Analyzing and Categorizing Virtual Private Networks to Overcome Security Issues

Suresh C
Department of computer science, Ganadipathy Tulsi's Jain Engineering College.

Abstract – The term VPN has been associated in the past with such remote connectivity services as the (PSTN), Public Switched Telephone Network but VPN networks have finally started to be linked with IP-based data networking. Before IP based networking corporations had expended considerable amounts of time and resources, to set up complex private networks, now commonly called Intranets. These networks were installed using costly leased line services, Frame Relay, and ATM to incorporate remote users. For the smaller sites and mobile workers on the remote end, companies supplemented their networks with remote access servers or ISDN. Today's VPN solutions overcome the security factor using special tunneling protocols and complex encryption procedures, data integrity and privacy is achieved, and the new connection produces what seems to be a dedicated point-to point connection. And, because these operations occur over a public network, VPNs can cost significantly less to implement than privately owned or leased services. Although early VPNs required extensive expertise to implement, technology has matured to a level where deployment can be a simple and affordable solution for businesses of all sizes.

Index Terms – Virtual private network, secure tunnel.

1. INTRODUCTION

Virtual Private Network is a type of private network and uses public telecommunication, such as the Internet, instead of leased lines to communicate. By the simplest definition, a network consists of two computers connected by a physical medium. However, networks can be implemented privately or publicly. VPNs use the Internet as the medium and create a secure "tunnel", which will be explained in further detail later. It is an inexpensive form of Wide Area Networks (WANs) and companies most commonly use private networks for employees who work at home or at another location so they can remotely access the organization. Businesses look into VPNs because of the higher level of cost savings and flexibility that VPNs provide over traditional dedicated leased lines or frame-relay circuits. The most essential characteristic to businesses is that the implementation of VPNs reduces costs tremendously. The growth of telecommuters increases the cost for modem banks, remote-access servers, and phone charges. However, these workers can connect to their company's network by dialing into the POP of a local ISP, thus reducing long distance charges, costs of installing and maintaining the banks of modems at corporate sites, and costs of leasing or building dedicated lines. The specific implementation discussed - Remote Access VPNs - uses specialized software on a client computer to initiate encryption and tunneling. It can also depend on the service provider. The software employs encryption protocols such as IPSec, L2TP, PPTP, and SOCKS to allow the service provider to be a secured transporter for the data. Businesses can also outsource to service providers to provide VPN configurations (Dennis).

2. VPN TOPOLOGY

Most VPNs rely on tunneling to create a private network that reaches across the Internet. Essentially, tunneling is the process of placing an entire packet within another packet and sending it over a network. Tunneling allows senders to encapsulate their data in IP packets that hide the underlying routing and switching infrastructure of the Internet from both senders and receivers. At the same time, these encapsulated packets can be protected against snooping by outsiders using encryption techniques. Tunnels can consist of two types of end points, either an individual computer or a LAN with a security gateway, which might be a router or firewall. Only two combinations of these end points, however, are usually considered in designing VPNs. In the first case, LAN-to-LAN tunneling, a security gateway at each end point serves as the interface between the tunnel and the private LAN. In such cases, users on either LAN can use the tunnel transparently to communicate with each other. The second case, that of client-to-LAN tunnels, is the type usually set up for a mobile user who wants to connect to the corporate LAN. The client, i.e., the mobile user, initiates the creation of the tunnel on his end in order to exchange traffic with the corporate network. To do so, he runs special client software on his computer to communicate with the gateway protecting the destination LAN.

3. FLOW OF ENCAPSULATION AND ENCRYPTION

If a business decides to implement a VPN, it must first lease a high-speed circuit from an ISP or common carrier that supports the preferred access rate and access technology for each location. Since it would be too costly to have VPN hardware on the sender or client's side, the VPN hardware usually resides with the ISP. Take the scenario of an employee accessing secure files on a corporate network. When a client sends a message, each packet of information is encoded with no VPN protocols. Once the packet reaches the ISP's access server, the packet is sent to a VPN device. The device encapsulates or

surrounds the existing packet that already has Application layer, Transport layer, Network layer, and Hardware layer frames encapsulating the primary message. In this scenario, it is assumed that the message is a file being sent through a dial-up connection, using FTP (File Transfer Protocol), to the corporation's file server. Thus, the application layer adds a FTP segment, transport layer adds a TCP (Transmission Control Protocol) segment, network layer frame adds an IP (Internet Protocol) segment, and the data link layer frame adds a PPP (Point-to-Point Protocol) segment, respectively. In this example, it is also assumed that L2TP is used to encrypt the data.

Once the packet reaches the ISP, the VPN device attaches the L2TP segment to the existing frame. At this point, the packet must be surrounded with the destination VPN device's address. Since this example uses IP as the network layer to identify the destination, an additional IP segment is added onto the packet. Finally, a segment indicating the type of high-speed medium used is attached. This could be a frame for a T1, T3, or OC circuit, each of which has its own data link protocol. At this point, the Internet comes into play in that the newly encrypted packet is sent over the Internet to the corporate office's FTP server. In effect, a tunnel is created since the process simulates a private packet-switched network. However, before the FTP server can understand the message, the packets must be decrypted by the destination VPN device. The device strips the high-speed medium's data link frame off the packet and the IP frame to determine whether or not the IP address matches its own. Then the device strips off the VPN protocol frame. Thus, upon removing L2TP from the packet, the packet is now decrypted and can be read by the FTP server. The FTP server follows the same process the client computer originally used, but in reverse. The file the client sent is now stored on the server (Dennis). It is essential to note that in this scenario, since a dial-up line is used, the employee's side does not necessarily have to have VPN software on its side; POTS (Plain Old Telephone Service) gives a private, dedicated connection between the client's home and the ISP. If the client had used a cable modem or DSL service to establish a VPN connection between their side and the corporation's servers, the employee would have to have a VPN client installed in the form of software. This would create a hybrid VPN connection in that the employee would have VPN software installed and the ISP would have VPN hardware.

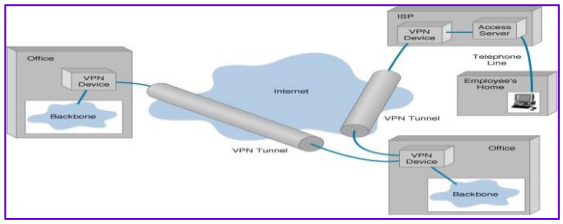

Fig. A macro view of the new VPN connectivity

4. VPN DEVICE TYPES AND THEIR ATTRIBUTES

A VPN can be implemented in three ways – Firewall-based, hardware-based, or software-based. Firewall based VPNs focus on the security aspects of Firewalls. In general, firewalls provide filters to block certain network traffic, ultimately denying certain sources from entering an intranet. Firewall-based VPNs also perform network address translation, provide strong authentication, and offer real-time alarms and extensive logging of activity. Apparently, most commercial firewall vendors "harden" the host operating system by stripping the OS system kernel of dangerous and unnecessary services. In effect, this bolsters the security of the VPN server. Often, the VPN firewalls are routers as well, thus serving as a dual-purpose hardware device. Furthermore, this is a cost-effective solution since there is no need for a separate, stand-alone router.

Hardware-based VPNs are usually encrypting routers in that they encrypt outgoing data and decrypt incoming data. They are often designed as plug-and-play devices, thus attributing both security and ease-of-use to them. The big plus is that they provide the highest network throughput of all VPN systems. However, that positive attribute comes with hefty price tag, generally making it the most expensive VPN solution. Another negative is that they are not as flexible as Software-based systems. Software-based VPNs are ideally suited for environments in which the two end points of the VPN communication are not controlled by the same organization. For example, client support or business partnerships would find this flavor of VPNs especially fitting. Another scenario in which software-based VPNs might be applied is when different firewalls are implemented within the same organization. The nature of software provides programming to normalize itself for diverse operating environments. However, these systems experience lower performance than hardware-based VPNs leaving Software-based VPNs the solution only when efficiency is not a heavy requirement. Furthermore, the benefit of versatility comes with its drawbacks. To be implemented, an IT staff is required to be familiar with the host operating system, the application itself, and appropriate security mechanisms (i.e. – PPTP or L2TP). Some software VPN systems require changes to routing tables and network addressing schemes. The latter can significantly lower productivity in labor and increase labor costs. Thus, the attributes businesses must consider when determining a type of VPN device to use are the following: cost, efficiency, flexibility, and functionality. Firewall-based VPNs offer the most functionality; hardware-based VPNs offer the highest efficiency; Software-based VPNs offer the most flexibility and lowest cost.

5. REMOTE ACCESS VPN

Remote Access VPNs permit secure, encrypted connections between mobile or remote users and their corporate networks via a third-party network, such as a service provider. The

client-to-LAN VPN application sends remote user traffic over the user's Internet connection. The advantage is that the remote user can make a local call to an Internet Service Provider, as opposed to a long distance call to the corporate remote access server. This solution is ideal for a telecommuter or mobile sales people. At the same time, VPN allows mobile workers, telecommuters and day extenders to take advantage of broadband connectivity. With the beginning of affordable broadband technologies, small and medium sized businesses can now use the Internet and Virtual Private Networking to bypass expensive, traditional WAN and remote access connections. With VPN solutions a company can tap into the benefits of remote access without the high cost and complex technical infrastructure. Here are some examples of typical VPN applications.

Site-to-Site VPNs extend the classic Wide Area Networks by providing large-scale encryption between multiple fixed sites such as remote offices and central offices, over a public network, such as the Internet. VPNs do not inherently change private WAN requirements, such as support for multiple protocols, high reliability, and extensive scalability, but instead meet these requirements more cost-effectively and with greater flexibility. The LAN-to-LAN VPN application sends network traffic over the branch office Internet connection, instead of relying on dedicated leased line connections. This can save thousands of dollars in line costs and reduce overall hardware and management expenses. The intranet VPN is a type of site-to-site network that "provides virtual circuits between organization offices over the Internet" (Dennis 209). The extranet VPN is also a type of site-to-site network that links various businesses in a particular supply chain, both vertically and horizontally. Finally, the most talked about throughout these discussions is the access VPN that enables employees to access an organization's networks from a remote location.

6. FUTURE OF VPN

Where do we see Virtual Private Networks going in the future? As far as its appeal to the public it varies substantially. Questions arise of whether businesses need to switch or implement a VPN due to a decrease in the costs of long distance or leased lines. At this point, why would the company want to switch its network when expenses have gone down? Also, companies may worry whether or not their current networks are application friendly if they were to switch to a VPN. If not, factors to consider would be additional costs of the conversion, and if it would be worth the expenses. Furthermore, as VPNs are growing, they are becoming more complex, thus, increasing costs for training. All these lead to hidden costs for the VPN technology, which may hinder the success of a VPN. However, we should expect VPNs to strengthen its standards and products and correct its flaws to avoid these uncertainties.

Despite all the doubts, VPN will continue to grow and improve to make VPN dominant in the market; thus, giving companies no choice but to switch. VPN providers along with Internet providers continue to view different aspects possible to be able to make any necessary improvements, and also help VPN clients be comfortable with the new technology. As stated in InformationWeek.com, "…GTE Internetworking, incumbent providers such as Bell Atlantic Corp. and MCI WorldCom…have stepped in to help companies handle VPN activation, security, and management" (By: Terry Sweeney). A case from Internetweek.com speaks of a VPN provider, Equant NV, enhancing their IP VPN by adding a service designed for video traffic, which is directed at large enterprises "that are cutting back on business travel but still want employees to interact regularly with distant colleagues." Furthermore, as the VPN market becomes larger, more applications will be created along with more VPN providers and new types of VPN. For instance, The University of Rochester is using a VPN provided by Information Technology Services (ITS).

The future should also expect networks to converge to create an integrated VPN to fit the many different industries that will soon enter the market. Since majority of VPN users are currently large companies, smaller companies should begin to join the trend due to the increasing variety of VPNs to choose from. Also, designing improved protocols will also improve VPNs. The flexibility and performance of VPNs would then improve also by reducing protocol or data traffic in the tunnels and customizing the ISP to work more closely with individual business needs since system reliability is dependent on these ISPs. With all these improvements in mind, we should expect a considerably rapid growth of the market for VPN in the future.

7. CONCLUSION

No matter how secure a company's network is, hackers will still look for vulnerabilities, especially when it comes to virtual private network (VPN) connections. Often, hackers will try to "piggyback" onto an existing VPN connection that a remote worker has established, either inserting viruses into a system or removing and viewing sensitive files. Signing on with a VPN provider that features its own asynchronous transfer mode (ATM) backbone is one way to circumvent hackers. Virtual private networks have generated their share of security concerns, but the focus has been primarily on flaws in VPN protocols and configurations. Although those issues are important, the most significant security threat in any VPN setup is the individual remote telecommuter making a VPN connection from home or an employee on the road with a laptop and the ability to connect to the corporate office via VPN. Therefore even though VPN offers cost effectiveness by eliminate long distance charges, it is not a 100% secure technology to fully trust on. It has its obvious tradeoffs.

VPN is an emerging technology that has come a long way. From an insecure break off of Public Telephone networks to a powerful business aid that uses the Internet as its gateway.

VPN's technology is still developing, and this is a great advantage to businesses, which need to have technology that is able to scale and grow along with them. With VPN businesses now have alternative benefits to offer to their employees, employees can work from home, take care of children while still doing productive, and have access work related information at anytime. VPN will also help to make the possibility of a business expanding its services over long distances and globally, more of a reality.

REFERENCES

[1] Goldberg, R., Architectural Principles for Virtual Computer Systems. 1973, Storming Media.
[2] Barham, P., et al., Xen and the art of virtualization, in Proceedings of the nineteenth ACM symposium on Operating systems principles. 2003, ACM Press: Bolton Landing, NY, USA.
[3] Kivity, A., et al. kvm: the Linux virtual machine monitor. 2007.
[4] Bellard, F. QEMU, a fast and portable dynamic translator. 2005: USENIX.
[5] Victoria, B., Creating and Controlling KVM Guests using libvirt. 2009, University of Victoria.
[6] Yu, J. Performance Evaluation on Linux Bridge. 2004.
[7] McLennan, M. and R. Kennell, HUBzero: A Platform for Dissemination and Collaboration in Computational Science and Engineering. Computing in Science & Engineering, 2010.
[8] Feitelson, D.G., The supercomputer industry in light of the Top500 data. Computing in Science & Engineering [see also IEEE Computational Science and Engineering], 2005.

Authors

Suresh C was born in Vellore, India, in 1990. He received the B.E. degree in computer science and engineering from Kings Engineering College, Chennai. He currently pursuing M.E degree in computer science and engineering from Ganadipathy Tulsi's Jain Engineering College, Vellore. His current research interests include cloud computing, enterprise application, big data, networking and software engineering.