ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 3; Issue 6; November-December-2015; Page No. 01-05

Performance Analysis of Various Protocols on Virtual Private Network for IPSec

[1] Prakriti Trivedi, [2] Rahul Kumar Jain

[1] Assistant Professor, DCSE, Govt. Engineering College, Ajmer

[2] Research Scholar, DCSE, Govt. Engineering College, Ajmer

Abstract

Many Corporations are seriously concerns about their security of network. Virtual private network is commonly used in business situations to provide secure communications over public infrastructure such as internet. VPN is proven technology that does provide security strong enough for home use and business use. VPN network allow two or more parties to communicate secure over public network using cryptographic algorithms and protocols In this paper we analyze the performance of protocols on TCP and Ftp in VPN router network on different data sizes and calculate the throughput of files on different encryption algorithms and then the result is compared to determine the performance throughput.

Keywords: VPN, IPSEC, DES, MD5, SSL, PPTP, Encryption.

1. INTRODUCTION

A Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public network such as the Internet. Large corporations, educational institutions, and government agencies use VPN technology to enable remote users to securely connect to a private network. Data transmission protocols, which are used in the internet, such as TCP/IP, are originally not designed to provide data security. In this context, the term security can be understood as follows: if Ali and Bob wish to exchange private information in an electronic way, and Mall wants to listen into the transmission in order to find out its content, the transmission is determined as secure, when Mall has no chance to succeed. In other words, by means of data encapsulation, encryption and authentication, Mall cannot use the transmitted data. This is reached by adding secure protocols, such as IPSec, L2TP or PPTP to the existing protocols which are used in the internet. These technologies provide secure data tunnels over an insecure network, which is referred to as Virtual Private Networks [2].

To implement VPN, there are numerous protocols and products available on the market, each having its own capabilities and features. Three protocols that are frequently used with operating systems are IPSec, PPTP and SSL. These provide encryption and integrity to data in transition. Each of these VPN protocols can be implemented with different algorithms – e.g. Data Encryption Standards (DES, 3DES) and Blowfish algorithms are used for encryption, while Message-Digest 5 (MD5) and Secure Hash Algorithm (SHA) for integrity [2]. The choice of VPN protocol and the associated algorithm affect the network performance of different by different amounts. In modern Internet systems, IP Security (IPSec) plays an important role in data communication, and provides a rich set of security protections for e-commerce and e-government applications. However, the IPSec does not address the issues on how the traffic should be handled at the IPSec endpoints. This problem is addressed by the IPSec policy which consists of lists of rules that designate the traffic to be protected, the type of protection, such as authentication or confidentiality, and the required protection parameters, such as the encryption algorithm [4]. Tunneling is a procedure where data is encapsulated and encrypted and then sent over a secure connection. This is done by encapsulating an encrypted packet within another packet containing the address of the destination. A good tunnel hides all information about the packet contents from the network layer and up to the application layer. Before starting a tunneling session proper authentication and integrity check mechanisms has to be done. This can be done by means of regular authentication, using user names and passwords, as found in many applications today. Together with digital certificates

Corresponding author: Prakriti Trivedi

one can identify users in a secure way. The ip security protocol can be used to implement encryption and message authentication in virtual private network and encryption and message authentication provided by IPSec require some computation time which degrade performance and increases the Security.

II. Background Information:--In this section the different VPN protocols/technologies are discussed. These protocols and technologies are broadly used in the industry as well as small home use.

A. IPSec:--IPSec is an open standard framework developed by Internet Engineering Task Force (IETF) that can be implemented for establishing VPN tunnels through the use of cryptographic security services. IPSec provides data confidentiality services to ensure that it is not illegal eavesdropping by users in the transmission. IPSec is an OSI Layer 3 protocol that supports network-level peer authentication, data origin authentication, data integrity, and data confidentiality and replay protection.

B. SSL: -- SSL is VPN technology which is developed by Netscape that is commonly used in web browsers to give users to seamless secure connection for transmitting documents over the internet. It protects data using encryption and uses hashing to ensure integrity [3]. SSL uses a private key to encrypt data which is sanded over the ssl connection. When SSL is properly configured then it also provide client authentication.SSL provides two layers of protocols in TCP framework SSL record which is mainly for the fragmentation compression encryption and standard http which provides the internet communication services between client and host. In the SSL first client and server negotiate cipher means which ciphers are to use by both side and then the key exchange and authentication algorithm. After that the encryption keys are exchanged and authenticated using chosen algorithm. In this Mac is also used which is mainly made up of hash cryptographic function. The SSL vpn is provide three access modes: clientless, Thin Client and Tunnel Mode .In clientless mode gives more secure web content resources and accessing most content which we expect to access to web browser, such as databases, online tools which employs a web interface. In thin client extends the capability of cryptographic functions of web browser to enable remote access to tcp based applications such as smtp, telnet and ssh and in the last tunnel mode offers extensive applications support through its dynamically downloaded ssl vpn client for web vpn. Full tunnel client mode delivers a lightweight, centrally configured and easy to support ssl vpn tunneling client that provides network layer access to virtually any applications.

C. PPTP:--PPTP was developed by vendor consortium of Microsoft ascend communications and 3com. PPTP is easy to configured and extension of point to point protocols. The pptp encapsulates the ppp frame (data can be encrypted and/or compressed) to be transmitted over an ip network using a modified version of generic routing encapsulation which is tunneling protocols that can encapsulates a wide variety of network layer protocols inside virtual point to point links over an internet protocol internetwork and provides flow control [14].In the other simple words PPTP client uses a ppp type connection to establish a link through the transmitted network from source to destination and after once the connection is established control connection is created after that from client to PPTP server and finally PPTP creates ip datagram containing encrypted ppp packets which is transmitted through tunnel [3]. PPTP have very simple operating mechanism. PPTP can be applied to establish VPN connections between the networks of internet service providers and their customers, who do not have to install additional VPN software.

III. IP Security protocols: -- This section describes the IPSec structure and using the encryption and authentication algorithm which is used on IPSec. There are two encryption modes in which IPSec can be implemented: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. This mode is commonly used to secure communication within a network. The more secure tunnel mode encrypts both the header and the payload and is generally used for securing communication that traverses unknown third party networks. That is, tunnel mode is used for network-to-network communication. IPSec has two protocols that is enables it to provide packet level security: Authentication Header (AH) and Encapsulating Security Payload (ESP). IPsec is very flexible and can be used in many ways. IPsec is used to create a majority of the VPN products found today. Checkpoint VPN-1, Cisco PIX, and the open source Open SWAN are all examples of commonly used VPN

solutions that implement IPsec [13]. IP Security system structure, referred to as IPSec, is a group of cryptography-based security of open network security protocols. AH (Authentication Header, AH) ESP (Encapsulating Security Payload, ESP) and IKE rule encryption and authentication and key management (ESP provide support for authentication).AH and ESP are used SA (Security Association. IKE is responsible for the establishment and maintenance of SA [6]. The basic purpose of IKE phase is to authenticate the IPSec peers and to set up a secure channel between the peers to enable IKE exchanges. IKE process authenticates the end points of the tunnel to each other, and securely exchanges the necessary information to create a more permanent tunnel using symmetric encryption [13]. IKE Authenticates and protects the identities of the IPSec Peers, Negotiates a matching IKE SA policy between peers to protect the IKE exchange, Performs an authenticated Diffie-Hellman exchange with the end result of having matching shared secret keys ,Sets up a secure tunnel to negotiate IKE parameters, Negotiates IPSec SA parameters protected by an existing IKE SA, Establishes IPSec security associations, Periodically renegotiates IPSec SAs to ensure security [9].
There is the two security mechanism of IPSec.

A. Authentication Header (AH):-- AH is algorithm independent, AH will operate with the algorithm of choice, depending on the level of security required. Currently the algorithm options are HMAC (Hashed Message Authentication Code) MD5 (Message Digest 5) or HMAC. Optionally AH will, if selected, provide protection against replays (man-in-the-middle attacks) as long as the receiver checks the sequence numbers [8]. The IP Authentication Header (AH) provides authentication, protection against replay attacks, and connectionless integrity for IP packets. The Sequence Number in the AH consists of a monotonically increasing counter value that is used to prevent replay attacks. Furthermore, the Authentication Data field contains the Integrity Check Value (ICV) for the packet. The ICV is the output of the chosen authentication algorithm computed over the entire IP packet. AH authenticates the entire packet including upper protocol data, with the exception of the destination address. AH used only alone when simple only authentication is just required or it can be used with the ESP when some higher layer security is required more then the authentication.

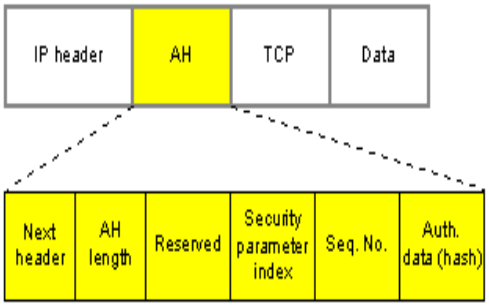

Figure 1: A simple representation of the Authentication Header

B. Encapsulating Security payload (ESP):-- ESP is normally is used to provide encryption and limited traffic flow confidentiality. ESP is used to provide confidentiality, data origin authentication, connectionless integrity, and anti-replay service (a form of partial sequence integrity). Authentication Header and encapsulating security payload are the two main components of IPsec that are added to the simple internet protocol to meet the security requirements. One another basic concept in the IPsec architecture is the security association. It is the one way relationship between the sender and a receiver which contains all the information for secured communication such which algorithm is used and encryption keys.ESP is also designed to be algorithm independent and the options are: Digital Encryption Standard (DES) (64 bit, commonly called 56bit), 3DES, RC5, Blowfish, Idea, Cast, and others are being added. ESP employs symmetric-key encryption algorithms such as RC5 and 3DES to provide confidentiality. ESP uses keyed hash algorithms such as SHA-1 and MD5 to provide message authentication and anti-replay service.DES, its common name, in ESP actually is DES-CBC (data encryption standard-cipher block chaining) with explicit IV (initialization vector) of 64 bits preceding the encrypted payload. Including the IV in each datagram ensures that decryption of each received datagram can be performed, even if some are dropped or reordered [8].

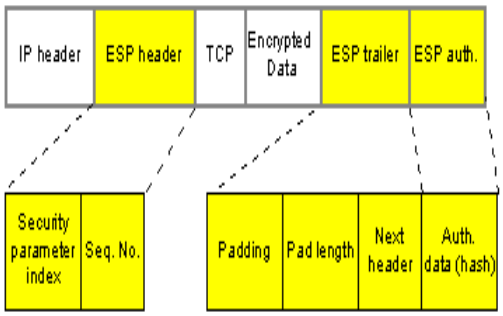

Figure 2: A simple representation of ESP

C. Encryption Algorithm: Encryption is a technique for scrambling and unscrambling information to guarantee the privacy of information as it flows over the internet. With 3DES,the data is encrypted ,decrypted and encrypted again but with different keys [12]. Several symmetric key encryption algorithms are defined for use in ESP. In this study, we use two ciphers in CBC mode: RC5-CBC and 3DES-EDE-CBC. DES, which is an acronym for Data Encryption Standard, is a symmetric-key block cipher that uses a 56- bit key to encrypt 64-bit blocks [1]. Triple DES (referred to as 3DES) provides more security than DES by encrypting a single block three times (with DES) using two or three different 56-bit keys. We implement 3DES. 3DES is cryptographically twice as strong as DES, but 3DES takes nearly three times as much computational time as DES to encrypt or decrypt blocks.

D. Authentication Algorithm: Authentication technology guarantees the identity of VPN participants (that gateways and client pc are who they say they are) and that the information received has integrity and has not been tampered with (verifies that a packet has not been altered during its trip over the internet) [12]. Two authentication algorithms that are defined for use with AH and ESP are MD5 and SHA-1. In this study, we shall evaluate the performance of both of these algorithms. MD5 message digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-bit) hash value, typically expressed in text format as a 32 digest hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications and is also commonly used to verify data integrity. SHA-1, a government standard, is a cryptographic hash function that accepts 64-byte plaintext blocks and outputs a 20-byte authentication value.SHA-1 is considered to be a cryptographically superior hash function, but MD5 is faster.

IV. Experimental Results: We present the finding of this research in this section. In this each IP vpn protocol (AH and ESP) implemented with different algorithms on ftp and http protocols and with 1MB size of files. In this first in ftp protocol the different encryption/Authentication applied with respect size in kb and then efficiency is calculated and then some different size the different combination is applied and similar process is applied on http protocols with some different using combinations. After that the avg throughput is calculated which is shown in figures.

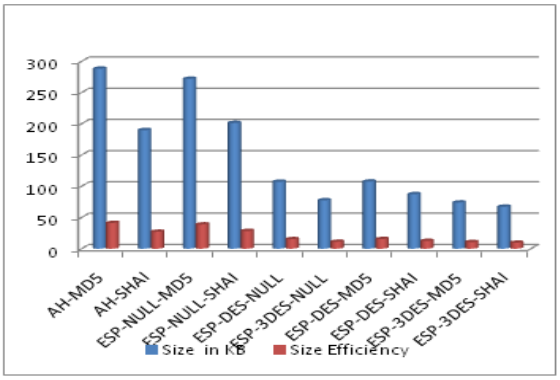

Figure 3: Throughput analysis of security protocol for FTP protocol Analysis of 1 MB size file

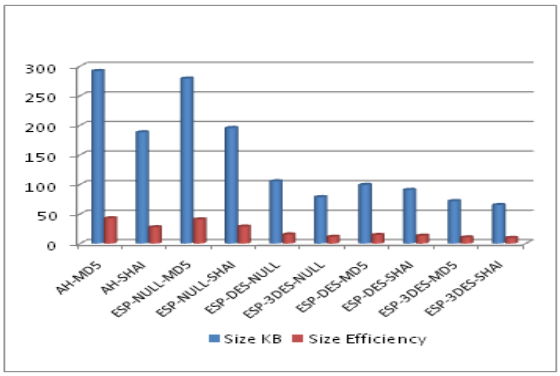

Figure 4: Throughput analysis of security protocol for HTTP protocol Analysis of 1 MB size file

V. Conclusion: -- In this paper we used different algorithm combination and calculate throughput analysis. In the first situation we calculate of 1mb file size in which AH-MD5 show higher efficiency and minimum efficiency is shown by ESP-3DES-SHA1 Combination because in this security is increased which impacted on performance and similar result in http of same file size.

VI. References:

1. John P. McGregor and Ruby B. Lee “Performance Impact of Data Compression on Virtual Private Network Transaction”, IEEE.
2. Thomas Berger “Analysis of Current VPN Technologies”, International Conference on Availability and Security, IEEE 2006.
3. Shaneel Narayan, Kris Brooking, Simon de Vere “Network Performance Analysis of VPN Protocols: An empirical comparison on different operating systems” International Conference on Network Security, Wireless Communications and Trusted Computing,2009IEEE.
4. Qi Li,Mingwei Xu,Ke Xu “Toward A Practical Scheme for IPSEC Management”.
5. P.Venkateshwari, Dr. T.Purusothaman “Comparative Study of Protocols Used For Establishing VPN” International Journal of Engineering Science and Technology Vol.1 (3), 2009.
6. Weili Huang, Fanzheng Kong “The research of VPN on WLAN” International Conference on Computational and Information Sciences,2010 IEEE.
7. Junhua Qu, Tao Li,Fangfang Dang “Performance Evaluation and Analysis of Openvpn on Android” Fouth Internation Conference on Computaional and Information Sciences,2012 IEEE.
8. Ritu Malik, Rupali Syal, "Performance Analysis of IP Security VPN ", International Journal of Computer Applications Volume 8, 2010.
9. Abdelmajid Lakbabi, Ghaixlane Orhanou, Said El Hajji “VPN IPSEC & SSL Technology” Next Generation Networks and Services NGNS, 2012.
10. Priyanka Rawat and Jean-Marie Bonnin, ”Designing a Header Compression Mechansim for Efficient use of IP Tunneling in Wireless Networks” CCNC IEEE2010.
11. Shaneel Narayan, Samad S. Kolahi, Kris Brooking, Simon de Vere “Performance Evaluation of Virtual Private Network Protocols in Windows 2003 Envirornment”, IEEE2008
12. Stanislav Milanovic, Zoran Petrovic,”Deploying IP-based Virtual Private Network Across the Global Corporation”.
13. Kotuliak,P.Rybar,P.Truchly,”Performance comparsion of IPsec and TLS Based VPN Technologies”,IEEE2011.
14. Abeer Eldewahi, Eihab Basheir,”Authenticated Key Agreement protocol for Virtual Private Network based on Certificate less Cryptography”, ICCEEE.
15. Craig Shue, Youngsang Shin, Minaxi Gupta, Jong Youl Choi,”Analysis of IPSec overheads for VPN Servers”,IEEE2005
16. Tarek S. Sobh, Yasser Aly,”Effective and extensive virtual private network” Journal of Information Security, 2011.