2014

Creating VPN's with IPsec

SPRING ENTERPRISE INFO SECURITY 4040/601

WILSON CHANCE HINCHMAN

This paper will define the term VPN, explain for what and why VPNs are used. IPsec, which is vital to the functionality of VPNs will also be touched on. I will start by defining the term VPN, the acronym VPN stands for "Virtual Private Network". This is an ambiguous term that gets thrown around a lot in the information technology industry. Many types of networks fall under the classification of virtual private network when taken out of context. For instance, frame relay networks, or private point to point WAN links could be considered virtual private networks. After all, there is no such thing as a purely nonvirtual network. ''A VPN doesn't necessarily mean communications isolation, but rather the controlled segmentation of communications for communities of interest across a shared infrastructure.''[1] That being said, the current characterization of a VPN is the use of IPsec to build a private and secure tunnel over the public internet. ''VPNs generally address two different needs. The first is the need to allow users to connect to a private network with an encrypted connection through some untrusted medium, such as the Internet or a wireless LAN (WLAN).''[2] ''The second VPN need is to create an encrypted point-to-point connection between two different networks over some untrusted medium. Whereas remote-access VPNs use a client-server model, point-to-point tunnels use a peer-to-peer model.''[2] So the two main applications for virtual private networks are site to site communications and remote access communications. Point to point virtual private networks connect two or more privet networks (see Figure 1.) while remote access VPNs allow one or more remote systems to connect to a secure network. (see Figure 2.) Both of these configurations use secure tunneling which is negotiated using the IPsec protocol sweet. These two distinct types of secure communication through the use of virtual private networks are

most often used in conjunction with one another to secure and extend the functionality of networks.

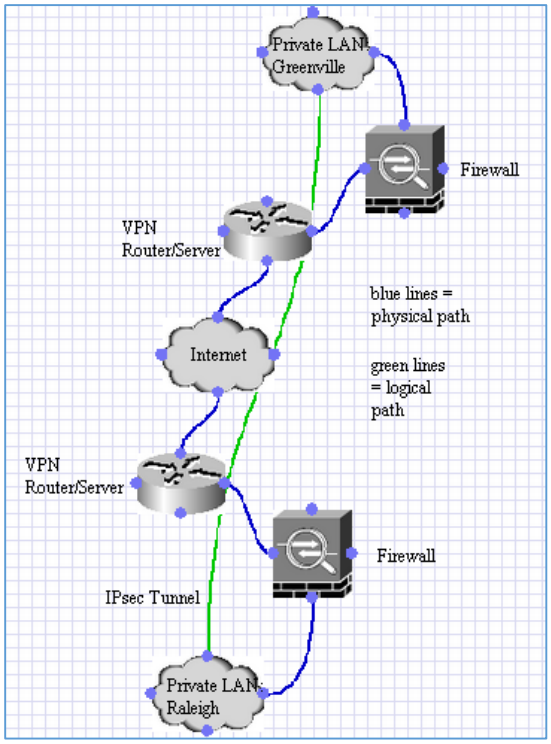

Figure 1. Point to Point VPN

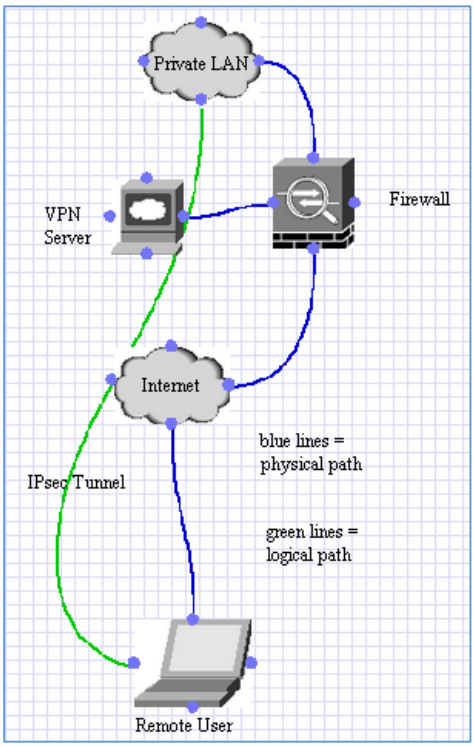

Figure 2. Remote access VPN

Now that we have been over what a virtual private network is and what it is used for what makes a VPN any better than other private network solutions? There are many reasons. Though cost, availability, flexibility, and security are at the top of the list and these are the selling points that will be covered in this paper. “The base motivation for VPNs lies in the economics of communications. Communications systems today typically exhibit the characteristic of a high fixed-cost component, and smaller variable-cost components that vary with the transport capacity, or bandwidth, of the system.” [1] It is much less expensive for a corporation to use the existing infrastructure of the World Wide Web than it is to lay its own fiber and create an

infrastructure form the ground up. Only the upper tier of businesses would have the capital to make this type of internetwork a reality and even if they have the means this type of strategy is no longer a viable solution. A decade ago the benefits of this type of infrastructure might outweigh the cons but in today's world of high speed cost effective internet it is much more practical for the majority of businesses to outsource the infrastructure to internet service providers and use IPsec to build very secure VPN over the public internet. The progression of speed and reliability that we have seen in the sector of public internet has prompted a surge in VPN technology that shows no signs of slowing. Virtual private networks are also a very flexible solution. When using frame relay "also known as leased lines" a company must pay an internet service provider on a fixed schedule for each reserved line. If additional lines are needed or changes to the existing infrastructure is required then there are additional charges. Though VPNs allow for many to many connections and these connections can be configured indefinitely with no additional increase in price. Also through remote asses configuration of the VPN employees are able to access corporate network form anywhere that the internet is available. Though the use of IPsec, virtual private networks are heavily encrypted. "There are several motivations for building VPNs, but a common thread is that they all share the requirement to "virtualize" some portion of an organization's communications—in other words, make some portion (or perhaps all) the communications essentially "invisible" to external observers, while taking advantage of the efficiencies of a common communications infrastructure." [1]

We will now touch on IPsec. "The IPSec protocol, which really is a set of security headers in the Internet Protocol (IP) v6 back-ported to IPv4, is the most open, powerful and secure VPN protocol." [2] "IPsec is actually a suite of protocols, developed by the IETF (Internet Engineering

Task Force), which have existed for a long time." [4] Additional protocols are can be, and are added as needed. What makes IPsec so secure is its ability to authenticate data, maintain data integrity, insure data confidentiality, and prevent data replay. Just as the TCP/IP protocol suite has sub protocols such as TCP, UDP, FTP, HTTP, and exedra. IPsec resides inside of the TCP/IP suite and has its own set of protocols such as AH, DES, MD5, DH1, and exedra. IPsec was designed as a shell for these protocols so that it could be modular, flexible, and sustainable. IPsec is a shell, this shell has "empty slots" these slots can be filled with whatever protocols that fit the current need. Not only that but the slots themselves are inter changeable. This is the engine of IPsec. There are two main modes of communication via IPsec; transport mode and tunnel mode. In transport mode IPsec encrypts all data from the transport layer and above while all data in the network layer and below remains in clear text. (see Figure 3.) Transport mode is ideal for use in internal networks because of this. Keep in mind that the vast majority of hacking attempts are made from inside of internal networks. VPNs using IPsec in transport mode can effectively stop attackers from packet sniffing production network traffic in the local area network. In regards to this paper IPSec's primary use is the creation of virtual private networks via the negotiation of secure tunnels. "Tunneling is a technique that encapsulates the packet header and data of one protocol inside the payload field of another protocol. This way, an encapsulated packet can traverse through networks it otherwise would not be capable of traversing." [4] In tunnel mode IPsec encrypts all data from the network layer and above. (see Figure 4.) This makes tunnel mode ideal for wide area networks. When a data packet transverses through a gateway in tunnel mode IPsec adds a new IP header. In this new header the private IP address is encrypted and the public address is added as the new IP header. Once

the packet traverses the public network IPsec then strips off the added public header and unencrypts the private IP header. This is the mile high version of how the IPsec tunneling described in this paper operates.

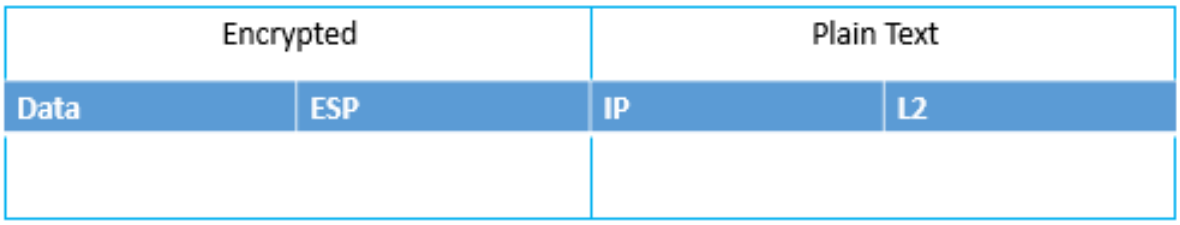

Figure 3. Transport Header

Figure 4. Tunnel Header

IPsec has many benefits. When IPsec is implemented on a firewall or router it can effectively secure all traffic crossing the network without incurring high processor overhead. Since IPsec is below the transport layer (TCP, UDP) it is not seen by the application layer. Because of this there is no need to update software on servers or workstations when IPsec is implemented on a boarder device. Even when IPsec is implemented in a networks firewalls and or routers, application layer software is not effected. IPsec is transparent to the end user. Their for, there is no need to train users on new security policy, distributing user keys, or updating user keys when employees leave the company." [5] IPSec can provide secure VPN access for individual users or entire sites as illustrated in (Figure 1.) and (Figure 2.). These features coupled with IPSec's ability to adapt to change insures that IPsec will be securing our virtual private networks for years to come.

Works Cited

*[1]Bauer, M. (n.d.). *Linux Journal.* Retrieved from Paranoid Penguin - Linux VPN Technologies: http://www.linuxjournal.com/article/7881

*[2]Paul Ferguson, Cisco Systems and Geoff Huston, Telstra. (n.d.). *The Internet Protocol Journal - Volume 1, No. 1.* Retrieved from What Is a VPN? - Part I: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/what_is_a_vpn.html

*[3]Paul Ferguson, Cisco Systems and Geoff Huston, Telstra. (n.d.). *The Internet Protocol Journal - Volume 1, No. 2.* Retrieved from What Is a VPN - Part II: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-2/what_is_a_vpn.html

*[4]Rosen, R. (n.d.). *Linux Journal.* Retrieved from Creating VPNs with IPsec and SSL/TLS: http://www.linuxjournal.com/article/9916

*[5]William Stallings. (n.d.). *The Internet Protocol Journal - Volume 3, No. 1.* Retrieved from IP Security: http://www.cisco.com/web/about/ac123/ac147/ac174/ac197/about_cisco_ipj_archive_article09186a00800c830b.html