VPN

Solution Overview – Virtual Private Networks

Headline/Title: Cisco VPNs Help Your Business Stay Connected with Mobile Employees, Customers and Partners.

Subtitle: VPNs enable small and medium-sized businesses to increase productivity by providing secure access to corporate information wherever there is an Internet connection and browser.

Web Abstract

Business productivity, profitability and competitive position depend on an ability to share data in a timely, secure manner. Site-to-site and remote access VPNs can make secure network access a reality for branch office and mobile workers. This VPN solution overview describes how:

- Providing secure, easy, cost-effective access to data is essential to maintaining a competitive edge
- Cisco VPNs effectively integrate hardware and software technologies, providing secure remote access for employees, customers, and partners
- A secure, efficient VPN helps boost productivity and enhance customer satisfaction
- VPNs increase profitability by reducing network operating costs

Article Contents/Section Headings
Challenge
Solution
Benefits
What Cisco Offers

Article Body:

Challenge:

Your organization's productivity, profitability, and competitive position depend on the ability to share data securely, cost-effectively, and immediately. Data sharing solutions must be flexible enough to support changing business needs, including the requirements of branch office workers, business partners and the rapidly growing number of mobile workers. In recent years, more and more businesses have been using virtual private networks (VPNs) to provide secure connectivity to protect sensitive data. But VPNs that rely on leased lines can be costly, especially if the data must be transmitted a great distance or there are many locations to connect. What's more, these site-to-site VPNs are not flexible enough for the requirements of mobile workers who frequently need to connect to the corporate network from a hotel room, airport, or other location far from a corporate office.

The growth of the Internet has spurred the development of new VPN technologies that offer small and medium-sized businesses new opportunities to securely connect more people at a lower cost. VPNs are no longer confined to site-to-site connections, and authorized users can now get secure remote network

access instantly from anywhere there is a browser and Internet connection. This new breed of VPN lets businesses engage customers and partners in new ways to boost profitability.

If your organization is considering a VPN, you have a wealth of software and hardware products and technologies to choose from. Facing so many choices, you must evaluate the various VPN solutions and select the solution that provides the right performance and encryption capabilities to meet your needs and fit your budget. The solution must also have the flexibility to evolve with changing business requirements, and be easy to deploy and manage.

Solution

Cisco offers three different approaches to implementing a VPN solution for your small or medium-sized business. With Cisco solutions you can implement both remote access and site-to-site VPNs with Cisco IOS® software, through software and Advanced Integrated Module (AIM) hardware encryption cards, or with hardware appliances, such as a VPN concentrator, router, Cisco PIX® Firewall, or dedicated VPN server for dial-up services.

- Every Cisco router that employs Cisco IOS® software supports IPSec (Internet Protocol Security) VPNs. IPSec functionality provides network data encryption at the IP packet level, offering a robust security solution that is standards-based. IPSec is the only way to implement secure VPNs. It supports remote access, intranet, and extranet VPN requirements.
- Incorporating all the standards-based encryption and authentication technologies, Cisco VPN Concentrators are built specifically for creating the remote access or site-to-site VPNs that small and medium-sized businesses need today. Cisco VPN hardware also includes VPN-enabled routers and VPN-optimized routers. VPN-enabled routers are designed for VPNs with moderate encryption and tunneling requirements. VPN-optimized routers, based on Cisco IOS® software, offer scalability, routing, security and Quality of Service (QoS). They are ideal for high encryption and tunneling requirements and often use additional hardware, such as encryption cards, to achieve high performance.
- The versatile Cisco PIX Firewall, another key component of Cisco's VPN solution, combines dynamic address translation, proxy server, packet filtration, and VPN capabilities in a single device. It also provides robust, integrated network security including Intrusion Detection (IDS). As with Cisco routers, PIX Firewalls support a variety of VPN standards such as PPTP, L2TP and IPSec VPN, as well as a number of encryption standards including AES.
- Cisco's modular VPN solutions offer exceptional flexibility. This flexibility extends to the remote access edge, where remote users have a number of options to choose from. The Cisco solution eliminates the requirement for a VPN client application, except for an Internet browser, with access delivered through Web-based applications. Depending on your business requirements, additional functionality may be easily provided with a host software client, including a built-in firewall. Further functionality and performance may be incorporated with a hardware client for "nailed-up" VPN services.
- Cisco's Secure Socket Layer (SSL) VPN functionality enables a user to connect with the Internet and corporate data with a browser, rather than a client. Since almost all Web browsers support SSL, any authorized user with a Web browser and Internet connection can access the data via the Cisco Web VPN.

Benefits

Cisco VPN solutions provide the vital link that helps ensure your employees, customers and suppliers have easy, secure access to data.

A Cisco VPN:

- Extends geographic connectivity, keeping employees connected to corporate data whether they are in a branch office or on the road. It enables mobile employees to be productive an additional 1-2 hours a day. They don't even need their own computer—they can simply go to an Internet café to make their connections, enjoying the same level of access, encryption, and security as they would have at your main office.
- Simplifies and enhances communication with partners and customers. It allows partners to collaborate and interact more easily, to update orders and check inventories, and enables customers to check order status. It also allows you to connect with customers and partners in new ways.
- Sends your business data fast, completely encrypted and secure. You can use a Cisco VPN for communications between networked fax machines or file servers.
- Includes essential security features. It ensures the data has not been changed while in transit, verifies the identity of the source of the data, and employs tunneling to hide the identity of the device originating the traffic.
- Is easy to use. There's no need to download software or install it on a PC.
- Is cost-effective and saves money. By connecting branch offices that have a basic broadband DSL or cable connection, a Cisco VPN makes it unnecessary to have a costly Frame Relay, T1, or other type of dedicated WAN link. A Cisco VPN provides a faster ROI than a traditional WAN. It also eliminates dialup charges. If an employee is at a hotel with Internet access, or has broadband at home, no additional cost is involved.

What Cisco Offers

Cisco offers a combination of technology, breadth of product line, and partners that no other vendor can match. With technologies such as Web VPN, exceptional modularity and integration of its extensive VPN offerings, and a family of partners to assist you with product selection and support, Cisco is the right choice for VPNs.

Cisco VPN solution offerings include:

- Cisco VPN 3000 Series Concentrators
- VPN-enabled Cisco routers, including the 800, 1700, 2600, and 3700 Series
- Cisco IOS software
- Hardware modules, including AIM cards
- Cisco hardware and software VPN clients
- Cisco Web VPN