

# Do you need a VPN?

Virtual private networking offers many benefits. **By James Gretta**

**A**s internal corporate networks grow and telecommuting/remote offices become more commonplace, companies are turning to virtual private networks (VPNs) to provide access to internal corporate resources.

A VPN is a collection of private data and voice networks utilizing the public communications infrastructure. VPNs operate on the premise of tunnels, which protect the data inside from external threats, utilizing predetermined parameters.

The goal of a VPN is to offer the same services to both internal and authorized external personnel, while at the same time minimizing overhead costs. The need for point-to-point leased lines can be virtually eliminated when a VPN is implemented properly.

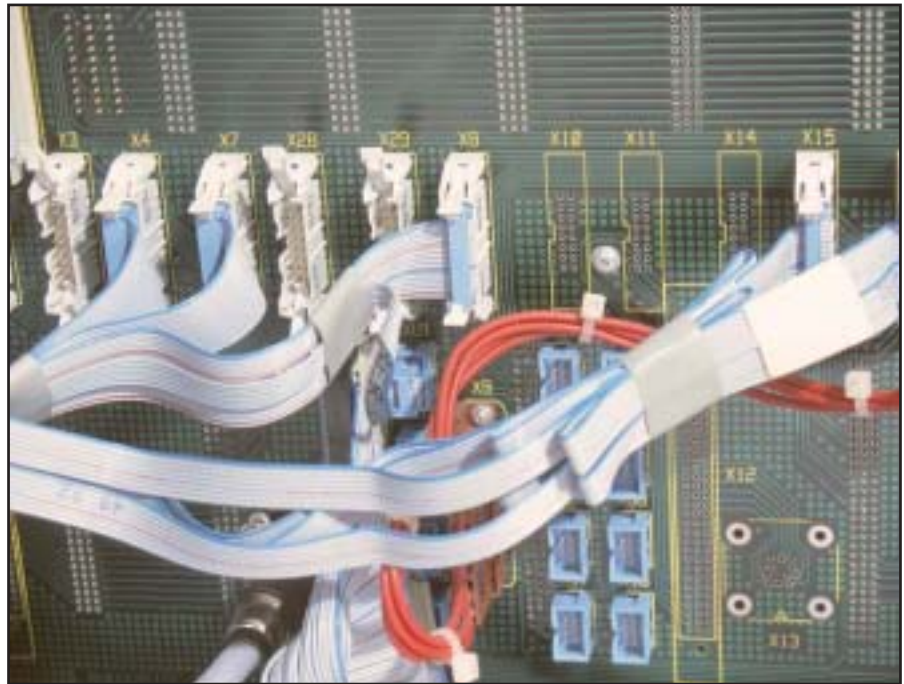
There are numerous vendors that offer a variety of VPN capable equipment. Several offer a variety of routers, firewalls, remote access clients and concentrators that support very scalable VPN implementations.

IP Security (IPSec) is the most dominant of all secure VPN technologies and is a standards-based method of providing integrity to data transmitted over IP. IPSec provides layer 3 encryption of data packets and utilizes various checks and balances to ensure data integrity. Key management and security associations, the IPSec parameters between devices, are negotiated utilizing the Internet key exchange.

The Internet offers a wide variety of opportunities and resources, but they do not come without inherent risks. These risks, as well as the need to protect sensitive information, are what drives the need for VPNs. The following three items may have you asking, "Do I need a VPN?"

■ **Data privacy** — Traffic traversing the Internet is unencrypted and can be viewed by unauthorized parties between the source and destination. This may be acceptable in many instances, but there are times when confidential information may be compromised.

■ **Data integrity** — While it may not be detrimental if unauthorized persons or entities could read your general e-mail, it



could be problematic if they could access and possibly modify more sensitive documents, bank transactions, etc.

■ **Identity theft** — Hackers are becoming more creative in their techniques, and identity theft is becoming more prevalent. Nonsecure data such as credit card numbers, Social Security numbers and bank account numbers may give people the information they need to take on your identity and, in turn, gain access to your confidential information.

Although the answer to the question, "Do I need a VPN?" may seem relatively easy, the solution needs to be planned and implemented diligently. Defining exactly what types of information need to be secured is the first step. Certain traffic, such as remote file and mail requests, may need to access the corporate Internet, whereas World Wide Web (WWW) requests do not.

VPNs reference a series of permit-and-deny statements to determine which traffic should and should not traverse the VPN. If traffic is marked as interesting, it follows the IPSec encapsulation and encryption

process and is forwarded to the other end of the tunnel for validation, de-encapsulation and decryption. Traffic that is not interesting will be routed in clear text, based on current implemented policies.

Another popular implementation is the use of remote access clients. These clients have software installed on PCs, laptops or PDAs and are able to securely access internal resources. Typically the software is very inexpensive and is a more-than-adequate solution for remote salespersons, managers, IT staff and executives.

Network and information security are becoming increasingly more important in corporate environments. VPNs offer another level of defense against unauthorized access to confidential information while still maintaining flexibility and scalability.

There are still instances in which point-to-point links make sense and are necessary, but in many cases, having a virtual point-to-point network is both cost effective and secure.

**JAMES GRETTA** is a network integration engineer at TriLogic Corp., a solutions integration company focusing on IT infrastructure solutions. He is a Cisco Certified Network Associate. Reach him at [jgretta@tri-logic.com](mailto:jgretta@tri-logic.com) or (724) 745-0200.