Nested Tunnel: Information Security in Hybrid Cloud Computing

Dinesh Taneja, S S Tyagi
Manav Rachna International University
India
dinesh.taneja@gmail.com
shyam.fet@mriu.edu.in

ABSTRACT: *Virtual Private Network, VPN is communication channel between two networks and is used for network security between two networks. In this era of cloud computing, data is accessed from anywhere anytime. For security concerns, data is exposed while data is at rest and data is in motion. Data in motion is referred to data in transition as it is moved from a stored state to same or another form to a different location. This mobility nature of data has driven the need for secure remote access from remote locations, end points, platforms and environments. Leased lines are supposed to be the most secured connection for remotely accessing the data but at the same time, it is not the cost effective solution and it restricts user's ubiquitous connectivity. As a cost effective measure to attain security and confidentiality of data, organizations are using legacy Internet Protocol Security (IPSEC) and Secure Socket layer (SSL) VPN solutions to remotely access their data. In this paper, a VPN Tunnel inside another VPN Tunnel is being proposed for higher security for the data in transition.*

Keywords: Cloud Computing, Nested Tunnel, VPN, Header Compression, SSL, IPSEC

Received: 19 November 2017, Revised 8 January 2018, Accepted 17 January 2018

DOI: 10.6025/isej/2018/5/1/24-28

1. Introduction

Cloud computing is becoming popular and at the same time its adoptability may be faster if security aspects [4] are addressed well. In Cloud implementations, Virtual Private Networks [3] allow users to securely access a private network and share data remotely through public networks and are more Virtual Private Network (VPN) is a combination of two networking concepts.

Virtual Networking: Splitting of a physical network into logically separate network. In case of VPN, remote users and network hosts to be administered as a single entity.

Private Networking: To incorporate data protection and confidentiality amongst hosts allowing trust relationships established and enforced on a network.

There are two main architectures of VPN prevalent in the industry:

Site to Site VPN which is cost effective solution of leased lines for connecting two different network deployed across geographies. This VPN provide access to multiple hosts concurrently and it is a permanent connection between two networks.

Remote Access VPN is used to provide secured access to roaming individual users. This is established between a single machine and a network only on demand and connection is destroyed after the individual has completed its work.

VPN technology uses different protocol suites such as MPLS, PPTP, L2TP, IPSEC, SSL and TLS. Out of this first three operate at OSI layer2 whereas IPSEC operates at Network Layer and SSL/TLS operate at higher layers. The two most used VPN Technologies are IPSEC and SSL (latest TLS).

2. VPN IPSEC Tunnel

IPSEC[3] is a suit of protocols as defined in IETF to achieve secure services over IP Packet switched networks. IPSec provides authentication, integrity, access control and confidentiality; the information exchanged using this protocol is encrypted. This protocol is used for site to site connection and remote access clients across an insecure network. The protocol uses following three major steps for communication.

IKE phase1 which sets up secure tunnel to negotiate PKS Phasee-2 parameters

IKE phase2 is used to negotiate IPSec SAs to setup the IPSec Tunnel.

After the tunnel is established using IKE phase2, packets are encrypted and decrypted using the IPSec SA.

In this case access control is based on the device IP Address instead of end user's role and privileges.

3. SSL VPN

SSL VPNs [5] fall into 3 distinct categories – Application Layer Proxies, Protocol redirectors and Remote control enhancers. A standard SSL VPN is used with a standard browser and does not require any client agent to be installed on end user equipment. Flow exchange between the client browser include handshaking protocol (determine encryption parameters between client and servers), record protocol (exchange applied data) and alert protocol (terminate connections in case of errors).

4. Comparison of IPSEC and SSL

Both IPSEC and SSL technologies enable to provide a secure access to corporate network. The two technologies are used for different type of requirements [7]. The comparison of two technologies is mentioned below in Table 1.

5. Tunnel Inside the Tunnel

Hybrid cloud is an environment which uses a mix of public cloud and on-premises private cloud services with orchestration between the two platforms. There are requirements to access different applications and subnets across two networks. Leased line is one way of connection between two organizations and provide connectivity for hybrid clouds. Internet is most Ubiquitous packet switched public network; therefore a VPN Tunnel deployed over the public Internet means a significant cost savings to the organizations as compared to a leased line point to point connection. As discussed in previous section, IPSEC VPN is preferred for connecting two networks of different organizations but it has certain limitations as compared to SSL VPN.

It is being proposed that for better security requirements, site to site VPN may be established using traditional IPSec Tunnel and SSL Tunnel both using following steps

1. The firewall of one network can initiate https request to the firewall of second network across internet and establishes a secured https connection as per standard SSL protocol. This shall result into providing a secured Tunnel between two firewalls of different networks. This shall establish a connection only between two entities (two firewalls of two different networks) but will not provide multiple client server connections from two different networks.

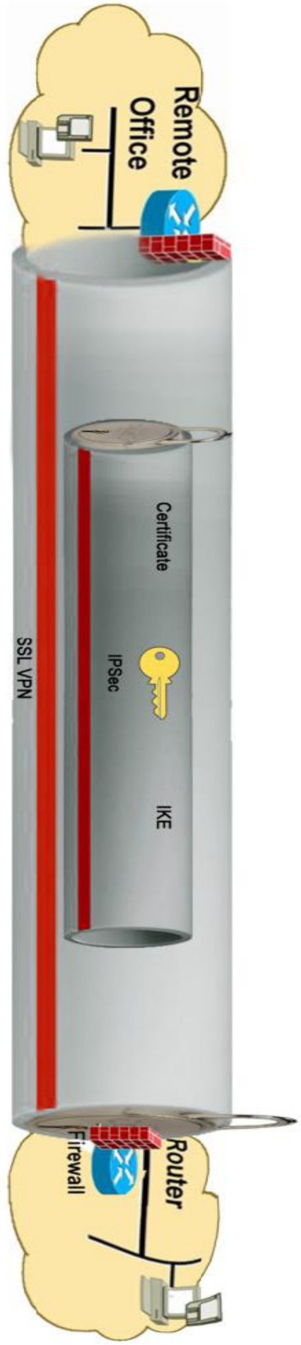
2. Traditional IPSec tunnel may be established between two firewalls using pre shared keys exchanged between two sides which will result into site to site VPN.

Component	**IPSEC**	**SSL**
Connectivity	Site to Site and remote access	Remote Access
Accessibility	Site to Site VPN is established between two well defined set of secured access device and/or client software	Can be accessed from anywhere using standard browsers
Installation	Require installation of client software (Remote VPN).	No Client software installed
OSI Layer	Presentation & Application Layer	Network Layer
Public IP address	Both sides need Public IP address	Only Server side needs public IP address.
Ports	Three different ports are used Protocol ID 50 for ESP Protocol ID 51 or AH UDP Port 5000 to allow ISAKMP traffic to be forwarded	Only one port 443 is used.
Access Control	Useful in case Trusted user groups require access to private servers and / or subnets	Granular access control requiring ole mapping, dynamic authentication for different resources.
End point Security	Does not support end point security	Supports end point security assessment
Intrusion Prevention	IPSEC access rights are static and can only be modified by network administrator manually.	Since SSL VPN works at Application and presentation layer, as soon as data is decrypted, it may be evaluated for IPS, anti malware, antivirus etc and dynamically modify network access rights

Table 1. IPSEC and SSL comparison

3. The access list for private networks on both sides can be established for providing access to various applications and networks.

4. The data exchanged between clients from first network to the server of second network shall first be encrypted and decrypted using IPSEC VPN



5. The IPSEC packets shall be encrypted again using SSL/TLS algorithm.

6. Finally the data exchange shall happen inside two tunnels resulting into more secured communication as depicted in Figure 1.

In the era of SDNs the tunnel inside tunnel is possible to achieve without additional appliances.

Hybrid cloud is being used across organizations due to various reasons, Site to Site VPN connectivity (IPSec) is a good cost effective solution as compared to leased line. At the same time there are security concerns of respective stake holders in corporates. IPSec Tunnel inside SSL Tunnel is being proposed for enhanced security. This is an example of deploying two locks instead of one for secure communication and two different algorithms to open these locks. The two different layers of security and different algorithm of encryption and decryption may make it more complex for MITM (Man in the Middle) exploitations.

Nested Tunnel have more header overhead than a single tunnel in the network. Nested Header compression [6] may help in reducing payloads.

6. Conclusion and Future Work

Both IPSec and SSL VPN enable organizations to provide their users a secure access for business needs. Tunnel inside the tunnel may provide a better secured connection. This technology as discussed in this paper shall not provide any security for data on rest and that should never be overlooked. There are many research papers published till date which mentions comparative analysis of IPSec and SSL Tunnel. This paper described the possibility of combining the advantages of both VPN technologies and suggested stronger site to site VPN which is a IPSec tunnel inside SSL VPN.

The future work can be carried out to for the payload comparison of having 256 bit encryption being used in a standard IPSec tunnel vs 128 bit encryption to be used in a tunnel inside tunnel technology.

References

[1] Jansen, Wayne., Grance, Timothy. (2011). Guidelines on Security and Privacy in Public Cloud Computing. National Institute of Standards and Technology (NIST) Special Publication 800-144, US Department of Commerce; December.

[2] Bangerter, E., Gullasch, D., Krenn, S. (2011). Cache games: bringing access-based cache attacks on AES to practice. *In:* 32nd *IEEE Symposium on Security and Privacy*.

[3] Kent, S., Seo, K. (2005). Security Architecture for the Internet Protocol. RFC-4301, December.

[4] Dinesh Taneja., Tyagi, S S. (2017). Information Security in cloud computing: A Systematic Literature Review and analysis. *International Journal of Scientific Engineering and Technology*; January.

[5] Su Hua SUN. (2011). The advantages and implementation of SSL VPN. IEEE.

[6] Seema Vanjire., Sachin Vanjire. (2014). Nested Header Compression Protocol in wireless Network with .NET Technology. International Conference on Communication and Signal Processing, April 3-5.

[7] Huaqing MAO., Li ZHU., Hang Qin. (2012). A Comparative research on SSL VPN and IPSec VPN. IEEE.

[8] Ahmed Laguidi, Aawatf Hayar, Michelle Wetterwald. (2012). Secure HeNB Network management Based VPN IPSec. Next Generation Networks and Services NGNS, 2-4 December.

[9] Lim, JaeDeok., Kim, JeongNyeo. Implementation of light-weeight IKE protocol for IPSec VPN within Router, ETRI Korea.

[10] Hamza, Yasir Ahmed., Omar, Marwan Dahar. (2013). Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing. *International Journal of Computational Engineering Research*, 03 (6) June.

[11 Berger, S., Cáceres, R., Pendarakis, D., Sailer, R., Valdez, E., Perez, R., Schildhauer, W., Srinivasan, D. (2008). Managing Security in the trusted virtual datacenter. *SIGOPS Oper. Syst. Rev*. 42 (1) 40–47.