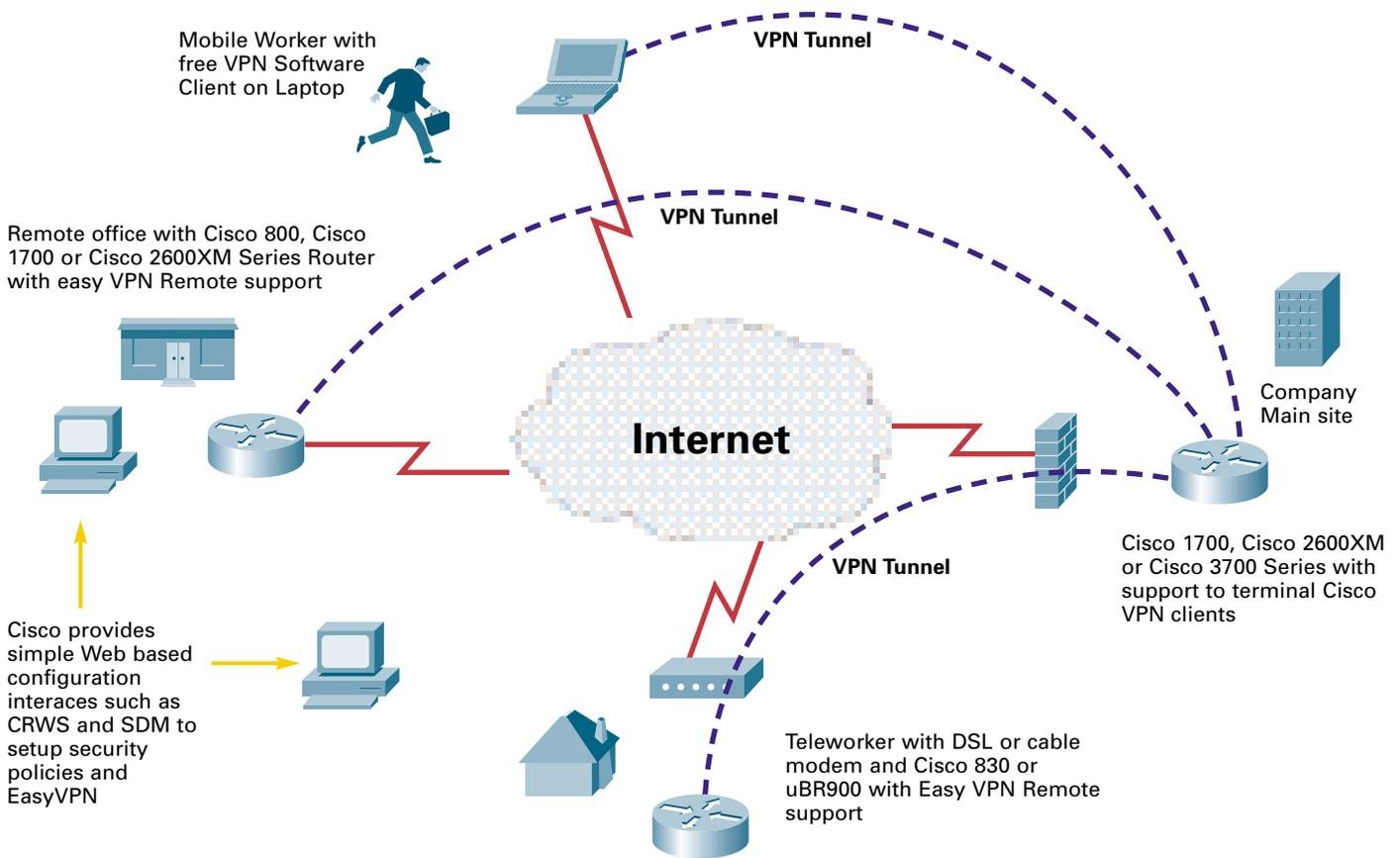
- Lower costs, improved communication – branch offices, remote workers and staff on the road can all have faster, easier access to network resources, at substantially lower costs than a conventional private network.
- Enhanced productivity – advanced Cisco solutions, such as IP telephony using Cisco AVVID (Architecture for Voice, Video and Integrated Data) and content networking technologies are fully compatible with Cisco VPN platforms. Growing businesses can take full advantage of emerging technologies to boost productivity and competitiveness.
- Investment protection - Cisco VPN solutions enable corporations to deploy VPNs on their existing Cisco networking gear. The entire line of Cisco router and firewall platforms is easily VPN-enabled through Cisco IOS® or Cisco PIX® Firewall software enhancements, providing a smooth migration path to a VPN environment.
- Ease of deployment - Cisco is uniquely positioned as the guide to the new world of VPNs. Cisco VPN solutions smoothly integrate the many facets of VPNs with existing Cisco products, such as routers, WAN switches, access servers, and firewalls.

How does Cisco provide VPN?

All Cisco Access Routers and Cisco PIX security appliances support secure VPN connections. VPN software for client computers/mobile workers is available free of charge. VPN services are set up easily using the Easy VPN admin tool.

What could the network look like?

The following diagram illustrates a typical SMB deployment of a 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 International BV
 Haarlerbergpark
 Haarlerbergweg 13-19
 1101 CH Amsterdam
 The Netherlands
 www-europe.cisco.com
 Tel: 31 0 20 357 1000
 Fax: 31 0 20 357 1100

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 6317 7777
 Fax: +65 6317 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.com Web site at www.cisco.com/go/offices.**

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Aironet, Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems Verified logo, EtherChannel, and GigaStack are registered trademarks or 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. (0206R)