VPN Equipment Comparison & Selection Guide

by: Daniel Figueiredo

Docid: 00016952

Publication Date: 0212

Publication Type: SELECTION GUIDE

Preview

A virtual private network (VPN) provides cost-effective answers to a business' need for simple, secure remote access. Although VPNs offer much to an enterprise, they have several drawbacks that should be considered when choosing a method of remote access. This report describes VPNs, discusses selection criteria, and compares the leading vendors.

Report Contents:

Executive Summary

[return to top of this report]

Telecommuting and mobile work are on the rise. So is the desire to grant suppliers, business partners, and customers limited access to the corporate network. This leaves IT departments hunting for a simple and relatively inexpensive means of providing secure remote access. Private leased lines can cost tens of thousands of dollars a month, while a corporate remote access server can also leave a dent in the budget. A virtual private network (VPN), which transports information back and forth via encrypted connections, also known as "tunnels," through the public Internet or a carrier's backbone, can provide major cost savings over other methods of achieving remote access. VPNs, however, are not without their (sometimes hidden) costs. A wise IT manager will do a cost-benefit analysis of several remote access alternatives, taking into account both hidden and obvious expenses, before settling on any particular solution.

Description

[return to top of this report]

Virtual private networks send private data securely through a shared network. There are three primary types of virtual private networks; remote access, Intranet, and extranet. They have four security components: firewalls to prevent unauthorized traffic, an encryption system to help conceal the data intended for transport, packet authentication, and a means of identifying users. Other components can be added for additional functions. VPNs also include tunneling protocols to protect information as it travels across the public network. In operation, a remote user connects to the Internet via an ISP. For example, the user sends data in the form of IP packets to a firewall. At the firewall, the data is encrypted and then sent via a "tunnel" through the public Internet. The intended recipient's VPN server decrypts the data packets and delivers the information.

Certain standards are associated with VPNs. The standard tunneling protocol, Level 2 Tunneling Protocol (L2TP), works with both of the formerly competing standards, the Microsoft and 3Com-backed Point-to-Point Tunneling Protocol (PPTP) and the Cisco-backed Layer 2 Forwarding (L2F).

The IP Security standard or IPSec, is the IETF-approved security standard for Internet-based VPNs. IPSec, which was specifically build for communications over the public Internet, measure confidentiality and integrity, as well as authentication. Authentication for VPNs can be measure by shared secrets, which are used in site-to-site VPNs, user names and passwords, proprietary tokens, or digital certificates.

VPNs help companies save vast amounts of money, but they have drawbacks. They combine networking and security components, which in most cases must be manually configured--and at remote sites with little or no access to on-site IT assistance. Occasionally, they require large amounts of troubleshooting, causing the IT staff to spend more time solving user problems. First-generation VPNs often did not provide automated policy enforcement, which is a problem many of the second-generation VPNs fixed.

New releases for VPN equipment are also starting to integrate Linux-based appliances, allowing for Linux users to incorporate various equipment within their products as well.

Selection Criteria

[return to top of this report]

While possible to achieve full implementation from hiring an outside company, such as AT&T, this guide is meant for those implementing their own VPN. If a company already has a network installed, adding a VPN should not be a problem.

The main factors to consider when purchasing a VPN are if the equipment can deliver the expected performance and the cost savings a VPN can provide. If not, than a VPN will be of little value to the users. It is important to consider other factors as well, including ease of use, speed, scalability, and vendor support.

Ease of Use

Several issues fall under this heading. Consider how easy the VPN will be to install, operate, maintain, and manage. The amount of manual upkeep an IT administrator must perform to keep the VPN running matters, and should be figured into the cost of the VPN. Automated features, particularly for policy-driven management, will ease the maintenance burden.

Additionally, it is important to look for Web-based management by finding out which browser the VPN supports for this function. Some ease of use issues may come as unpleasant surprises. For instance, a

few VPNs needlessly separate routing and firewall functions into separate boxes, which means multiple devices need to be connected at each remote site. Ease of use is perhaps the most important deciding factor when choosing a VPN. A poorly configured VPN will not do its job, making it useless. The VPN installation should be relatively easy, especially if remote users are expected to install the VPNs themselves. Some VPN's support remote software installation, which alleviates countless headaches from less tech-savvy users. The user logs in, and the host takes over, downloading and configuring the users setup.

Speed

For a VPN to work at its best, it must work quickly. A VPN that is slow can lead to frustration amongst its users. For larger enterprises, a slow VPN can lead to numerous complications. Some manufacturers are currently able to offer VPNs with speeds of 2G bit/second. Check with the vendor for the maximum speed and the number of users that the VPN supports.

Scalability

Not only must a VPN be able to support the company's present number of remote users, it must also consider whether the VPN will be able grow with the company. Not all VPNs scale well, and with the number of telecommuters and mobile users increasing, planning ahead may save headaches and costs in the future. While most VPN equipment is scalable to some degree, it is important to know exactly how far its features will stretch. This makes having an extension plan, or at least an idea of future growth, becomes vital to the future costs a company can endure.

Performance

Similar to the issue of ease of use, the performance of VPNs cover several factors. Consider whether the VPN's functions are quick enough for the company's purposes, even when it has multiple users connected at the same time. Also consider the security of the VPN since it will carry confidential business information. Although usually industry-wide, check to see if the VPN supports all of the appropriate standards. A VPN that supports many standards is one that will most likely have a longer and more useful life.

Vendor Support

A company can directly deploy its own VPN over standard Internet services, or it can outsource the VPN to a carrier or a service provider. Either way, a VPN deployment is no simple matter. It pays to make sure the vendor will stand behind its work. Find out whether the vendor will help distribute client software to remote users, configure IPSec parameters on remote PCs, and resolve problems resulting from program conflicts. A cheap VPN with poor support will cost more in the long run. Again, a poorly installed VPN will prove worthless, since the smallest security loophole defeats the very purpose of having the VPN. It is also important that equipment is able to integrate with current or future equipment and environments.

Market Leaders

[return to top of this report]

Avaya Communications, Cisco Systems, Enterasys, and Nortel Networks are the market leaders, with many other companies entering the very lucrative market every month.