Security and IP/VPNs:
A Package Deal

By Joan Burek

Joan Burek

There's been quite the discussion (and suspicion) surrounding IP/VPN (Virtual Private Networks) and network security. The general assumption is that IP/VPNs are open invitations to non-authorized access, and the foolish that choose to implement this swiss cheese network get what they deserve. The bony finger of suspicion is always pointed at IP/VPN's dial access and Internet overlay – the purported weakest links in the communications chain.

However … IP/VPNs do provide the necessary security. Their attributes extend to cost-effective, high-speed access, and, national and international reach. These benefits can position IP/VPN networking for many applications that currently run on traditional facilities, such as Frame Relay and dedicated links.

First off, let's review the IP/VPN topology and its "reason for being".

IP/VPNs were originally devised for the road warriors among us – those individuals that required intermittent, on-demand access, from a variety of locations, to connect to their corporate LAN. This access would permit the road warrior to read e-mail, pull down files, invoke "thin-server" software; allowing the individual to establish an office away from an office (a derivation on a home away from home). As many of us have experienced, we now have the opportunity to work, with all the necessary tools and software, regardless of where we are physically located.

As depicted in **Figure 1**, the individual connects to the company LAN via the following steps:

(a) Access is initiated by the PC's "dial-up networking" facility. This access uses a network provider's PSTN (Public Switched Telephone Network) or ISDN (Integrated Services Digital Network) to connect to the IP/VPN's NAS (Network Access Server). (Think of the NAS as a bank of dial modems – with some additional functionality – that serves as the gateway to the IP/VPN network).

(b) During the "dial-up networking" operation, a userid and password, unique to that individual is requested. The "road warrior" enters their specific information – as their keys that unlock the IP/VPN and company's services and LAN.

(c) The connection request (userid and password) is routed to the AAA (Authentication, Authorization and Accounting) Security Server and a preliminary authentication is performed. This authentication verifies that the requesting individual has the authority to access a pre-determined path to the company's home gateway router.

(d) The connection request (userid and password) is then routed to the company's Home Gateway Router and a subsequent authentication is performed. This action verifies that the requesting individual has the authority to access the company's Home Gateway Router (and beyond). In addition, additional security options can be implemented to perform a finer degree of authorization (potentially permitted limited access to files, software, and such).

(e) Once all authentications are received and reported, only then a tunnel is built from the end user to the Home Gateway Router (and potentially the application). This tunnel is specific to the accessing individual and the Home Gateway Router.

(f) From that point on, the individual has access to the authorized applications and services from his company's mainframe +.

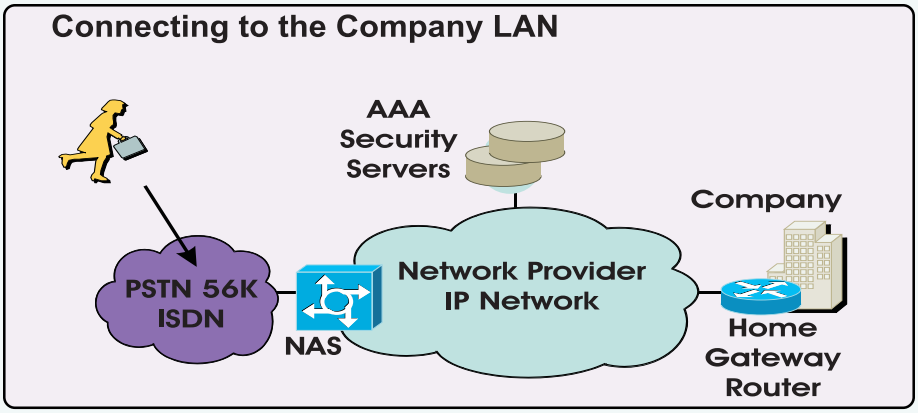

Figure 1.

Initial connection to application access takes approximately 20-30 seconds, dependant upon network provider. Then, (again dependant upon network provider,) idle and session timeout values differ, (where idle timeout refers to a session where no activity has occurred for "x" minutes, and session timeout refers to the session's overall on-net time, and can be terminated after "y" hours).

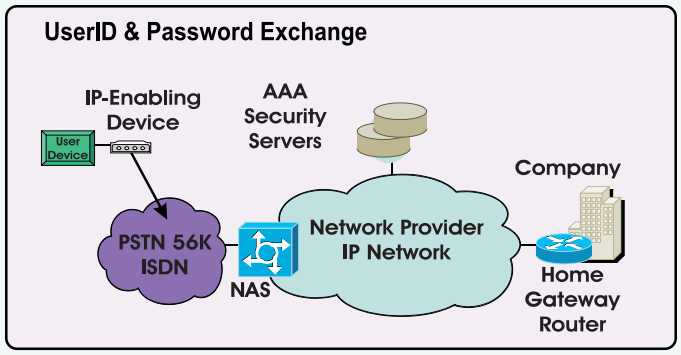

Figure 2.

The significant security factors for IP/VPN networking involve the terms, userid and password, and tunnel. Under current IP/VPN deployments, access is ONLY gained if the userid and password criteria is met – and note that the "gained" verb only refers to the network provider's AAA server and the customer's Home Gateway Router. Those two watchdogs guard against unauthorized access to the host system (and application) by providing preliminary verification. If the userid/password doesn't pass muster, a tunnel is never built between the user and the host system.

The tunnel itself provides a locked in path between the end points and virtually eliminates the possibility of anyone else scooting in. When a tunnel is invoked – there is no swinging door at the host location – the tunnel only permits the one individual, who has passed the security criteria, to enter and use the host facilities and applications.

So, IP/VPN is a great medium for road warriors; but how does this accommodate other traditional, applications-based environments? How can remote, stupid devices utilize the IP/VPN network, (and all its inherent benefits such as cost effectiveness, reach, cost effectiveness, speed and cost effectiveness) to meet their access needs? Some IP-enabling manufacturers have realized this as a potential opportunity for the "less than 128 Kbps market" and have programmed scripts into their communicating devices. It was early recognized that the remote environment (device, personnel, etc) could or would not provide the IP/VPN exchange (userid and password). In addition, it was realized that the connection time (20-30 seconds) was much too long and idle/session timeouts would seriously affect the overall performance of the application.

All three issues were / are being resolved through the cooperation of the IP-enabling manufacturers and the network providers. Programming within IP-enabling technologies has permitted the device to simulate the "road warrior": actions and responses, without human intervention.

Upon an appropriate trigger, the IP-enabling device initiates the dial sequence, and offers a password-protected and pre-programmed userid/password to the IP/VPN. Although the connection time cannot be reduced at present, it was felt that as long as only "one" connection attempt occurred, prior to the beginning of the business day that could attract customers to the IP/VPN family. In addition, through a device-programmed initiative, "keep-alives" can be implemented to eliminate the idle timeout concern. Lastly, network providers are realizing the significance of this market and have/are investigating the extension or elimination of the session timeout.

As discussed earlier, the move to IP/VPN for traditional applications isn't as much as a leap, when one considers all the parameters, including the security aspect.

User authentication, via id and password, for road warriors or smart devices and the specific, one-path tunnel, can provide the cost-effectiveness and speed demanded by your organization. T🖫G

After many years of dabbling in the creation of Telco-based network architecture for new protocols and processing philosophies, Joan is now creating IP-enabling components and opportunities for legacy protocol devices. She is Vice President, Canadian POS for Precidia Technologies Inc. Telephone: (905) 886-4192 Cell: (416) 702-3547 E-mail: jburek@precidia.com