International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 2, January-February 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Comparative Research on SSL VPN and IPSec VPN

Vaibhav Gahlot

Masters in Computer Applications, Jain (Deemed-to-be) University, Bangalore, Karnataka, India

ABSTRACT

With information technology growth, VPN In a variety of areas, technology has been commonly used. Here we are. Two forms of VPN are studied in paper: IPSec and SSL VPN Detailed implementation, protection, scalability and breadth Other dimensions, benefits and contrasts are analyzed and compared. Inappropriate collection comparison is summarized, finally, Standard suggested. Standard proposed.

KEYWORDS: *VPN, IPSec, SSL*

How to cite this paper: Vaibhav Gahlot "A Comparative Research on SSL VPN and IPSec VPN" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-2, February 2021, pp.54-55, URL: www.ijtsrd.com/papers/ijtsrd38333.pdf

IJTSRD38333

INTRODUCTION

VPN (Virtual Private Network) is referred to as an encoding and access management technology for the public network, providing private communication networks. VPN is transparent to users and appears to be using a personal circuit between users. The utilization of VPN technology can significantly minimize the users' costs relative to a conventional Intranet network; it improves the simplicity commonly used in many fields. PPTP, L2TP GRE IPSEC SSL etc are part of the VPN network protocols. IPSec VPN is a network security system delivering security communication between a pair of nodes. The widely implemented VPN applies to IPSec VPN and SSL VPN. IPSec VPN is used to address VPN links between one and other gateways, including access protection, confidentiality, integrity security and authentication of original data etc. SSL VPN achieves remote information connection through a simple approach contrasted with IPSec VPN.

Any computer installed in the browser will use the SSL VPN. But the client program of the IPSec VPN should be installed on all customers. IPSec VPN is the standard remote access control solution of the company. SSL is ideal for remote access. As the SSL VPN Implementation was developed, more and more organizations started implementing the SSL VPN Network Architecture. The paper specifically looked at IPSEC VPN and SSL VPN and evaluated them from certain perspectives, including application, complexity and reliability. Finally, in connection with the situation the paper explains how to use the VPN technologies.

Literature Review

Some papers and publications argue very simply that VPN does not explicitly incur overhead processing on the network, but that the Internet has an effect on efficiency. According to an article that VPN Consultants reported in the San Francisco Bay Area on security FAQ, the bulk of slowdowns in efficiency were in fact triggered by incoherent internet links rather than overhead encryption processing.

Liu, L, also, says. And Gao, W. And Gao. (2007), clarified that IPv4 (a commonly used Internet protocol) networks have inherent vulnerabilities that are now barriers to network growth. They contend that network-implemented VPNs, i.e. the internet itself automatically inherits some other issues such as high network overheads, lack of service quality assurance (QoS), the NAT-crossing problem, etc. They propose to address this problem effectively with VPNs that are implemented on the version 6 (IPv6 Internet Protocol), known as Next generation protocol."

Often a VPN tunnel can be impacted by high packet loss and packet rearrangements. Any bridged protocols can have issues with rearranging.

IPSEC &SSL PROTOCOLS

IPsec protocol

In order to protect communication for the IP layer, IPSec is a type of security protocol that is introduced by the IETF IPSec working group. IPsec protocol contains confidentiality and main negotiating protocols. The contact methods are specified in the protection protocol. The negotiating conditions and verification of identity are established in key negotiations. The IPSec protocol offers two types of contact security mechanisms: ESP and AH (Authentication Head).

The ESP system preserves information secrecy and honesty; the AH mechanism protects the integrity.

Anti-replay attack can be avoided by ESP and AH systems. The IKE protocol in IPSec protocol has been introduced for the negotiation of automated parameters in terms of confidentiality. IKE agreed security parameters include encryption and authentication algorithms, key-encoding and authentication key(s). ESP provides two encapsulation modes for IP packets namely transmission mode and tunnel mode. The initial IP head remains unchanged in the transmitting mode, only the transport layer data are encrypted. In tunnel mode, a new IP head is connected to the entire IP data packet.

SSL protocol

SSL (Secure Sockets Layer) is an array of Netscape Company's internet data authentication protocols that are typically used to authenticate identity and transfer data between Web browsers and the Server. In the TCP/IP protocol and other application layer protocols, the SSL protocol is used. It offers data transmission protection assistance. There are two layers of the SSL Protocol: SSL Handshake, SSL Log, SSL Change Cipher Specific Protocol and SSL Warn. SSL Script Protocol is based on a trusted transportation protocol (such as TCP) which provides higher-level protocol support for data encoding, compression, encryption and other basic functions. The SSL Handshake Protocol is based on SSL login protocol, which is used in the current data transmission before all parties communicate for identity verification, consultation, encryption key exchange and encryption algo.

COMPARISONS BETWEEN IPSEC AND SSL VPN

Features	SSL	IPSEC
Identity authentication	One-way authentication Mutual authentication Digital certificate	Mutual authentication Digital certificate
Encryption	strong	Very strong
Encryption type	Key length 40 bits to 128 bits	Key length 56 bit to 256 bits
Full security	End-to-end security, from the client to the resource, end the whole encryption	Network edge to the client, encryption only between the VPN gateway
Access	Easy Selection at anytime, anywhere	Access restrictions to the defined controlled user access
Cost	Low	High
Installation	Easy	Complex
Application	Web File sharing Email	All protocol based on IP service
User	Customers, partners, suppliers, users, remote users more	Internal users
network	Operates at layer 4-7	Operates at layer 3
Gateway location	Usually deployed behind the firewall	Usually implemented on the firewall
Scalable	Easy configuration and expansion	Easy expanding at the server end but difficult for the client

VPN selection

The analyzes demonstrate that each VPN has its own advantages and drawbacks. The current VPN range should satisfy the user needs as seen in the table-

SSL VPN	IPSEC VPN
Browser based with optional thin client	Require host based clients
Remote access network	Site to site access

Conclusion

VPN is used extensively in the safe technology of transmission. It uses public network secure contact protocol to create a safe and secure channel for data transmission ensuring privacy and computer confidentiality. In this article, the range of SSL-VPN and IPSec-VPN technologies is analyzed and a comparative analysis is performed.

References

[1] The Hot market for SSLVPNs Database and Network, 2005 Vekemans, John.

[2] IP Virtual Private Networks (VPNs) Rosen E, Rekhter Y.

[3] Security Framework for provider-provisioned Virtual Private Networks (PPVPNS), 2005, Fang.

[4] Research of VPN based on SSL, Technology and application of network security, 2004 Lihong Bao, Liya Li.

[5] The security implementation of IPSec VPN, CarIton, R. Davis.

[6] Technology of IPSec VPN, Beijing: Posts & Telecom press, 2008, Baohong He, Tianhui.

[7] Firewall policy and VPN configuration, 2008.Lucas, Xielin.

[8] Study into the SSL VPN Access Control System Wireless Local Network Architecture, 2007.

[9] Practical network support for IP trackback, Proc of IEEE／ACM Transactions on Network, 2001, Savage S, Wetherlal D.

[10] Cryptographic Suites for IPSec, December 2005, P. Hoffman.