A Conceptual Survey of Sturucture, Security and Advantages in Virtual Private Network

Shubham Patni
Ajeenkya D Y Patil University, Pune

Mayuresh Sambudas
Ajeenkya Dy Patil University, Pune

Shabnam Sharma
iNurture Education Solutions Bangalore

ABSTRACT
There is an increasing request nowadays to connect to core networks from different places. Workers regularly need to connect to internal private networks over the Internet from home, hotels, airports or from other external networks. Security becomes a main attention when staff or business partners have constant access to internal networks from insecure external locations. Currently, such a secured access is realized with Virtual Private Network (VPN) connections. Although operational, the current VPN solutions suffer of severe limits. Most of the VPN solutions are not satisfactorily secured since they are using weak authentication. The more secured ones are quite often expensive and require the usage of security tokens that demand administration from the service provider. On the user's side there is a need for additional care and attention since he/she has to carry an extra device. In this paper, the focus is to examine the structure, security, and benefits of VPNs.

Keywords
Security, Administration, Authentication, Network, Server

1. INTRODUCTION
Using the Internet as the support for communication promises trustworthiness of service. The Internet provides further benefit for VPN users. Even extremely remote locations have access to the Internet via dial-up modems. VPNs promise secure communication for dial-in users. Mobile users cannot possibly use rented lines for their communication with the corporate site and so VPN technology is the only real solution to this problem. The goal of a VPN solution is to establish a secure communication channel between different network. Additionally, with user-based authentication, companies can keep a closer watch on the information their employees are accessing and thus limit internal fraud. VPNs use the Internet for communication. The Internet does not provide the highest performance solution, but they allow users to use the Internet as their own private networks. This gives users access to the wealth of information available, while allowing reliable, secure communication channels between parties at low cost.

While the Internet has transformed and significantly 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. The goal of a VPN solution is to establish a secure communication channel between different network. Although network attacks are probably 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 slightly inconvenient to completely breakdown. These are significant costs with implications for important data, privacy, network downtime, and third-party legal claims.

A VPN is a typical way of connecting networks over a public network setup. Although several cloud providers offer VPN access to their residents this can be undesirable in certain situations (e.g., the resident does not trust the provider and/or the resident wants to have better controls over the VPN policies and key generation and distribution process). The goal of a VPN solution is to establish a secure communication channel between different network. VPN-as-a-Service (VPNaaS) using virtualized VPN software, essentially making the VPN yet another building block for a service.

2. LITERATURE REWIEW
Virtual Private Network (VPN) [1] One of the most important issues regarding VPN technology is how to assure the security of private data passing through a public channel. Most VPN solutions on the market today offer security for corporate communication needs. VPNs use the Internet for communication. VPN security falls into three categories: encryption, authentication and integrity. Encryption is the function of scrambling data so that only the intended receiver can read it. Authentication is the process of verifying the sender to the receiver. Integrity ensures that the data has not been tampered with during transmission.

Pervasive Service Access with SIM-based VPN [2]. The goal of a VPN solution is to establish a secure communication channel between different networks, or between a user and a specific network (e.g. the enterprise network), from remote locations. The secure channel is typically established across a public network, usually the Internet. After the establishment of a VPN connection, hosts on one of the networks will perceive hosts on the other network as part of the same Local Area Network (LAN), and users are thus able to access services as if they were local. A special configuration often referred to as "road warrior" is commonly used by employees to remotely

Design and Modelling of an IPSec VPN in Virtualized Environment [3]. There exist different approaches through which the data can be accessed across a VPN: host-to-host, site-to-site and remote access configurations. Each of their advantages and disadvantages have been studied, to select the best suitable. Site-to-site are built when accessing of data is done across different geographical locations or through different subnets. VPNs use the Internet for communication. Host-to-host configurations establish connections between two different hosts initiated by either one. This approach is suitable for communicating to a remote web server or to a backup system. Remote access VPNs are set up usually for connecting from a remote place to the home network in so-called “road-warrior” scenarios.

2.1 VPN—Virtual Private Network

The term VPN is described as network communication which operate the combination of other technologies to establish the secured connection via untrusted network. The data transmission is done as if it were forwarding via private network. The Analysis of Firewall and VPN in Enterprise Network Performances [4] The data transmission is executed by means of tunneling process. Before the transmission of the packets, it is wrapped i.e. encapsulated into a new packet and add new header information. The routing information is provided by this added header, so the packet is traverse a shared communication network before get into tunnel end point. VPNs use the Internet for communication. This logical pathway of the encapsulated packet is known as tunnel the data confidentiality is achieved in VPN by the encryption process. The most commonly used tunneling protocol in the VPN is IPSEC (Internet Protocol Security). The IPsec use two security protocols; Authentication header (AH), Encapsulated Security Payload (ESP) in order to provide the authentication, encryption and integrity of data. In [8], author has provided brief insight on the concept of Virtual Private Network.

2.2 Authentication Header

It uses the intelligent approaches of security deployment by security professionals to establish the customized solution of networks to provide the connection and resources availability to the particular and authorized users in the proper manner i.e. secure and satisfy the need of network architecture requirements.

Deployment of a Policy-Based Management System for the Dynamic Provision of IPsec-based VPNs in IPv6 Networks [5] The policy-based management paradigm is being currently considered as a promising approach to provide dynamicity to the definition of services. VPNs use the Internet for communication. One service of great importance in IPv6 networks is VPN. Using security policies and the related policy management architecture, VPNs can be dynamically and securely deployed.

2.3 Security Considerations

2.3.1 General VPN Security Considerations

1. VPN connections can be strengthened by the use of firewalls.
2. An IDS / IPS (Intrusion Detection / Prevention System) is recommended in order to monitor attacks more effectively.
3. Anti-virus software should be installed on remote clients and network servers to prevent the spread of any virus / worm if either end is infected.
4. Unsecured or unmanaged systems with simple or no authentication should not be allowed to make VPN connections to the internal network.
5. Logging and auditing functions should be provided to record network connections, especially any unauthorized attempts at access. The log should be reviewed regularly.
6. Training should be given to network/security administrators and supporting staff, as well as to remote users, to ensure that they follow security best practices and policies during the implementation and ongoing use of the VPN.
7. Security policies and guidelines on the appropriate use of VPN and network support should be distributed to responsible parties to control and govern their use of the VPN.
8. Placing the VPN entry point in a Demilitarized Zone (DMZ) is recommended in order to protect the internal network.
9. It is advisable not to use split tunneling to access the Internet or any other insecure network simultaneously during a VPN connection. If split tunneling is used, a firewall and IDS should be used to detect and prevent any potential attack coming from insecure networks.
10. Unnecessary access to internal networks should be restricted and controlled. In [9] author has provided architecture for board band virtual network in under costumer control.

2.3.2 Extranet VPN Security Considerations

1. Strong user authentication mechanisms should be enforced.
2. The VPN entry point should be placed inside a DMZ to prevent partners from accessing the internal network.
3. Access rights should be granted on an as-needed basis. Only necessary resources should be available to external partners. Owners of these resources should review access permissions regularly.

2.3.3 Client-Side VPN Security Considerations

The following are general security considerations for VPN users:

1. Strong authentication is required when users are connecting dynamically from disparate, untrusted networks.

3. CONCLUSION

VPN have the capability to offer the best possible availability, essential security, multicast support and management essential components for a reliable, trouble-free, Scalable network. The goal of Virtual Private Network is to simulate a regular network connection to create virtual point-to-point link, any data that is transmitted. VPNs use the Internet for communication. A VPN solution can reduce the need for dedicated equipment by using existing internet equipment. VPNs are scalable solutions which allow new users to be added without major restructuring. Implementing a VPN solution for home/school links would be extremely beneficial. VPN provides a means of accessing a secure, private, internal network over insecure public networks such as the Internet. A number of VPN technologies have been outlined, among which IPsec and SSL VPN are the most common. Although a secure communication channel can be opened and tunnelled through an insecure network via VPN, client-side security should not be overlooked.

4. REFERENCES

[1] Harkins, D. & Carrel, D., RFC-2409: The Internet Key Exchange (IKE), IETF, Network Working Group,841November 1998, online: http://www.ietf.org/rfc/rfc2409.txt

[2] Pereira, R. & Beaulieu, S., Extended Authentication within ISAKMP/Oakley (XAUTH), IETF, online: http://tools.ietf.org/id/draft-ietf-ipsec-isakmp-xauth06.txt

[3] Samar, V. & Schemers, R., Unified Login with Pluggable Authentication Module (PAM), Open Software Foundation, October 1995, online: http://www.opengroup.org

[4] Kent, S. & Sea, K., RFC-4301: Atkinson, R., & Kent, S. (1998). Security architecture for the internet protocol., December 2005, online: http://www.ietf.org/rfc/rfc4301.txt

[5] Phifer, L. (2006). Understanding IPSec identity and authentication options. Search Security. com, June., SearchSecurity.com, June 2006, online: http://searchsecurity.techtarget.com.

[6] Kritika, M., Priyadharsini, M., & Subhas, C. (2016). Virtual Private Network-A Survey. International Journal of Trend in Research and Development, 3(1), 78-81. – A Survey: IJTRD | Jan - Feb 2016 Available Online@www.ijtrd.com.

[7] Ortiz (1997) "Ortiz, S. (1997). Virtual private networks: leveraging the Internet. Computer, 30(11), 18-20.. 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/production/en/Conn_VPN.asp?frame=true.

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

[10] Xiangping Chen, Mohapatra, P. (2002) "Chen, X., & Mohapatra, P. (2002). Performance evaluation of service differentiating Internet servers. IEEE Transactions on Computers, 51(11), 1368-1375.Computer, IEEE Transactions, Vol. 51, 1368-1375.

[11] Caronni, G., Kumar, S., Schuba, C., & Scott, G. (2000, December). Virtual enterprise networks: the next generation of secure enterprise networking. In acsac (p. 42). IEEE.G.; Kumar, S.; Schuba, C.; Scott, G. Computer Security Applications, 2000. ACSAC '00. 16th Annual Conference, 2000 Page(s): 42 –51

[12] Isaacs, R. (2000, March). Lightweight, dynamic and programmable virtual private networks. In Open Architectures and Network Programming, 2000. Proceedings. OPENARCH 2000. 2000 IEEE Third Conference on (pp. 3-12). IEEE., 2000. Proceedings. OPENARCH 2000. 2000 IEEE Third Conference on, 2000 Page(s): 3 –12