Measures of VPN Technology

Anurag Gupta
Assistant Professor, BBK DAV College for Women, Amritsar

Abstract

This paper provides a general idea of VPN and core technologies of VPN. The salient of this paper is to focus on need behind VPN technology (IPSec). With the changing requirements and advent of technology, a sense of wide coverage of network arises to encapsulate the data transfer needs with security enforcements. As the usage of internet is increasing constantly, all the possible techniques are being enforced to use this global network as a private and secured network for personal data transfer issues within a group or more. As no system is complete and flawless in itself, there is a need to fill the patches to incorporate every changing core requirements. The best possible effort has been made to suggest various remedial concepts to cope with vulnerabilities.

Indexing Keywords

VPN, IPsec, Security enforcements, Remedies.

Academic Discipline and Sub-Disciplines

Computer Science, Computer Networking.

Subject Classification

Data Communication

Type (Method/Approach)

Journals, Books.

INTRODUCTION

The technology of VPN (Virtual Private Network) makes the possible use of public infrastructure through security mechanisms and tunneling protocols. VPNs can be used to provide the security features of private leased line to the organization using shared public infrastructure (Internet) at much lower cost. Using VPN service, company need not to incur high cost for owning their own private networks for secured data transmission, rather, can use internet as their leased line for data and resource sharing. It means, VPN can be used as virtual private network for wide-level intranets as well as extranets. This shows that the technology of VPN provides a medium of protecting and reliably transmitting information over the Internet by allowing remote/end users to establish a virtual private "tunnel" to securely enter an internal network, accessing various resources, data and communications via an insecure network such as the Internet.

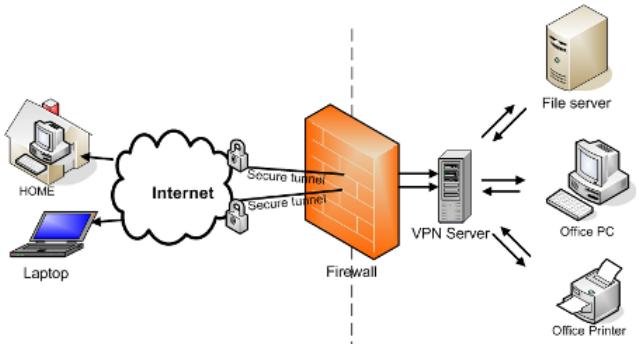

Fig. 1: (VPN for security, posted on fri, jun14,2013, by HobbitTR, retrieved from http://barrakam.com/vpn-for-security/)

Due to huge technology measures, VPNs are enormously popular with companies as a means of securing sensitive data when connecting remote data centers. Such networks are also becoming increasingly common among individual and remote users.

METHOD OF TRANSMISSION

VPN technology deals with transmission of data by means of **"Tunneling".** It is the process of forwarding data packets from one node to another within vpn in such a common way as if the two nodes are connected directly with each other. Tunneling is achieved by encapsulating the data by adding an extra IP header with an outgoing data packet from transmitting end and is forwarded by various intermediate nodes based on routing header information without taking a glance on original packet contents.

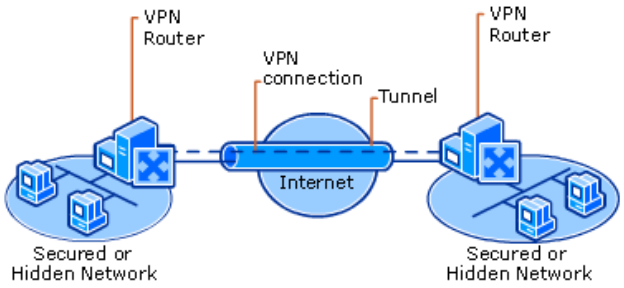

Fig. 2: (Technet-What is VPN, March 28, 2003, retrieved from https://technet.microsoft.com/en-us/library/cc739294(v=ws.10).aspx)

Before transmitting a data packet, it is encapsulated (wrapped) in a new packet form including a new header and other information This header provides special routing information so that it can access a shared or public network, before it reaches its tunnel endpoint. This logical path, which is travelled by the encapsulated packet, is called a tunnel. When each packet reaches the tunnel endpoint, data packet is decapsulated and passed to its final destination. Both tunnel endpoints need to support the same tunnelling standards and protocols. Tunnelling standards are operated at either data-link layer or network layer of OSI model. The most commonly used tunnelling protocols are IPsec, L2TP, PPTP and SSL. A packet having non-routable IP address can also be sent inside a packet having unique IP address, thereby extending a private usage network over the Internet. Out of all available standards, the most commonly used tunneling protocol is Ipsec Vpn.

IPSec (INTERNET PROTOCOL SECURITY)VPN

An IPsec VPN protocol technology creates a tunnel between two communicating endpoints through which any number of connections and protocol types (web, email) can travel. In it, the original IP data packet is re-encapsulated, so all application protocol information is hidden during the actual transmission of the data, thereby increasing the sense of security. It allows a system to select the required security algorithm(s) and secret keys to be used for the services requested. It gives a sense of basic authentication, data integrity and encryption services to protect unauthorized viewing and modification of data.

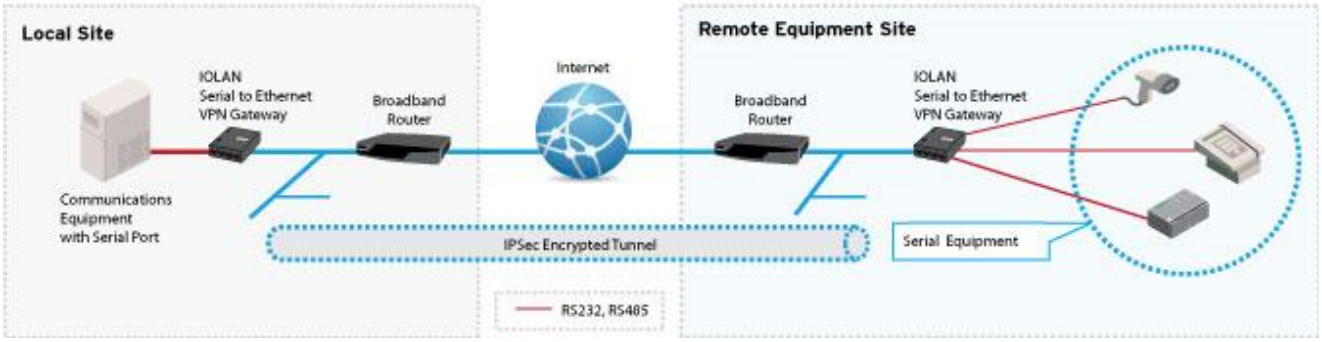

Fig. 3: (Perle systems technical notes, IPSEC VPN gateway, retrieved from https://www.perle.com/supportfiles/iolan-vpn-gateway.shtml)

It enables the system to use two security protocols named AH (Authentication header) and ESP (Encapsulated Security Payload), for required services.

Authentication Header (AH)

It provides a sense of authentication of sender system and integrity of IP packets, but it does not have any encryption scheme. An AH header added to the simple IP packet contains a collection of data, a sequence number etc. and other control information that can be used to verify the sender's identity, ensure data integrity and prevent echo attacks.

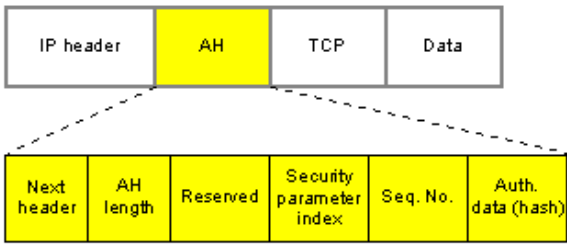

Fig. 4: (VPN Security, February 2008, the Government of the Hong Kong Special Administrative Region)

AH works in two modes – Tunnel and Transport. In tunnel mode, a new IP header is created for each data packet whereas no such extra overhead is done in transport mode.

Encapsulated Security Payload (ESP)

It provides data privacy or confidentiality of data along with source authentication and integrity. ESP uses symmetric(private key) encryption algorithms (such as 3DES) to provide data privacy.

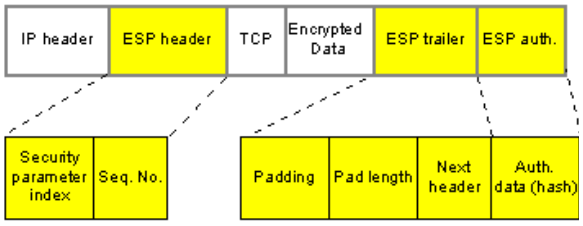

Fig. 5: (VPN Security, February 2008, The Government of the Hong Kong Special Administrative Region)

Like AH, ESP also works in two modes. In tunnel mode, it create new IP header for each outgoing packet. In ths mode, both encryption and integrity can be provided for both encapsulated IP packet as well as ESP header. In transport mode, both encryption and integrity protection can be provided for payload of IP packet and ESP header.

COMMON VPN SECURITY FLAWS

Poor User Authentication

VPN does not provide the committed sense of security by ensuring user authentication. VPN connection needs only to be established by authenticated user only. It does not take any special preventive measures to ensure authentication and integrity of message.

Hacking Attacks

VPN machine is a good point to stag the attack from the network. An intruder and spoofer may target vpn client machine to launch an attack. Various types of attacks can be committed but two special attacks named VPN Hijacking and Man-in-the –middle attack.

- VPN Hijacking is the attack that helps the intruder to be an incharge of an established vpn network by defacing and impersonating client for the remote machine over vpn network.
- Man-in-the-middle is the attack that affects the overall data traffic travelling over the network. In this attack, intruder intercepts the outgoing and incoming messages to scramble the data form by inserting, deleting, modifying extra data bits to change the original bit patten.

Virus/Malware Infections

The whole VPN network can become victim of infection is client or remote machine is virus affected. In case, if client machine is infected with virus then there is full risk of leakage of vpn network security password to an attacker.

PREVENTIVE MEASURES TO IMPOSE SECURITY

As every problem comes with solution, VPN networks are also supposed to be a follower of basic and successful preventive measures as:

- Proper Anti-virus software must be installed on server machine to prevent any error or infection, originated from either end.
- Regular training classes and sessions should be conducted by vpn network authorities to introduce them with new level of vulnerabilities.
- Suitable security policies and guidelines should be supported by VPN network to govern the implementation schemes.

CONCLUSION

This paper focused on discussion of typical means of accessing a secured and private network over insecure public infrastructural networks such as the Internet (termed VPN). This research was to highlight the prime flow of VPN technology along with all the vulnerabilities coming on its way of functionality. As no system is flawless and invulnerable to be implemented with closed eyes. Various preventive measures and suggested workflows need to be implemented for successful and smooth functionality of private network.

REFERENCES

[1] "Guide to IPsec VPNs" by Sheila Frankel Karen Kent Ryan Lewkowski Angela D. Orebaugh Ronald W. Ritchey Steven R. Sharma.

[2] IPsec Virtual Private Network Fundamentals-An Introduction to VPNs, Cisco Systems, James Henry Carmouche, CCIE No. 6085.

[3] VPN Security, February 2008, The Government of Hong Kong Administrative Region, http://www.infosec.gov.hk/english/technical/files/vpn.pdf

[4] Vulnerabilities of VPN using IPsec and Defensive Measures, Byeong-Ho Kang, University of Tasmania, Australia, Maricel O. Balitanas, Hannam University, Department of Multimedia Engineering,Postfach, International Journal of Advanced Science and Technology, Vol. 8, July 2009, http://www.sersc.org/journals/IJAST/vol8/2.pdf

[5] Virtual Private Network, Ritika Kajal, Deepshikha Saini, Kusum Grewal, ITM University, Gurgaon, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 10, October 2012, ISSN:2277 128X.