

Virtual Private Networks— Real-world Challenges and Solutions

Michael E. Huang
President, FirstVPN, Inc.

<http://www.firstvpn.com>

Commissioned by Internet Asia Magazine



April 1, 2000

Introduction

VPNs have arrived. A virtual private network, or VPN, uses encryption and tunneling to connect users or sites over a public network, usually the Internet. In comparison, a private network uses dedicated lines or virtual circuits between each point and is usually a much more expensive solution. Having matured from proof of concept into a worldwide reality, VPNs offer significantly lower communications costs to both small and large companies, especially when deployed in concert with low-cost broadband technologies like DSL.

WAN Killer

Make no mistake about the importance of VPN technology— it will eventually replace leased lines, frame relay, and ATM. As an indicator of market velocity, VPN manufacturers are being acquired in the US at a break-neck pace, led by Cisco's acquisition of Altiga Networks for 500M USD, and more recently, Efficient's purchase of NetScreen Technologies for 900M USD. VPN has become big business.

The combination of VPN and DSL completes the replacement strategy on which the Internet will thrive in the coming years. The Internet is inherently valuable because it has unprecedented global reach, yet at the same time, it is a dangerous medium for transferring proprietary or sensitive information. In the past, CIO's were confronted by an obvious trade-off between cost and security, but with the introduction of VPN the distinction is blurred and the choices are more subtle.

First VPN

While VPN is a major replacement threat to traditional WAN technologies, it is also ideal for users who are building their first wide area network. With such a dramatic decrease in cost, many small companies can now afford to connect themselves using VPN. Small businesses find VPN attractive for several reasons. For the retailer, multiple stores can use the Internet to exchange data quickly, while other professionals like doctors and lawyers can share and protect privileged information. Whatever the reason for adopting VPN, the challenges remain the same for all.

QoS

Currently, one of the most significant components involved in the design and management of a VPN is QoS, or quality of service. Compared to wide area networks built on leased line, frame relay, and other technologies, DSL-based VPNs can save fifty to sixty percent, but the service level agreements are not yet comparable to those available on traditional services like T1 and E1. As a work-around, FirstVPN advises users to deploy redundant T1 / E1 Internet access services at their major corporate offices, and single circuit DSL at the smaller sites.

Interoperability

Interoperability between manufacturers is another major design issue. IPSec is clearly the emerging standard, but many vendors have slightly different implementations, and further, most vendors have incomplete or immature product lines— Some have excellent high to middle range products, but they have not developed an affordable system for the SOHO space. Driven by the need to reduce total cost, users need to integrate multi-vendor solutions, which is possible in theory, but extremely difficult in reality. FirstVPN has worked with major manufacturers to offer multi-vendor solutions, especially between Cisco / Altiga, NetScreen, and RedCreek. For example, we use the Altiga concentrator at the central site, and the NetScreen and RedCreek devices at the small offices, while the remote access users have the Altiga IPSec client. Combining equipment delivers an extremely robust and affordable solution.

Supportability

Perhaps the most significant obstacle to adopting a VPN relates to supportability. The technology is relatively complicated, training is not yet available, experts are scarce and expensive, so outsourcing might be the answer. Much has been written on the pros and cons of outsourcing, but for many organizations, there is very little choice. As in any

external arrangement, each party in the agreement must clearly state and understand their responsibilities. VPN is just as easy to outsource as any service and should fall under the same selection criteria when soliciting proposals. Keep in mind that bigger is not necessarily better. In fact, choose a provider based on their experience. The second system effect applies here—the second VPN will always be better than the first, so choose a provider with depth and experience.

Politics

In most organizations, political agendas abound, and adopting a VPN can become a lightning rod in a politically charged environment. It seems to be an axiom that in most organizations new technology is selected and adopted with three criteria prevailing in a definite order. Decisions seem to be made first by political factors, then by business case, and finally on technical terms. Common sense will not always prevail. Remote access managers might see VPN as an encroachment of their authority, while WAN administrators might feel that a VPN will represent huge overtime burdens and some very late night troubleshooting sessions. Your CFO will love the financial returns, but the CIO might not want to change a network infrastructure that already works reliably. An outside consultant can take the political heat and survive in scenarios that might otherwise be untenable. If you are a proponent of VPN and a consultant is not a possibility, take the time to analyze political, business, and technical issues.

Conclusion

Adopting a VPN is well worth the time and effort, but keep your expectations realistic. VPNs secure the traffic between multiple points on the Internet, but they are not suitable as a replacement for the effective perimeter security provided by firewalls. Many solutions seem viable, but fail to deliver their promised features. Choose wisely and recognize that the best value is the lowest total cost of ownership, not simply the lowest equipment or software cost.