The Advantages Of A Virtual Private Network For Computer Security

Sid Sirisukha

School of Information Technology
Auckland University of Technology
sitsir69@aut.ac.nz

Proceedings of the 16th Annual NACCQ, Palmerston North New Zealand July, 2003 (eds) Mann, S. and Williamson, A. www.naccq.ac.nz

ABSTRACT

Computer and network security are leading edge risk challenges for executives and managers of organizations. The speed of change results in organization management teams that are often not fully aware of the many advances and innovations in Internet security technology. Without this knowledge, many organizations are not able to take full advantage of the benefits and capabilities of the network.

This paper discusses how VPN (Virtual Private Network) can be advantageous for securing computer communications. It will describe how effectively a secure solution can be implemented by providing VPN services and protocols.

Keywords

Virtual private network; computer security; protocols.

1. INTRODUCTION

Organizations have become increasingly dependent on computer network systems for their daily business communications, database information retrieval, and distributed data processing. Baukari and Aljane (1996) state that as the Internet became more and more accessible and bandwidth capacities grew, organizations began to offload their Intranets to the web and create what are now known as Extranets to link internal and external users. Emphasis on network security has also increased, as a result of well-publicized security break-ins, threats, and as government regulatory agencies have issued security-related pronouncements.

While the Internet has transformed and greatly improved information access for businesses, this vast network and its associated technologies have opened the door to an increasing number of security threats for which organizations must protect themselves. Although network attacks are presumably more serious when they are inflicted upon businesses that store-sensitive data, such as personal medical or financial records, the consequences of attacks on any entity range from mildly inconvenient to completely debilitation. These are significant costs with implications for important data, privacy, network downtime, and third party legal claims.

The central focus of this paper is a study in progress on how organizations can benefit by using VPN (Virtual Private Network) services and protocol to securing their computer network systems. The issue is discussed in terms of how organizations value computer network security differently, and the many that reasons exist for preferring a private network to a public network. I then raise the issue of enhanced trust and e-business opportunities, increased service opportunities, and most importantly, increased cost savings secured by VPN preferences. There are many advantages by implementing secure connections to suppliers, customers, partners, and branch offices, organizations can build customer loyalty, improve time-to-market, and reduce inventories.

2. VPN TECHNOLOGIES

A VPN is a network provides inter-connectivity to exchange information among various entities that belong to the VPN. A VPN is an especially effective means of exchanging critical information for employees working

remotely in branch offices, at home, or on the road. It can securely deliver information between vendors, suppliers, and business partners, who may have a huge physical distance between them. Such networks are deployed within a public network and aim at providing a private working environment to its users while also takes advantage of the efficiencies of the underlying infrastructure. Liang et al (2002) point out that it is also private and with all the characteristics of private network.

A private network supports a closed community of authorized users, allowing them to access various network related services and resources. The traffic originating and terminating within a private network traverses only those nodes that belong to the private network. Further, there is traffic isolation. That is, the traffic corresponding to this private network does not affect nor is it affected by other traffic extraneous to the private network.

A final characteristic of a VPN is that it virtual. A virtual topology is built on an existing, shared physical network infrastructure. However, different administrative bodies usually administrate the virtual topology and the physical network.

Why organizations need VPN because they can transmit sensitive information over the Internet without needing to worry about who might see it. Everything that goes over a secure VPN is encrypted to such a level that even if someone captured a copy of the traffic, they could not read the traffic. Further, using a secure VPN allows the organization to know that an attacker cannot alter the contents of their transmissions, such as by changing the value of financial transactions.

Another reason is the mobility of today's workforce. Many organizations are increasing employee's productivity by equipping them with portable computing facilities. Affordable laptops and various palm-based devices have made it easy for people to work without being physically present in their offices. Weber *et al.* (2001) say that besides increased productivity, organizations are encouraging telecommuting to reduce their investments in real estate. Also, it reduces traffic and pollution from automobiles.

2.1 Common Services of VPN

Halpern (2001) explains that Interconnect VPN services help to interconnect local area networks located at multiple geographic areas over the shared network infrastructure. Typically, this service is used to connect multiple geographic locations of a single company. Several small offices can be connected with their regional and main offices. This service provides a replacement for the expensive dedicated links.

Ortiz (1997) defines that the Dial-up VPN service supports mobile and telecommuting employees in accessing the organization's Intranet from remote locations. The remote employee (user) dials into the nearest Remote Access Server (RAS, the technical term for modem pool). This is typically a local Point-of-Presence (PoP) of an Internet Service Provider (ISP) or the shared network infrastructure.

Mun Choon Chan *et al.* (1996) describes that an extranet VPN service combines the architecture of Interconnect VPN services and dial-in VPN services. This infrastructure enables external vendors, suppliers and customers to access specific areas of the organization's Intranet. The allowed specific area is denoted as the Demilitarized Zone (DMZ). When a supplier's representative connects to the organization's Intranet, either from the supplier's Intranet or dialing in remotely, the firewall and authentication mechanisms ensure that the connection is directed to the DMZ. A company employee or user, on the other hand, has full access to the organization's Intranet.

2.2 Basic VPN Requirements

There is one very important requirement that is common to secure VPN. Regardless of the type of VPN in use, a VPN is meant to have capabilities that the regular network does not. Thus, the VPN administrator must be able to know at all times what data will and will not be in the VPN. The following significant features must be supported by a VPN.

Enhanced Security: A dedicated network is generally viewed as secure simply because of its physical isolation and restricted usage. The openness of the Internet, on the other hand, produces a relatively insecure environment that cannot be trusted. An IP-based VPN overcomes the security limitations of a public network by applying mechanisms such as tunneling, access control, encryption, user authentication and data integrity to each separate group of users. These levels of protection can be tailored to each user's specific needs.

Performance Control: Because they have a private dimension, VPN must provide well-defined performance and quality characteristics, which can be managed using service level agreements and deployed with a clear distinctions among traffic classes. The fact that the underlying resources are shared becomes invisible to the user. Robust VPN will invoke mechanisms (such as bandwidth management, traffic classification and traffic queuing) in order to control performance at both the underlying trunk level and the individual VPN user level. The types of controls that can be applied can be defined for each individual VPN.

Service Flexibility: A dedicated network is limited by the very fact that it is physically defined -it has fixed capacity, fixed locations and limited configuration flexibility. Adding or deleting sites, installing new physical facilities, changing bandwidth or altering service agreements is time consuming and costly. A VPN, on the other hand, is more flexible since re-configuring the network can be as simple as changing software parameters, with no need to modify the physical network itself.

Ease of Application and Service Integration: Users on one network may need to access a variety of applications or services on different VPN both within and external to the organizations. Because VPN is standards-based, users on one network with the proper permissions and security capabilities can connect to other networks of trading partners and even communicate across different service provider boundaries.

Cost Savings: In addition to the fundamental cost savings associated with using the Internet, sharing network access links to reach many different VPN and non-VPN sites can result in a network that is less expensive to build, operate and administer than an equivalent set of discrete networks. Outsourcing the VPN to a service provider can produce even greater savings.

2.3 VPN Protocols

Security in a VPN is achieved through tunneling. Tunneling is the encapsulation of a message packet within an IP packet for transmission across the Internet with the encapsulated packet is stripped from the IP packet at the receiving network to get the original message packet.

The most popular tunneling protocols for VPN are: PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), and IPSec (IP Security).

2.3.1 PPTP (Point-to-Point Tunneling Protocol)

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a virtual private network (VPN) across TCP/IP-based data networks. PPTP supports on-demand, multi-protocol, virtual private networking over public networks such as the Internet.

Anderton (1993) explains that the networking technology of PPTP is an extension of the remote access Point-to-Point protocol defined in the document by the Internet Engineering Task Force (IETF) titled "The Point-to-Point Protocol for the Transmission of Multi-Protocol Datagrams over Point-to-Point Links," referred to as RFC 1171. PPTP is a network protocol that encapsulates PPP packets into IP datagrams for transmission over the Internet or other public TCP/IP-based networks. PPTP can also be used in private LAN-to-LAN networking.

2.3.2 L2TP (Layer 2 Tunneling Protocol)

Patton *et al.* (2000) explain that the layer Two Tunnel Protocol (L2TP) is an emerging Internet Engineering Task force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer 2 forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP) [5]. L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for VPN.

PPP defines an encapsulation mechanism for transporting multiprotocol packets across layer 2 (L2), point-to-point links. Typically, a user obtains a L2 connection to a Network Access Server (NAS) using one of a number of techniques (dial-up, ISDN) and then runs PPP over that connection. In such a configuration, the L2 termination point and PPP session endpoint reside on the same physical device.

L2TP extends the PPP model by allowing the L2 and PPP endpoints to reside on different devices Interconnected by a packet-switched network. With L2TP, a user has an L2 connection to an access-concentrator and the access-concentrator then tunnels individual PPP frames to the NAS. This allows the actual processing of PPP packets to be divorced from the termination of the L2circuit.

L2TP uses UDP messages over IP internetworks for both tunnel maintenance and tunneled data. L2TP therefore uses message sequencing to ensure the delivery of messages. L2TP supports multiple calls for each tunnel. To identify the tunnel and a call, there is a Tunnel ID and Call ID in the L2TP control message and the L2TP header for tunneled data.

2.3.3 IPSec (IP Security)

IP Packets have no inherent security. It is relatively easy to forge the addresses of IP packets, modify the contents of IP packets, replay old packets, and inspect the contents of IP packets in transit. Therefore, there is no guarantee that IP datagrams received are (1) from the claimed sender (the source address in the IP header); (2) that they contain the original data that the sender placed in them; or (3) that the original data was not inspected by a third party while the packet was being sent from source to destination. IPSec is a method of protecting IP datagrams.

IPSec is designed to provide interoperable, high quality, cryptographically based security for Internet protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). The set of security services offered includes access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/ or upper layer protocols.

Yurcik and Doss (2001) defines that the IPSec protocols-AH (Authentication Header) and ESP (Encapsulating Security Payload)-can be used to protect either an entire IP payload or the upper-layer protocols of an IP payload. This distinction is handled by considering two different modes of IPSec. Transport mode is used to protect upper-layer protocols; tunnel mode is used to protect entire IP datagrams. In transport mode, an IPSec header is inserted between the IP header and the upper-layer protocol header; in tunnel mode the entire IP packet to be protected is encapsulated in another IP datagram and an IPSec header is inserted between the outer and inner IP headers. Both IPSec protocols, AH and ESP, can operate in either transport mode or tunnel mode.

3. ADVANTAGES OF VPN

The services provided by a VPN platform must exhibit the reliability, scalability and manageability that are required for any large scale IP VPN solution. This means VPN functions should be implemented in a consistent and coordinated manner, using a tightly integrated IP-based system architecture that is designed for high performance packet processing. In addition to raw performance, the VPN platform must support flexible service definitions and controls that allow each specific type of application to be accommodated. Choosing an integrated platform that offers sustained performance, high availability, ease of management and superior price/performance is the obvious answer for both enterprise users and service providers.

An Integrated VPN platform offers a number of important benefits:

Reliability: Early VPN implementations were assembled from many separate internetworking devices, including routers, bandwidth managers, gateways and firewalls. Unfortunately, component based systems introduce additional points of failure that are often hard to avoid (or at least are expensive) and which reduce overall reliability.

If any one of these components fails, the entire communication path may be lost or severely compromised. Combining all the necessary VPN functions into a single box and adding advanced redundancy features (such as multi-homed connections and reliable router recovery mechanisms) is a far more robust solution.

Technical Integration: Discrete components need to be chained together to create a complete VPN solution. This can lead to technical problems such as increased latency and performance mismatches that compromise the scale of the entire solution. The use of multiple components often leads to a multi-vendor environment in which device interoperability may not have been fully tested. An integrated platform in which all of the functions are engineered to work together is less likely to have compatibility problems.

Scalability: Close integration of security, routing, and QoS functions allows the network to scale to larger sizes than would be possible if separate components were required. Configuration complexities are reduced as functions are naturally integrated and supported by a single user interface. Advanced features such as integrated routing further reduce complexity by allowing, for example, the use of such as dynamic routing to discover the secure tunnels that are available to a VPN user.

Management Simplification: Discrete single function components can also add considerable complexity to the operation and management of the VPN. Different support systems would need to be learned and coordinated for each of the components. Reducing the number of separate configuration tasks will eliminate errors that cause outages. An integrated management system can eliminate configuration mismatches, lack of alarm correlations, etc. Complications also arise when the distinct devices have different owners or administrators. An integrated VPN platform, with a similarly integrated element management system, allows a simpler and more powerful network management framework.

Cost Savings: Combining multiple devices onto a single platform also reduces the total hardware and software cost. Integration of packaging and power supplies reduces duplication and allows common tasks and data to be shared. Inter-component interfaces can be eliminated (or at least can be built directly into the software). An integrated VPN platform also requires less physical space, less power and less cabling, all of which result in lower total cost of operation. An integrated platform will also be covered by a single vendor's support and maintenance contract, providing the savings from "one-stop shopping."

4. DISADVANTAGES OF VPN

It is a known fact that remote access VPNs can be a devastating weak point in perimeter security. To permit VPN traffic, organizations must open an access point through their firewall. Remote access VPNs lack strong user authentication. As a consequence, user identity is not positively authenticated before access is permitted through the VPN gate.

Most VPNs verify user identity with only a reusable static password, or some use a digital certificate protected by a password. These approaches offer only marginal security because passwords are frequently compromised due to a multitude of reasons. When this happens, privacy is jeopardized and corporate information is at risk of exposure, theft, and misuse.

There are some concerns with VPN solutions are often raised.

VPN require an in-depth understanding of public network security issues and taking proper precautions in VPN deployment.

The availability and performance of an organization's wide-area VPN (over the Internet in particular) depends on factors largely outside of their control. VPN technologies from different vendors may not work well together due to immature standards.

VPN need to accommodate protocols other than IP and existing (legacy) internal network technology.

5. VPN MANAGEMENT

As organizations build larger and larger VPN, they are faced with a chore that grows with the networks: effective management. It's an important issue to pay attention to because a good VPN management platform is not just a matter of convenience; it can also save organizations money.

With all networks, the complexity of management and its costs increase with the number of devices, and this is also true with VPN, perhaps even more so. Each site connected to a VPN must have gear that secures traffic before it crosses the Internet or some other public IP network that is being used as the VPN backbone.

Major management challenges have included the time, cost and expertise required to create large numbers of secure tunnels between participating sites or between a central site and large numbers of remote clients. Each pair of subnets that needs to communicate securely over the Internet must have a secure tunnel defined. As an example, a large corporation might require the sales departments in each major large city to be interconnected in a full mesh configuration, with potentially hundreds or thousands of separate tunnels. Manual or semi-automated VPN design techniques require expert network designers, are quite time consuming and are prone to error. Moves, adds and changes can add considerably to the overall workload and can be disruptive to the service. For a large network, the management overhead can easily outweigh the advantages of implementing VPN technologies. Similarly, the process of creating, distributing and managing tunnel parameters at remote clients is complex.

Another management challenge is to ensure accuracy and consistency in matching user requirements (as expressed by the service level agreement) to VPN profiles. At its simplest, the source and destination VPN configurations must be compatible and loading them into the access nodes must be coordinated. Integrating the access nodes with QoS controls that are available within the network adds additional complexity, especially in a multi-vendor environment.

Centralized, policy-based management systems can dramatically reduce the time it takes to design and deploy a VPN-based infrastructure. By providing central control over VPN provisioning, new users and sites can be added (or modified) quickly and efficiently with much less chance of error than would otherwise be possible. This increases the scale of operations and range of customers that can be handled by a VPN administrator (and hence the profitability of a managed service). In general, the level of expertise required is also reduced since many of the configuration rules can be embedded in the policy workstation.

6. CONCLUSIONS

Network security is increasing in importance for organizations of all sizes. Whether to protect information in transit in remote access sessions, branch network connections, or internal networks, solutions for this form of security are essential. This paper takes security seriously and is working on a number of initiatives to provide the advantage of Virtual Private Network (VPN).

VPN technologies are designed to provide the appearance of a dedicated network despite the use of shared resources for physical connectivity. IP-based VPN offer a standard way to exploit the benefits of the public Internet without compromising on the security, reliability and performance that are delivered from dedicated networks. VPN open up new opportunities for implementing e-business applications, for extending customer access worldwide, and for connecting remote

employees to corporate resources. The deployment of VPN is expected to be a major enabler for business use of the Internet. This paper described how effectively a secure solution could be implemented by providing VPN services and protocols.

REFERENCES

[1] Anderton, S. (1993) "Issues for VPN users". Virtual Networking, IEEE Colloquium, London, UK, 3/1-3/6.

[2] Baukari, N. and Aljane, A. (1996) "Security and auditing of VPN". Services in Distributed and Networked Environments Proceedings of Third International Workshop, Macau, 132-138.

[3] Braun, T., Guenter, M., & Khalil, I. (May 2000) "IP-Oriented Operations and Management: Management of Quality of Service Enabled VPNs". Institute of Electrical and Electronics Engineers (IEEE) Communications Magazine, 90-98.

[4] Halpern, J. (2001) "SAFE VPN IPSec: Virtual Private Networks in Depth".

Accessed August 2, 2002. <http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm>

[5] Kyte, S. (1993) "Global virtual private networks". Virtual Networking, IEEE Colloquium, London, UK, 5/1-5/5.

[6] Liang, H., Kabranov, O., Makrakis, D., and Orozco-Barbosa, L. (2002) "Minimal Cost Design of Virtual Private Networks". Proceedings of the 2002 IEEE Canadian Conference on Electrical & Computer Engineering, 3, 1610- 1615.

[7] Ortiz (1997) "Virtual Private Netoworks: leveraging the Internet". Computer, Vol. 30, 18-20.

[8] Microsoft (n.d.) "Virtual private network (VPN) connections overview". Accessed July 15, 2002. <http://www.microsoft.com/windowsxp/home/using/productdoc/en/default.asp?url=/WINDOWSXP/home/using/productdoc/en/Conn_VPN.asp?frame=true>

[9] Mun Choon Chan, Hadama, H., and Stadler, R. (1996) "An architecture for broadband virtual networks under customer control". Network Operations and Management Symposium, IEEE, Kyoto, Japan, 1, 135-144.

[10] Xiangping Chen, Mohapatra, P. (2002) "Performance Evaluation of Service Diffrentiating Internet Services". Computer, IEEE Transactions, Vol. 51, 1368-1375.

[11] 3Com (n.d.) "Technical Paper: Virtual Private Networking". Accessed June 7, 2002. <http://www.3com.com/corpinfo/en_US/technology/tech_paper.jsp?DOC_ID=5349>

[12] Venkateswaran, R. (February/March 2001) "Various Services and Implementation Scenarios: Virtual Private Networks". Institute of Electrical and Electronics Engineers (IEEE) Potentials, 11-15.

[13] Weber, S., Oppliger, R., and Hogrefe, D. (1992) "An optimization method for virtual private network design". Private Switching Systems and Networks, Second International Conference, London, UK, 31-36.

[14] Younglove, R.W. (2001) "IP security: what makes it work?". Computing & Control Engineering Journal, Vol.12, 44-46.

[15] Patton, S., Smith, B., Doss, D., and Yurcik, W. (2000) "A layered framework strategy for deploying high assurance VPNs". High Assurance Systems Engineering, Albuquerque, NM, USA, 199-202.

[16] Yurcik, W. and Doss, D. (2001) "A planning framework far implementing virtual private networks". IT Professional, 41-44.