



Improve Your Communications with a Managed Virtual Private Network

Why VPNs are hot...

Virtual private networks (VPNs) provide the means for companies to securely network their business using less expensive Internet technology. Basically, VPNs let businesses carve out "private" IP-based networks without the need for expensive dedicated circuits. A company's VPN traffic is carried across a carrier's high-speed backbone and/or across the public Internet.

Security functions are performed on the data packets so they are safely routed across the shared infrastructure. With the right security precautions, selected segments of the VPN may even be opened to business partners, suppliers and clients.

By drawing on the economies and efficiencies of the larger Internet, VPNs offer substantial cost savings over traditional private lines or more expensive packet-switched services. VPNs are also replacing costly and slow dial up access for remote users, reducing the expense of modem banks, Long Distance and Toll free usage.

Innovative business applications

VPN services enable a wide variety of business applications, including:

- Multimedia services and graphics sharing
- Video applications, including video conferencing or remote training/education

How your business can benefit with a managed VPN...

- Establish secure, low cost, site-to-site connectivity via the Internet.
- Provide easy access to company-wide applications without regard to distance.
- Connections are sized to meet each location's unique bandwidth needs.
- Facilitate deployment of an Extranet to connect business partners in the supply chain.
- Predictable flat-rate billing simplifies IT budgeting.
- Access to a secure Web Portal for viewing reports, requesting changes, and obtaining online technical support.

- Voice over IP
- Access to Internet/intranet/extranet applications and services

In addition, a VPN offers more security for corporate data and it increases connectivity by empowering mobile professionals to be "in" the office, no matter where they may be working. This gives them access to company servers, applications and e-mail, allowing them to work just as efficiently off-site as in the corporate headquarters.

Access for your VPN

Although Frame Relay and ATM may be used to create a VPN, the Internet is by far the most popular way to build a VPN. Not only is the Internet available everywhere, but the technology is comparatively inexpensive. Large companies can leverage their Dedicated Internet Access connections to access their VPN, while smaller businesses can use an economical bundled service like Verizon's Flexgrow, which packages Internet connectivity as well as local and long distance calling. Remote users can take advantage of whatever they have to access their company's VPN, including DSL, ISDN or Cable.

Managed or unmanaged VPNs

VPNs are offered as fully managed, co-managed, or customer-managed services. Customers of a managed VPN service typically pay a single, all-inclusive service price, which includes equipment, software, maintenance, and 24 × 7 proactive management and monitoring. With a managed VPN, the customer is relieved of the entire management burden, making this service ideally suited to smaller companies with multiple locations or remote users. In the case of carrier-managed VPNs, service-level guarantees are available.

Companies that opt for the managed VPN services of an experienced provider like Verizon can save by not having to:

- Invest in and maintain expensive capital infrastructure
- Track emerging security problems and perform complicated security application upgrades
- Recruit, hire and retain qualified IT staff.

A managed VPN allows companies to concentrate on managing their business instead of maintaining their network, worrying about configuration details and performance issues, and staying on top of security threats.

How does a VPN work?

VPNs implement “tunnels” over which data and voice applications are supported. A tunnel is a dedicated end-to-end connection (Figure 1) similar to a virtual circuit (VC) used to transfer data over a Frame Relay or ATM service. Since a tunnel goes only to a designated destination, it provides secure transport. By themselves, however, some of the tunneling protocols do not provide for data security. To enhance security, a device may be added to every access location on the VPN. In addition to helping secure the VPN at each location, this box enhances security with a firewall, intrusion prevention, anti-virus and content filtering capabilities.

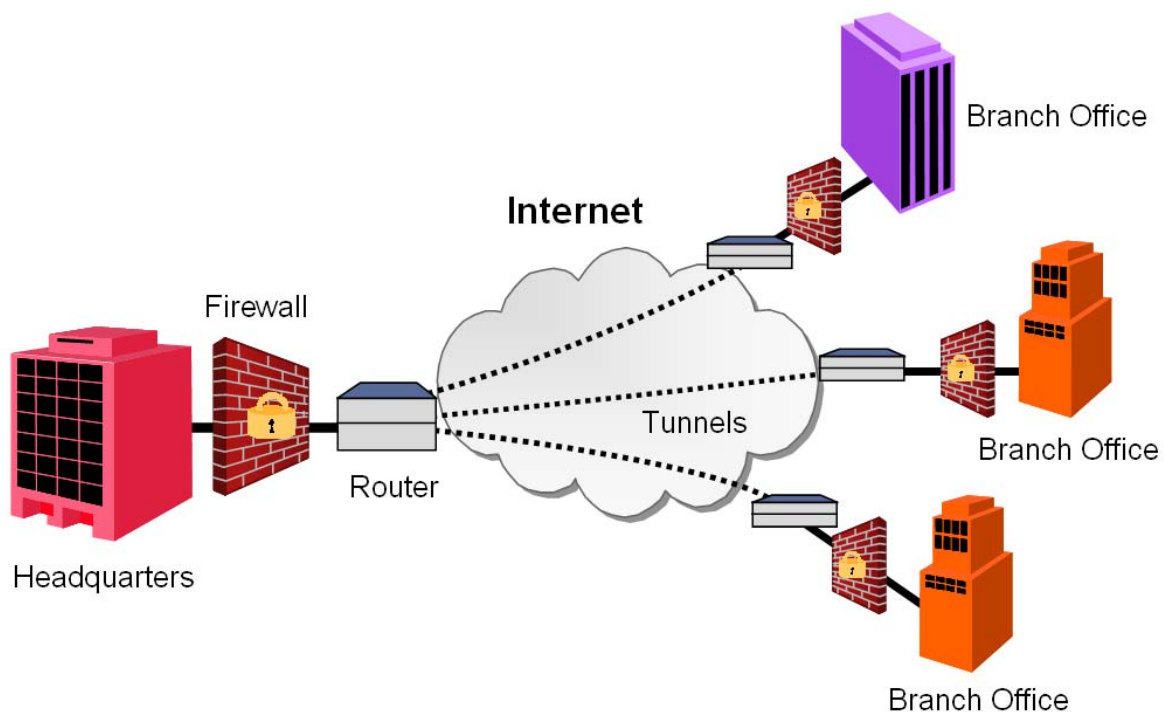


Figure 1 -- A VPN is implemented with point-to-point connections called “tunnels” that provide secure data communications between locations on the Internet. Additional security is provided by other devices such as firewalls.

VPN security

Without a secure and effective network connection, online corporate resources may be susceptible to malicious hacking and theft of company information. Fortunately, carriers are addressing these issues. Verizon's VPN Service offers a flexible, cost-effective solution that combines tight network security with increased connectivity. It includes the same hardware and security features as a premises firewall, while allowing the use of encryption technology to create secure data connections, allowing secure remote access to the corporate network.

Firewall SonicWALL SOHO3

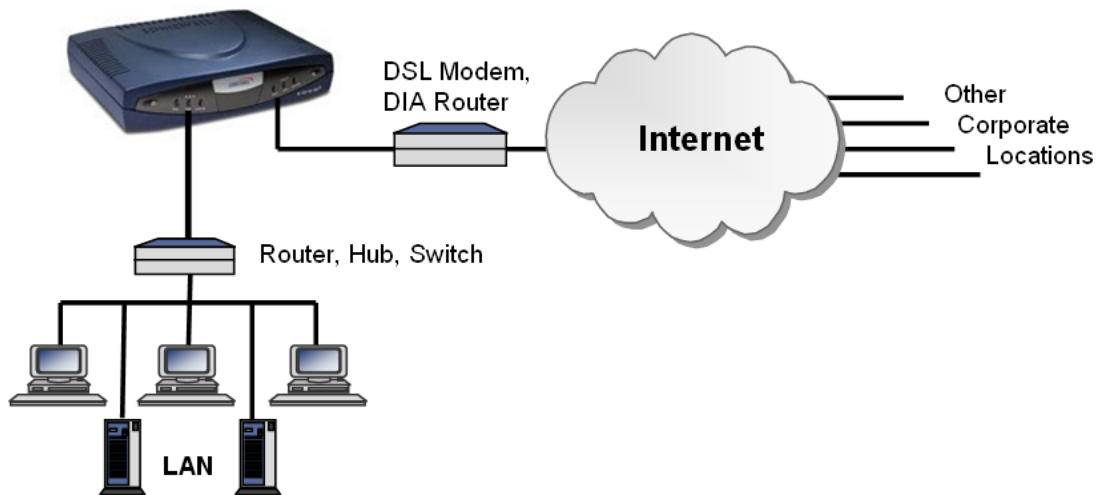


Figure 2 -- A plug-and-play SonicWall™ hardware appliance is shipped pre-configured to the customer, specific to their Internet connection and security policies.

With the help of a SonicWALL™ security appliance at each corporate location (Figure 2), the Verizon Premises Firewall:

- Detects and rejects denial of service and other attacks to help keep your network up and running.
- Provides secure site-to-site connections that can enable your company to share data securely between multiple business locations via encrypted, site-to-site VPN tunnels over the Internet. Each site has both its own static IP access and a managed SonicWALL™ hardware device.
- Gives you control of access via standard security settings, or Verizon can work with you to create customized configurations for your specific business needs.

- Features advanced firewall technology called “stateful” packet inspection, which intercepts and reads incoming packets until it has enough information to determine the security status of a connection.
- Provides monthly Web-based reports to help identify the time and origin of attacks on your network. This information can assist your company in evaluating and changing its security policies.
- In addition to monitoring the system status of your SonicWALL™ security appliance, Verizon’s security operations center offers centralized management and customer support on a 24 x 7 basis.

The SonicWALL™ security appliance at each office location, combined with remote VPN client software downloaded onto the PCs and laptops of employees, provides authentication and encryption to help ensure that only authorized users access your network remotely and minimize the risk that your data will be intercepted. With the VPN client software, remote users simply need Internet access to efficiently use the company LAN.

Further considerations

Once your business has decided to get serious about implementing a VPN, there are some key elements that deserve further consideration. A review of these may also help determine whether a managed or unmanaged solution makes sense for your business.

Establish firewall protection. To seal the network against outside threats, it is recommended that a firewall be implemented in conjunction with the VPN. The firewall will protect the internal network against attacks from the Internet. Some routers not only support VPNs but include an integral firewall as well. Additional capabilities of these routers include address authentication, reporting, and flexible alerts.

Choose equipment carefully. As noted, there are several tunneling protocols available for implementing VPNs, some of them favored by particular vendors. But when companies are acquired or merged, interoperability can remove some of the pain and expense of consolidating networks. Equipment should be chosen with future change in mind. Because most manufacturers now support the IPSec standard, their VPN gear can be configured to interoperate at some level with other vendors’ equipment. This is good because it lets businesses create networks that do not rely on a single vendor. Therefore, it is wise to choose equipment that supports IPSec.

Implement authentication. Look into authentication mechanisms to protect the VPN from unauthorized access, such as digital certificates and directory services. Digital certificates can be used to authenticate the encryption keys of IPSec end stations, while network directory technologies and products can play a large role in managing authentication and security policy information. These directories are the logical place to store user profiles, and make the storage and management of digital certificates more efficient.

Use longer encryption keys. As hackers and technology increase in sophistication, there is a demand among companies for more sophisticated and secure encryption technology for their VPNs. Although encryption based on 40-, 56- and 64-bit key lengths is generally accepted as the minimum requirement today, VPNs that rely on longer keys and stronger encryption algorithms are more resistant to attack. Therefore, it is recommended that 128-bit or higher encryption keys be used to protect the VPN. It is also advisable to choose routers that can be upgraded to support future encryption algorithms. For example, a router that supports 3-Data Encryption Standard (3DES) should be able to accommodate the newer standard called the Advanced Encryption Standard (AES) when the company requires it.

Deploy intrusion detection. As threats to networks increase in sophistication and complexity, the ability to detect and react to these threats becomes critical. One important feature to look for is how easily the intrusion detection threat database can be updated. A threat profile is a pattern of attack used by hackers which identifies it as an attempt at intrusion. These patterns or “signatures” can be loaded into the threat database to thwart intrusions that match that attack profile.

Implement policy-based security. Policy-based security systems help network administrators keep up with new vulnerabilities and threats. Unlike point-to-point management where security devices are configured one by one across the network to attain the right level of security, policy-based security allows network administrators to address groups of devices or all devices on the network directly, enabling patches and updates to be pushed to each device on the VPN in an automated, uniform fashion, while also receiving verification that the new configurations have actually been executed. With point-to-point management there is a window of opportunity that can be exploited by hackers until all devices are reconfigured to stop an attack; policy-based security management closes that window.

Network management. An extension to the enterprise network, the unique aspects of VPNs must be viewable and controllable all the way through the wide area and out to the remote VPN user -- preferably from a browser-based interface.

Address special needs of telecommuters. If a VPN is extended to the homes of telecommuters, the IT department must consider securing the home in the same way as they would a company network. Firewall appliances are the easiest way to do this because they require minimum involvement by users, they can be integrated into corporate firewall policy management, and they have the added benefit of being remotely managed and updated by the corporate IT security team.

Moving ahead

Staying competitive requires that businesses work toward improving productivity and managing costs in every aspect of their operations, including communications. This in turn is making managed services more attractive to companies of all types and sizes. CNS recommends giving considerable weight to a service provider's experience, reliability and accountability.

After the choice of service provider is made, start with a phased implementation and if the quality and performance of the VPN solution meets your expectations and the price is right, you're ready to negotiate a timetable for installation across the enterprise.



Choice Network Solutions, Inc.

1025 Connecticut Avenue, NW

Suite 1000

Washington, DC 20036

202-828-12143

888-588-2171

www.choicenetwork.net