

SE 4C03 Winter 2005
VPN Technology:
A Method to Secure Transmissions over the World Wide
Web

Researcher: Yasemin Hassan
Student Number: 0048576
Revised: April 5, 2005

SE 4C03 Winter 2005
VPN Technology:
A Method to Secure Transmissions over the World Wide Web

Researcher: Yasemin Hassan

Revised: April 5, 2005

Introduction

With the vast conveniences of the World Wide Web, it is easily understandable why a company would take advantage of all its functions. One main and largely beneficial use of the Internet for an enterprise is the ability to transfer information between different locations. It could be the case that a corporation has multiple offices where communication is necessary amongst all branches or a large firm that employs sales representatives mobile within the field and need to connect to the company's private network from various remote locations.[3] Thus, it is of the utmost importance that corporations are accommodated with higher quality security. Not only is the amount of information passing enormous but the location where these transactions are established are not just within company headquarters making this idea of data transfer extremely alarming because private information is sent via the World Wide Web during these transactions. In any case, more and more companies are relying on the World Wide Web and assuming it is secure enough for confidential information to be exchanged so prominently. Two questions can be posed here, are these transfers safe and if so, what occurs to guarantee that the transfer does not expose information to potential eavesdroppers or hackers?

VPN Technology

Virtual Private Network (VPN) is a network which uses a public network to transfer information using secure methods.[4] This technology connects separate sites over the Internet and allows them to function as a single, private network. The information is sent through encrypted tunnels across the Internet but remain private during this transmission.[1,2] Our above two questions are partially answered through the definition of this type of software, using VPN can help make transfers safe and will not give outside intruders the opportunity to get a hold of data within the tunnel technology that VPN makes use of. Let us further investigate this concept with details of the types of VPN, VPN encryption and tunneling and firewalls and IPSec in conjunction with VPN, which are explained below.

Types of VPN

Two types of VPN technologies will be discussed, remote access and site-to-site VPN. Remote access VPN is a user to local area network (LAN) connection. This can apply in a number of cases, such as a student from home trying to access the McMaster network or an employee of a large corporation with hundreds of sales persons who needs access to the corporations' private internal network. Here highly confidential information regarding company statistics could be sent back and forth. How this is secured will be discussed further into this paper.

The other type of VPN is site to site, where multiple fixed sites over a public network such as the Internet are connected.[3] Here, remote locations (for example,

office buildings located in different areas) can be part of one private network that use a LAN to LAN connection.

In both the above cases, private data is being sent through the Internet. The next point of discussion is how information is secured before transmissions.

VPN Encryption

The data is first encrypted using either symmetric or public key encryption before being sent to another computer. Encryption is defined as the process of encoding data that will be sent from one computer to a recipient computer, which has the capacity to decode this information.

Symmetric key encryption, also referred to as secret key cryptography, involves one key.[1] The message or data, similarly called plaintext, needs to be sent to the recipient computer but initially needs to be turned into ciphertext with the use of the key. This key is an essential part of the encryption and decryption alike, both computers must have obtained copies of the secret key and this must be exchanged with extreme caution as any eavesdropper with access to this key and the algorithm could cause havoc on the exchanged personal information.[5] The different selections of algorithms will not be discussed as they are mainly for performing substitutions and permutations to the plaintext and ciphertext.[5]

Public key encryption, also referred to as asymmetric cryptography, involves two keys as opposed to one. Here, the sender and recipient both have a public and private key.[1] To encode the data the public key is used on the plaintext. Once the encrypted data is received, the ciphertext is turned into plaintext with the private key. With the public key, additional security is added since a digital signature can be generated. The private key “signs” the message and the public key verifies the “signature” on the other end.

Both encryption methods are widely used, however, public key encryption is a better method as there are less keys to share and the concept of the digital signature confirms that the message came from the intended party. Once the message is secured, the path to which the data will travel must be as well. Further investigation on tunneling technology that VPN is known for will be discussed.

VPN Tunneling

VPN relies on tunneling to create a private network that reaches across the Internet between a router at both ends.[2] It is the process of encapsulating a packet within another to forward datagrams over a network. To guarantee privacy, VPN encrypts each outgoing datagram before placing it in another packet for transfer through the tunnel. As described above, we see two examples of types of encryption that could be used. The network understands the outer packet but the inner packet cannot be decoded, as the key is exclusively available to the recipient and sender.

In order for the datagram to reach its destination, the outer packet has the IP address of the source router available, which is located at the beginning of the tunnel and the IP address of the destination router, which is located at the end of the tunnel.[2] If

this was not visible then the packet would be lost during transmission since the original source and destination are hidden within the inner packet.

Using Firewalls and VPN

The above discussion has given the reader the basic infrastructure of VPN. Using encryption and tunneling is the main portion of this technology, however there are other pre-existing security methods that enhance the VPN security system. Using these other devices, namely firewalls and IPSec, will only make transfers more reliable. Firewalls will be discussed within this section while IPSec will be further investigated below.

Although a firewall is a mechanism that is widely used on its own to protect resources of a private network from other users and networks, if used in conjunction with VPN it will increase the security capabilities of the VPN, as previously explained. A firewall works closely with a router program to filter network packets and then determine whether or not to forward these packets to their destination. By using Cisco's 1700 routers, which is a VPN product, they can be upgraded to include firewall capabilities. It is recommended that a good firewall be in place before incorporating the VPN technology into the existing network, however a firewall is not a necessity for VPN to do its job.[3]

Using IPSec and VPN

IPSec stands for Internet Protocol Security Protocol, it provides better encryption algorithms and a more extensive authentication system.[3] IPSec uses a transport mode and a tunnel mode. The transport mode adds on IPSec information between the IP header and the rest of the packet, where as tunnel mode adds on a new IP header and IPSec information outside of the existing packet.[1] Transport mode is used more often when the packet is sent from end to end. Tunnel mode is used if a packet is sent from firewall to firewall, so data is only secured through part of the tunnel.[1] Again, without use of IPSec, this will not hinder the security of the VPN, it will only make it better.

Conclusion

It can be seen that VPN is a necessary tool to protect against eavesdroppers and aid in securing data transmitted over the Internet. VPN is a flexible technology as its infrastructure is capable of accessing remote networks or to integrating different sites. The fact that VPN uses both encryption, which is done to convert personal information into ciphertext, along with tunneling, that is used to add extra security during transmission, makes VPN known as a high-speed performance and maximum-security technology.[7]

By combining the IPSec client and firewalls, VPN is able to control access to private information with the highest level of security for corporate networks. From Fortune 500 companies to hosted e-business sites, branch offices and finally to mobile or remote workers, VPN not only secures information over the Internet but it has secured itself in the industry and shown its success with revenues that doubled to \$706 million in 2001, which was up from \$313 million in 2000.[7]

References

- 1.Kaufman, Charlie, Perlman, Radia & Speciner, Mike. (2002). Network Security (2nd ed.). New Jersey: Prentice Hall.
- 2.Komer, D.E. (2000). Internetworking with TCP/IP (4th ed.). New Jersey: Prentice Hall.
- 3.How Stuff Works. (2005). How Virtual Private Networks Works. Retrieved April 5, 2005 from the World Wide Web:
<http://computer.howstuffworks.com/vpn2.htm>
- 4.McMaster University. (2005). Virtual Private Network (VPN) Service. Retrieved March 26, 2005 from the World Wide Web:
<http://www.mcmaster.ca/cis/network/vpn/>
- 5.Krishnan, Kartik. (2005). 4C03 Lecture Notes: Lecture 22-24 (pp. 1). Hamilton: McMaster University.
- 6.Krishnan, Kartik. (2005). 4C03 Lecture Notes: Lecture 22-24 (pp. 9). Hamilton: McMaster University.
7. Intranet Journal. (2005). VPNs: The Time Is Now? Retrieved April 5,2005 from the World Wide Web:
http://intranetjournal.com/articles/200110/vpn_10_03_01a.html