Virtual Private Networking
Is Real Technology - Now

by
Tom Ferrell
Compatible Systems Corporation
tferrell@compatible.com

Remote network access is a fact of corporate life today. Even medium-sized companies have several branch offices scattered around the country or the world. Field sales people utilize remote access to take advantage of corporate network resources. Intranets and extranets allow suppliers to strengthen their bond with customers, and consultants can remove more barriers between their services and their clients. In addition, corporations can now hire telecommuting professionals from a talent pool far beyond their local area. VPN lets IT staff eliminate costly dial-up circuits, leased lines and administration-intensive modem banks, using local Internet Service Providers as a gateway to the Wide Area Network.

VPN is already making its mark. Infonetics Research estimates that the percentage of corporate employees requiring remote LAN access will climb from 8% in 1997 to 22% in 1999. With markets constantly expanding, remote offices also require access to the central network. Internet access is now ubiquitous, with Infonetics estimating that 99% of all companies will be connected by 1999, and the cost of high-speed corporate Internet connections is falling, encouraging IT departments to employ T1 or greater speeds. This combination of supply and demand only strengthens the business case for VPN.

If It's Virtual, Is It Real?

While there is no standard definition for VPN, most network analysts agree that a "real" VPN solution features:

- Use of a public network such as the Internet
- Tunneling, or the establishment of a secure data path using a protocol such as IPSec or PPTP (Point-to-Point Tunneling Protocol)
- Authentication, encryption and a method of controlling access privileges
- VPN management software

The benefits of VPN technology come in the form of cost savings – 30% - 75% of traditional WAN and RAS – simplified maintenance and ease of adding or modifying user accounts. In a VPN remote access application, remote users or LANs connect to a local ISP. Once connected, remote users and sites access the central network via TCP/IP tunnels.

What Flavor?

There are four basic types of VPN solutions.

- Hardware solutions employ dedicated processors and client software to create a VPN connection. These products are generally the most performance-driven in the category, often including dedicated encryption processors and other performance enhancements.
- Software solutions run on existing server platforms. Software lowers the cost of entry but places additional demands on the server's processor, degrading performance, and also creates a single point of failure.
- Firewall add-ons were the pioneers of VPN access. However, these products first require a specific type of firewall, creating a single-vendor situation that can limit options. Configuration and management of firewall-based VPNs tends to be

difficult, utilizing the same complex interface as the firewall software itself. Again, the VPN tasks must share a processor with the server running the firewall.

- VPN services from Internet Service Providers, who offer "turnkey" managed services by utilizing hardware-based or firewall-based VPN products housed at their own facility. The major consideration with managed VPN services is that your company's security infrastructure will not be directly under your control.

Tunnel to Freedom

VPN vendors create secure multiprotocol links across the Internet through a process called tunneling. Think of the tunnel as a "channel" opened inside the public network, in this case the Internet. Once connected, a remote user can utilize the tunnel to exchange information and access servers and services on the corporate network.

No matter the VPN technology, tunneling works by performing three basic operations.

Encapsulation

In order to transmit information securely over the Internet, VPNs encapsulate standard IP packets inside "protected" packets. The protected packet can then be routed through the Internet to its destination, where the encapsulation is stripped off, leaving the original data.

Several tunneling protocols have surfaced, most notably PPTP (Point-to-Point Tunneling Protocol) and IPSec. For security reasons, many vendors have moved to the more robust IPSec protocol, preferring its Layer 3 performance and strong authentication encryption and key management routines to the Layer 2 operation of PPTP.

Authentication and Encryption

While encryption gathers the most security ink, authentication is actually the most important security element of an IP tunnel. Authentication ensures that tunnels will only be established between verified tunnel partners. IPSec authenticates each packet that passes through an established tunnel. Under this method, each packet is authenticated using encrypted secrets in order to prevent session "spoofing," in which an authenticated session is taken over by an outside agency. PPTP, by contrast, authenticates only the session request, using traditional PAP (Password Authentication Protocol) and CHAP (Challenge/Handshake Authentication Protocol) routines.

Encryption is simply a method of "scrambling" data before transmitting it onto the wide area link, in this case the Internet. At the remote end, the data is de-coded using a private "key." Most VPN technologies include DES (Data Encryption Standard) or Triple DES encryption services to prevent "sniffers" from picking up data transmissions.

Behind the Firewall

Unlike traditional modem banks, VPN servers can be deployed behind or parallel to the corporate firewall. In these applications, network managers can filter out all traffic except packets containing the destination address of the VPN server. This provides a double layer of security. There are fewer holes in the corporate firewall, and packets much be authenticated again at the VPN server before being allowed on the network.

A VPN Checklist

As security issues become more well-known and understood, performance issues rise to the top of the network manager's list of concerns. While your VPN configuration and

needs depend greatly on your specific application, there are a few guidelines you should always follow.

- Choose an ISP with nationwide coverage. A national ISP – or a regional one that provides access points nationwide – will allow you to take full advantage of local calling for remote access connection. You should also ask potential ISPs about technical support policies, internal network benchmarks and optional services such as bandwidth reservation.
- Use filtering. More than 80% of all network security breaches are caused by unauthorized access that proper filtering configuration would have prevented.
- Assess the criticality of the data to travel the VPN link and configure for performance. Know what kind of traffic your remote users will generate and ask your ISP for their recommendations in optimizing the network link. Set internal policies regarding the transfer of mission-critical or highly confidential data.
- Integrate VPN into existing remote access systems. VPN is the remote access technology of the future. If you already provide remote access, add VPN on a departmental basis. Look for VPN products that incorporate full VPN routing, allowing you to scale the rollover from traditional connection to VPN.
- Choose a VAR or ISP will full support capabilities. Even an easy-to-use networking solution can be tough to configure and manage. Look for help from a reputable networking VAR in your area or from the service arm of your ISP.

Is VPN for You?

If your business relies on a number of remote users, VPN technology may well be the answer for you. VPNs are also excellent choices for providing access to corporate intranets and extranets.

The best advice is to do a thorough assessment of your remote access and intranet/extranet needs. How many users do you need to support? What information do they need to access? How confidential or mission critical is the data that will be sent and received over the VPN link? Then do the math. You'll be surprised at the savings VPN can offer.