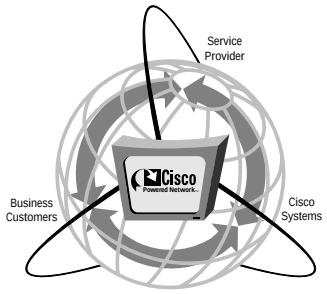
Access VPNs for the Enterprise



WHETHER YOU BUILD YOUR OWN OR OUTSOURCE TO A SERVICE PROVIDER, IP-BASED VIRTUAL PRIVATE NETWORKS (VPNS) OFFER A SECURE, RELIABLE, AND COST-EFFECTIVE REMOTE-ACCESS SOLUTION THAT CAN EASILY SCALE TO MEET CHANGING BUSINESS NEEDS.

Executive Summary

The strain on today's corporate networks is greater than ever before. Network managers must continually find ways to connect geographically dispersed work groups in an efficient, cost-effective manner. Increasing demands from feature-rich applications used by a widely dispersed workforce are causing businesses of all sizes to rethink their networking strategies. As companies expand their networks to link up with partners, and as the number of telecommuters and remote users continues to grow, building a distributed enterprise becomes ever more challenging.

To meet this challenge, VPNs have emerged, enabling organizations to outsource network resources on a shared infrastructure. Access VPNs in particular appeal to a highly mobile work force, enabling users to connect to the corporate network whenever, wherever, or however they require.

Partnering with a service provider to construct an Access VPN can offer businesses a secure, private, and reliable means of communication and they reduce the total cost of ownership. The service provider becomes the enterprise's expert on interbusiness and intrabusiness communications needs, allowing the company to focus on its primary business goals and core competencies.

In deciding to partner with a service provider to buy a VPN service, enterprises should focus on services that carry the Cisco Powered Network label. The Cisco Powered Network moniker ensures that customers will obtain an Access VPN solution based on trusted network policies and optimum compatibility with existing standards. In addition, businesses can protect their initial investment in existing Cisco infrastructure by simply upgrading their Cisco IOS® software and making those ports VPN ready. Cisco Powered Network VPNs are the most secure, reliable, and flexible solutions available today.

Introduction—What is a VPN?

VPNs offer enterprise-scale connectivity deployed on a shared infrastructure with the same policies enjoyed in a private network. These policies include security, prioritization, reliability, and end-to-end management. A VPN can be deployed over the Internet or built on a service provider's existing IP, Frame Relay, or ATM infrastructure.

VPNs based on IP can naturally extend the ubiquitous nature of intranets—over wide-area links, to remote offices, to mobile users, or to telecommuters. Further, they can extend extranets to communities of interest outside the

organization linking business partners, customers, and suppliers, to provide better customer satisfaction, market differentiation, and reduced manufacturing costs.

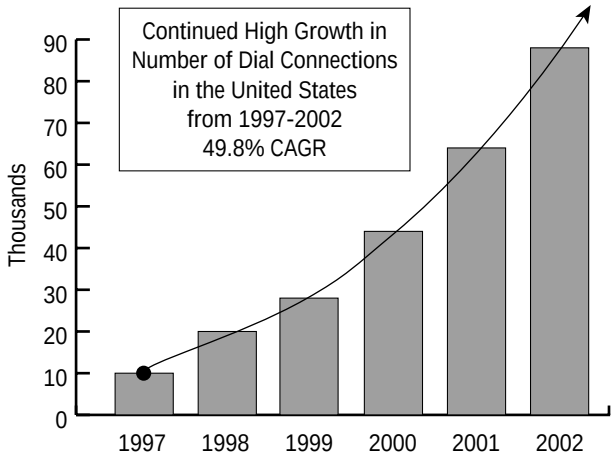
The three basic types of VPNs are Access VPNs, Intranet VPNs, and Extranet VPNs. Access VPNs appeal to a highly mobile work force, handling remote-access connectivity for mobile users, telecommuters, and small offices through a broad range of technologies.

Enterprise Business Dynamics

The business case for VPNs is irresistible. Forrester Research reports that 55 percent of enterprise companies surveyed plan to establish VPNs as extensions to their current networks. The reasons given by both small and large businesses alike are the same: price/performance advantages and the flexibility afforded by an IP-based offering.

Market trends all point to a growing demand for Access VPNs. According to a March 1998 report from International Data Corporation, the number of dial connections is expected to climb from 20,000 in 1998 to 85,000 in 2002 (see Figure 1). Strong growth is also predicted in the wireless and DSL access market segments.

Figure 1 Growth in Dial Connections



IDC, March 1998

The reasons for this rapid growth include the phenomenal success of the Internet and a steadily increasing number of telecommuters. As telecommuters, mobile users, and satellite offices all vie for dependable access to company intranets, businesses of all sizes are beginning to perceive the advantages of an Access VPN solution.

Service Provider as Business Partner

New networked applications such as videoconferencing, distance learning, and information-rich publishing applications offer businesses the promise of improved productivity and reduced costs. As these networked business applications become more sophisticated, companies need more than a basic transport service from their service providers. They need security controls to maintain the integrity of their own networks. In addition, these emerging services will require application resource controls and management controls to optimize business applications and information flows.

Why buy an Access VPN from a service provider when companies have been building their own private networks with leased lines for years? One of the most compelling advantages is to reduce the total cost of ownership. The cost of building a private corporate Intranet includes the cost for capital equipment, bandwidth, staffing, and operations. These costs are magnified when companies seek to upgrade their network to enjoy advancements in new technology. Rather than fund this endeavor in-house, business customers can seek the network resources of their service providers, resulting in lower network and operational costs.

Another issue is expertise, an increasingly scarce resource in today's competitive market. Outsourcing VPN Access alleviates the challenge of keeping in-house staff trained on the latest network technologies. This factor is especially relevant for small and medium-sized businesses. With frequent advancements in new technologies, product life cycles become shorter, thus requiring further investment in capital and operations.

Another important benefit is improved connectivity. By purchasing an Access VPN, companies can enjoy broader reach and higher levels of connectivity through a carrier-grade service offering. Businesses are connected worldwide through the enormous span of the service provider's IP, Frame Relay, or ATM infrastructure, often in conjunction with the Internet. This makes access to a corporate network from a home office or small branch office no farther than a local or toll-free phone number. VPNs also enable the delivery of broadband services that are capable of delivering emerging multimedia applications. Some of these will be delivered over DSL links to the home or business and some will be direct, high-speed access connections via fiber or broadband wireless access.

Access VPNs include comprehensive security policies—another valuable commodity to businesses. With an Access VPN supporting business communications, organizations can be confident that their corporate data remains private, and that their company transmissions are secure, because they will have the management tools to control their own access privileges. Finally, the ability to prioritize traffic over a VPN ensures that the necessary bandwidth is available to mission-critical applications when required. This will allow service providers to offer IP-based service level agreements (SLAs) to their business customers.

Companies that outsource their networking requirements can focus on gaining a competitive advantage through improved information flows and content, rather than putting their energy and resources towards building a private network. The efficient flow of information is what empowers businesses to become leaders in their respective industries.

Cost Savings of an Outsourced Solution

As illustrated in Table 1, an outsourced Access VPN solution for 1000 users can be 38 percent less expensive than an access solution developed in house.

Table 1 Financial Model: In-House or Outsourced Remote Access

	In House	Outsourced	Savings
Ports and Toll-Free Access	$957,000	$700,000	$257,000
Network Backbone	500,000	450,000	50,000
Staffing	440,000	0	440,000
Security	185,000	100,000	85,000
24x7 Help Desk	750,000	500,000	200,000
Network Management	75,000	0	75,000
Total	$2,907,000	$1,800,000	$1,107,000
	Savings Based on Outsourced Solution = 38%		

The remote access solution could encompass local dialup access, local dedicated access, and toll-free (800/888) dialup access. Mobile access is another alternative to allow remote users to connect to their corporate network when a phone line or other direct connection is not available.

These figures serve as a consistent guideline of the cost savings that will result from buying a VPN from a service provider, rather than building a VPN from scratch. Buying an Access VPN rather than building a remote-access network saves a company costs in the following ways:

- Eliminates the buying, installing, and configuring of remote-access servers and modems
- Minimizes or eliminates equipment costs
- Manages client software
- Oversees the installation of telephone lines
- Monitors remote-access traffic
- Minimizes dialup telephone costs
- Employs and trains highly skilled networking professionals
- Scales the required number of ports for increasing access requirements
- Minimizes line costs
- Provides a single port to headquarters with no port contention issues

Case in Point

Bankers Trust New York Corporation, a leading financial services company headquartered in New York City, is purchasing an Access VPN solution that will allow employees in more than 50 countries worldwide to dial directly into its corporate network. According to Saul Adler, the company's vice president of Network Engineering, outsourcing a portion of his remote access operation to a service provider eliminates the expense of purchasing and managing communications servers in every remote location where Bankers Trust has an office. The solution also saves money on long-distance charges, because users pay local phone rates instead of international toll charges to link to the VPN.

Adler and his staff retain in-house control over their own network security by maintaining a CiscoSecure access control server (ACS) at their central site. The CiscoSecure ACS product line includes access control servers that determine who can access the network and which services they are authorized to use. CiscoSecure ACS is used in conjunction with dialup access servers, routers, and firewalls.

"Leveraging off a service provider's infrastructure will give us the global presence we need and all the security and benefits of a private dialup solution," explains Adler. "It's a win-win for both of us."

VPN Architectures

For all three types of VPNs—Access VPNs, Intranet VPNs, and Extranet VPNs—Cisco IOS® software is the common thread that ties the system together, enabling end-to-end networking across enterprise and service provider domains with consistent policies over a shared infrastructure.

Access VPNs

Telecommuters, field sales and service representatives, branch offices, and other remote and mobile users are all prime candidates for Access VPNs. Access VPNs provide access to a corporate Intranet or Extranet over a shared infrastructure with the same policies as a private network. They cover remote-access connectivity through dial, ISDN, DSL, wireless, and cable technologies.

Access VPNs enable businesses to outsource their dial or other broadband remote access connections without compromising their security policy. They encompass two architectural options: client-initiated or Network Access Server (NAS)-initiated connections.

With client-initiated Access VPNs, users establish an encrypted IP tunnel from their clients across a service provider's shared network to their corporate network. With a client-initiated architecture, businesses manage the client software tasked with initiating the tunnel. Client-initiated VPNs ensure end-to-end security from the client to the host. This is ideal for banking applications and other sensitive business transactions over the Internet. With client-initiated VPN Access, the end user has IPSec client software installed at the remote site, which can terminate into a router-based firewall or an appliance-based PIX firewall for termination into the corporate network. The Cisco IPSec solution fully supports Internet key exchange (IKE) and certificate authority to generate the encryption, authentication, and certificate keys to be used to ensure totally secure VPN solutions.

Another architecture for Access VPNs defines tunnels initiated from the NAS. In this scenario, remote users dial into the local service provider point of presence (POP) using a local or toll-free number, and the service provider initiates a secure, encrypted tunnel to the corporate network. With NAS-initiated architecture, service providers authenticate the user entering the corporate network; however, businesses retain control of their own security policy, defining the user's authorization privileges and accounting for where the user traversed the network. This two-tier authentication ensures that the service provider authenticates who enters their NAS, and the enterprise authenticates again at the home gateway and firewall.

The key benefits of an NAS-initiated Access VPN include prioritization, load sharing, and redundancy. NAS-initiated Access VPNs relieve companies of the details involved in managing a secure network, allowing the service provider to handle many details that are not part of the company's core competencies. However, some applications may require a client-initiated Access VPN when the user wants to ensure the data is encrypted from the source computer to the host. With NAS-initiated VPNs, standard telephone or ISDN lines are used and the payload is only encrypted from the NAS to home gateway, where the threat of intrusion is more probable.

Cisco provides scalable platforms and robust Cisco IOS software for deploying either client-initiated or NAS-initiated Access VPNs over dial and broadband technologies. Companies should watch for the Cisco Powered Network mark to ensure that an Access VPN is architected with trusted network policies and optimum compatibility with existing standards. Most of the world's Internet infrastructure is powered by Cisco networking equipment.

Intranet and Extranet VPNs

Intranet and Extranet VPNs link remote offices and external communities of interest. However, the Access VPN technologies previously mentioned must have the ability to terminate telecommuters and other remote users into corporate intranets. These VPN services are typically based on dedicated access and can be deployed over several architecture choices including:

- IP tunnels based on IPSec, a proposed standard in the IETF for IP security, or based on Generic Route Encapsulation (GRE)
- Virtual circuits based on ATM or Frame Relay
- IP and ATM converged through tag switching/ Multiprotocol Label Switching (MPLS).

Intranet and Extranet VPN services based on IPSec or GRE create secure tunnels across an IP network. IPSec and GRE technologies leverage industry standards to establish secure point-to-point connections in a mesh topology that is overlaid on the service provider's IP network or the Internet.

Both also offer the option to prioritize applications. An IPSec architecture, however, leverages the IETF proposed standard for IP security and enables encrypted tunnels from the access point to and across the Intranet or Extranet. GRE is supported in Cisco IOS software and in Cisco routers, and IPSec is available in Cisco IOS software and in Cisco routers.

VPN Building Blocks

The building blocks for any business-ready VPN service are security, scalability, quality of service (QoS), manageability, and reliability, all of which are provided through the industry-leading Cisco IOS software and hardware.

Security

Security is critical for any corporate network. As such, it is the primary concern for businesses contemplating the use of a VPN. With the proper security provisions in place, information flowing over a shared infrastructure can be as secure as it is on a private network. Cisco technology includes many robust security measures to keep information confidential such as encrypting data, restricting access to authorized users, and tracking users once they are connected to the network.

VPNs are built around authentication, authorization, and accounting (AAA) capabilities. CiscoSecure ACS provides the foundation to authenticate users, determine access levels, and archive all of the necessary audit and accounting data.

A tunnel creates a logical, point-to-point connection in a connectionless IP network. An encrypted tunnel provides network, data, and addressing privacy by scrambling data so that it is understood by designated senders and receivers only.

IPSec embodies many dependable and proven encryption technologies. Encapsulating Security Protocol (ESP) and the Data Encryption Standard (DES) are employed by IPSec to protect the "payload" or data portion of the packet.

Quality of Service

QoS is an essential ingredient of a VPN since it determines the network's ability to assign network resources to mission-critical or delay-sensitive applications. Mission-critical applications, which are fundamental to business operations, include financial reporting, order processing, and shipping systems. They require precedence over bandwidth-consuming applications such as Web surfing. Delay-sensitive applications, such as distance learning or videoconferencing, require QoS to allocate enough bandwidth to avoid jitter and poor quality.

QoS addresses the two fundamental requirements for applications that run on a VPN: predictable performance and policy implementation. Policies are used to identify applications, project groups, or other organizations based on designated priorities. The increasing volume of network traffic, along with project-based requirements, results in the need for businesses to control their network bandwidth and to better align network policies with business obectives.

Cisco has a broad set of QoS capabilities that allow users to prioritize service classes, manage bandwidth, avoid congestion, and link Layer 2 and Layer 3 QoS guarantees. One of the best examples is Committed Access Rate (CAR), which allows the service provider, the user, or the application to establish traffic classes and enforce policy. Weighted random early detection (WRED) performs congestion management and ensures predictable service in the face of oversubscription. Cisco is an industry leader in merging Layer 2 and Layer 3 QoS integration, and supports the emerging Diff-serv working group.

Manageability

As enterprise companies entrust their mission-critical interbusiness and intrabusiness communications to a service provider, they need clear and intelligent management from their communications partners. A service-level agreement (SLA) that is concise and simple to understand and includes distinct accounting documentation, sets the stage for trusted VPN services and applications. Enforcing policy with the guarantee of an SLA allows service providers to differentiate their service offerings and guarantees that mission-critical data is transported without interruption.

Comprehensive management and end-to-end policy provisioning make Cisco Powered Network VPNs the most secure, reliable, and flexible VPN solutions available today. The company's infrastructure, service provisioning, and service-level management provide open, documented application programming interfaces with outstanding reliability.

Reliability

Business customers need to know that their VPNs are performing at the required levels of service to deliver business transactions. VPNs built on Cisco IOS software provide the

necessary reliability by allowing packets to transparently cut over to a different path should a link or device fail. Additionally, Cisco equipment provides full redundancy in hardware components reducing the risk of downtime due to an equipment failure.

Cisco Powered Network Services

A service offering with the Cisco Powered Network mark means confidence, leadership, and quality that enterprise companies can rely on. Cisco partners with service providers to enable them to offer network services that are business-ready with the same scalability, performance, and policies deployed in private networks around the world.

The Cisco Powered Network program helps businesses find service providers with industry-leading networking services based on Cisco equipment. Eighty-five percent of enterprise companies already depend on Cisco equipment. Companies deploying VPNs can extend this infrastructure to obtain optimal, end-to-end compatibility with their existing networking equipment.

Cisco Powered Networks are the most reliable, scalable and secure solutions on the market. They help companies gain a competitive advantage by powering network services that enable the most efficient deployment of tomorrow's enterprise business applications.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
http://www-europe.cisco.com
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
http://www.cisco.com
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

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

For more information about services solutions for service providers, visit http://www.cisco.com/spservices

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong • 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 • Singapore Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

1/99LW