Go SECURE with VPN

VPN provides a flexible, ubiquitous communication infrastructure for companies to reinvent themselves and their relationship with customers and partners thereby helping businesses to scale greater heights - quickly, easily, and cost-effectively

G P VINAYBABU

With Internet as a backbone, more network infrastructures are being developed that will aid enterprises to be globally relevant. Globalisation of enterprises has ensured that workers, that are spread across different geographical locations, co-ordinate. One of the innovative variations of the Internet is that it helps members of an organisation be in touch with core business information from diverse locations is Virtual Private Networks(VPN). This technology emerged as corporations looked for ways to overcome long-distance charges piled up by mobile workers. The simplest definition of a Virtual Private Network is a private network connected over a public network infrastructure such as the Internet. VPNs allow users to tunnel through the public network and provide the same security and features available in a private network. Encryption and authentication are used to guarantee privacy.

A VPN can be between two end systems or it can be between two or more networks. A VPN across the Internet logically functions as a Wide Area Network, or WAN. For workers who

need long-distance access, companies are using an Internet Service Provider and a VPN. Essentially, VPN consists of a central box and client software. The black box resides on the company's network; the client software on the mobile worker's computer. The scheme allows a mobile worker to dial into an ISP and use the internet to establish a secure connection to his company's computers. Since that call to an ISP is usually a local one, the set-up allows the company to side-step long-distance phone call charges. When the mobile worker contacts the central box at the home office, the device verifies the identity of the person accessing the system, or at least it verifies the person accessing the system has a valid identity. And it creates a virtual tunnel to the worker's computer. All information that passes back and forth in the tunnel is encrypted and if intercepted by a hacker midway no data is lost.

Sending encrypted information on the Net is nothing new. Secure servers, for example, take and confirm orders for goods and services that way. But in a corporate environment, for mobile workers to have access to information on an organisation's internal network, access to information that sits behind the protection of a firewall is necessary. That is provided by the sophistication of a VPN. The VPN software at the mobile user's end of the connection makes his PC appear as if it is connected to the company's internal network. In addition to safeguarding data transfer through encryption and network access through certificates of authentication, the VPN contains additional security to make sure its box isn't used to compromise the company's firewall.

The best thing about VPN technology is its non-allegiance to any service provider. It doesn't care if a traveler is accessing the network through IBM or GTE or even through a cable modem. That can be a big plus for corporate budget watchers. Since VPNs don't require co-operation from a service provider, mixing and matching service providers, depending on the pricing and availability of their various technologies and getting the best deal for your business is possible.

VPN variations

VPN typically uses the Internet as the transport backbone to establish secure links with business partners, extend communications to regional and isolated offices, and significantly decrease the cost of communications for an increasingly mobile workforce. Depending on the type of business, Internet-based VPNs have been classified into three different categories. A specific business may have one or more of the following three types of VPNs:

Remote Access VPN

Remote access VPNs is communication networks between a company and its remote and/or mobile employees. In such a network, the employees of a company may be stationed anywhere in the world as long as there is ISP connectivity available to the Internet.

Intranet VPN

Intranet VPNs provide secure communication between a company's internal department and its branch offices.

Extranet VPN

Extranet VPNs provide secure Internet communication between a company and its strategic partners, customers and suppliers.

VPN Benefits

Significant Cost Savings

A number of studies have shown that migrating from private to virtual private networks can generate cost savings of between 20%-90%. This wide spectrum of savings underscores a wide range of business communication environments. A major part of the savings results by eliminating long distance dial-up charges. Although cost saving is a major driver for moving to a VPN solution, other factors such as network simplification and additional features at lower costs are equally attractive. A Forrester Research study compares the costs of a traditional dial-up network with a VPN alternative.

Costs Comparison for 1000 Users

	Traditional Remote Access	Costs Internet VPN Costs
Phone/ISP Charges	$1.08M	$0.54M
User Support	$0.30M	$0.00M
Capital Expenses	$0.10M	$0.02M
T1 Lines	$0.02M	$0.03M
Total	$1.50M	$0.59M

(Source: Forrester Research Inc.)

Strategic Power

Even more important than the substantial cost savings are the strategic avenues that VPNs open for an organization. A flexible, ubiquitous communications infrastructure enables companies to pursue powerful new strategic initiatives and relationships, improve communication with offices and customers, lock in vendors and partners while creating barriers to competition, and develop and deploy new products with improved time-to market.

Reinvent the Business

A flexible, ubiquitous communication infrastructure provides companies the opportunity to literally reinvent themselves and their relationship with customers and partners. VPNs provide the freedom and flexibility to scale a business - quickly, easily, and cost-effectively.

WAN/Extranet

At one time, X.25 lines, frame relay links, and dedicated phone/ISDN lines were the only solutions available for connecting LANs into a WAN or interconnecting two companies' systems. These solutions proved to be cost-prohibitive for most companies, and, in the case of extranets, it was difficult to agree on who would incur the associated costs. Now companies can use VPNs to form

Key Players

- Microsoft offers VPN solutions packaged in their Windows 2000 OS. The Windows 2000 Server operating system integrates complete network services to let organizations affordably set up and manage networks, connect remote employees, connect branch offices, and set up partner extranets.
- The TimeStep Secure VPN Solution from Newbridge Networks brings flexibility, reliability, scalability and security to global communications over the Internet or the service provider's backbone. The solution supports triple DES data encryption standards and IPSec standards for compatibility with other compliant products. The TimeStep solution enables the service provider to offer a business-quality VPN service that allows customers to provide secure remote access to corporate networks, securely communicate with branch offices and establish encrypted communications with external organizations such as customers, business partners and suppliers.
- 3Com offers an end-to-end VPN solution with policy-based management and control, differentiated service levels, and its own Tunnel Switching Architecture. The latest component of 3Com's end-to-end VPN solution, 3Com's new DynamicAccess® technology offering enables remote workers to use the Internet or public networks to securely communicate and share information with corporate offices from around the world. For IS departments, implementing VPNs with 3Com's new DynamicAccess VPN encryption software dramatically reduces the cost and effort required to deliver remote access. 3Com's DynamicAccess VPN encryption software offering also includes 3Com's DynamicAccess mobile configuration manager to simplify VPN remote access for the PC user and further reduce IS support costs.
- Shiva VPN products uniquely combine inexpensive Internet-based access with unparalleled security. The Shiva Virtual Private Network Client is a software package that allows users to dial local ISPs and create secure tunnels to the corporate office. The Shiva VPN Client Deployment Tool is VPN software that allows the maintenance of Shiva VPNs
- Cisco VPN solutions encompass all segments of the networking infrastructure - platforms, security, network services, network appliances, and management - and thus provide the broadest set of VPN service offerings across many different network architectures. Cisco VPN solutions enable corporations to deploy VPNs on their existing Cisco networking gear. Cisco VPN solutions tightly integrate the many facets of VPNs with existing Cisco products---such as routers, WAN switches, access servers, and firewalls---ensuring the smooth integration of VPN technology into Cisco enterprise networks.

a secure connection across the Internet.

LAN Security

HR documentation and other sensitive data should not be seen by just anyone. Solutions prior to using a VPN were (a) access control and (b) separation of LAN segments. Neither of these solutions offered the high security of a VPN as data passed through the systems.

Business Applications of VPNs

Connecting a Remote Client to a Private LAN

VPNs are commonly used to connect a single remote user to a corporate LAN while maintaining security standards and privacy. The remote user merely calls a local ISP and the VPN software creates a VPN between the user and the corporate intranet across the Internet.

Connecting Two Remote Networks Over the Internet

A VPN can be used to connect a branch office to a corporate LAN using local Internet facilities. The router at the branch office can use either a dedicated line or a dial-up link to call the local ISP, but the corporate VPN server must use a dedicated line to connect to the local ISP. There are two business models for this type of VPN application: WANs and Extranets.

Connecting Two Computers on the Same LAN

VPNs can be used to solve the problem of protecting a department's confidential or sensitive information from the rest of the users on the same LAN while not creating any information accessibility problems.

Future of VPNs

As the Internet creates an ever-larger global community, the need for secure and seamless communication increases. Virtual Private Networks (VPNs) have provided solutions for those wishing to have secure remote communication with private networks connected by the Internet. Two issues are shaping the future of this technology: the integration of VPNs into the physical infrastructure of computer networks and the drive to increase the interoperabiliy of physical hardware as well as hand held web devices.

Integration

Until recently, VPNs were created with stand-alone software and hardware. However as the importance of secure and cheap communication has grown, large hardware vendors, particularly Cisco, have moved towards integrated products that combine the traditional stand alone elements into a single product and shifts the VPN technology into the core network infrastructure.

Interoperability

This move towards consolidation underscores the second fundamental issue of the future of VPNs, that of interoperability. As VPNs grow in importance the need for clear standards becomes greater. Due to complaints about the slow pace of the International Computer Security Association (ICSA, the organization for interoperability testing), and the need for faster and more reliable information, the industry formed its own organization to address these issues leading to the creation of the Virtual Private Network Consortium (VPNC). This group has been formed by leading vendors including IBM, Cisco and 3Com along with smaller companies in order to provide a forum and website where interoperability of products can be discussed directly among vendors rather than relying on third-party testing. As VPN technology becomes ever more important (by 2003, the market will grow at over 90% annually an reach $32 billion), these trends of consolidation and standardization will accelerate.

The author is Executive Editor with Strategicnewspaers.com
email - vinayg@strategicnewspaersd.com