International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 04 | April - 2022 Impact Factor: 7.185 ISSN: 2582-3930

VPN : BOON OR A TRAP?

Prem Sanjay Lingayat

Guide: Asst. Prof. Gauri Ansurkar

Keraleeya Samajam's Model College, Khambalpada Road, Thakurli, Dombivli (East), Kanchangaon, Maharashtra

ABSTRACT

In moment's world, the security and sequestration of data that peregrination through the cyberspace have come an essential concern for the individual druggies and the associations. Piecemeal from this, the government of numerous countries has also assessed numerous Suppression rules on the way their citizens should use the Internet. All this has redounded in VPNs (Virtual Private Network) getting veritably popular as it allows the druggies and associations to secure and circumvent their Internet connection to a great extent. In this paper, we substantially study three types of utmost common VPNs and present a relative study of their features, performance, security and a many other aspects. We hope that our exploration will offer a clear understanding of the druggies and will help them make their decision on choosing the correct VPN grounded on their need and precedence regarding security, speed, and cost

INDEX TERM

Encryption, security, devices, threats

1. INTRODUCTION

VPN (Virtual Private Network) is a networking armature which is enforced over public network to support sequestration in participated public network, it surfaced as a cost effective and dependable result in networking and telecommunication associations.VPN are most favorable part of any IT assiduity because it saves the huge cost of structure by using the public Internet to establish largely secure communication medium from corporateoffice to remote spots and remote druggies.

Tunneling protocol provides a secure mode of transport for the network services which essential network doesn't support directly (10). The VPN service can be looked from the perspective of different stockholders, presenting the views of the stoner, client, network provider and service provider (4).VPN establishes a logical secure channel (3) for communication between two realities over Internet by using the system of tunneling, which encapsulates the IP datagram into a tunneling

protocol therefore hiding the original data from meddler or hacker who are present in nearly all the networks.
It nearly establishes a point-to- point or multipoint link between the communicating parties in both the transmitting and entering ends through public or participated communication network. Traditional VPN uses DES (Data Encryption Standard), AES (Advance Encryption Standard) and Blowfish algorithm for encryption of stoner's data. The link in whichencrypted and encapsulated data is transferred is known as VPN connection.

2. BACKGROUND AND DEVELOPMENT

Many decades ago, VPN was proposed as new conception to harness the great convenience and vacuity of the Internet similar that it can be used as secure medium for private disposal. VPN creates a logical private network under public communication network which reduces the need of expensive leased lines connections for businesses and associations. Moment VPN is being used byalmost all businesses who bear to geographically expand their operation without important investing in IT structure. Utmost merchandisers similar as Cisco, Checkpoint and Microsoft,etc. began developing similar product that give secure channel to the business for their development requirements. Beforehand VPN development was functional in personal terrain, the system of encryption and their supported protocols made it either a veritably good choice or a bad one because it can be fluently compromised. Currently, IPsec- grounded VPN came an assiduity standard because IPsec along with its relative protocol provides acceptable encryption, complexity and security to insure that data integrity is maintained throughout the session (9).

VPN enables a computer or network- enabled device to securely shoot and admit data across participated or public networks as if it is directly connected to the private network, while serving from the functionality, usability and operation programs of the public network (5). Stoner data may contain private information, nonpublic train, voice, videotape and most importantly fiscal deals. So security of stoner data needs to be assured, the generally enforced VPN remains confined to DES (Data Encryption Norms) encryption algorithm for encryption of stoner data inside an reprised lair packet. DES is considered as largely complex and infeasible to decrypt without knowing the keys, it also been proved that indeed a supercomputer will took times to decipher a single DES translated packet. But we should also consider the growth of the computer technologies and its affiliated trouble. To further enhance the security of stoner's data in a VPN title, a complex algorithm is demanded to help data tampering indeed in the case of compromised link. Multi-phase encryption algorithmprovides such a complex and robust medium to secure data inside a packet by performing encryption using different encryption algorithm in multiple position and multiple times, which is also been proven as veritably secure mode of encryption by using the standard encryption fashion. In multiphase encryption fashion, indeed an outdated algorithm can be used to enhance the complexity of cipher textbook and overall timber more secure packet.

3. Part OF MULTIPHASE ENCRYPTION

TECHNIQUE IN VPN SECURITY

Multi-phase encryption algorithm is proven to be more secure as compare to traditional encryption ways similar as DES (Data

Encryption Standard), AES (Advance Encryption Standard), and DSS (Digital Hand Algorithm). By using this approach of encryption we will insure the confidentiality and integrityof thevaluable stoner's data inside an reprised packet of the lair which is used by the VPN. The proposed fashion won't intrude any operations of the VPN and its tunneling process rather it only applies to contained stoner data by the lair reprised packet, by applying multiple encryption multiple times produced cipher- textbook is largely complex and tamperproof. When applying this fashion with the stoner data in each packet of the session will produce a largely complex and unbreakable cipher- textbook, which will be veritably sophisticated for the meddler to break or reverse the algorithm. Thus, druggies will be served with the enhanced security of their precious data. Businesses similar ase-commerce, health care, legal,etc. they all can suitable to get the advantage of the public communication network without compromising their confidentiality and sequestration. The proposed fashion will offer largely complex, secure, and tamperproof result for those guests who are more concerned about their sequestration.

In addition of business associations, military operations similar as in case of disaster, terrorist attack, commandeer,etc. can also be served by the VPN and its proposed encryption fashion.

4. TYPES OF VPN

A.MPLS VPN

It is an IPSec VPN based on MPLS (Multiprotocol Label Switching) technology. It is an implementation of the IP Virtual Private Network (IP VPN) which uses MPLS technology on network routing and switching equipment, simplifies the routing of core routers, and uses label switching in combination with traditional routing technology. The best thing about MPLS is that it uses a combination of switching and routing technology that comes from Layer 2 and 3 of OSI technology producing a high performance when addressing the significant issues of VPN, such as service classification and traffic engineering. Therefore, MPLS VPN is increasingly preferred by the operators in settlement of enterprise interconnection and providing a variety of new business.

B. SSL VPN

SSL (Secure Sockets Layer) VPN is a VPN technology based on HTTPS (Secure HTTP that supports SSL HTTP protocol) and works between the layer 4 (transport layer) and layer 7 (application layer) of OSI layers. To establish a connection that is secure for communication between application tiers, SSL VPN uses the certificate-based authentication, data encryption, and message integrity verification mechanisms provided by the SSL protocol. The use of SSL VPN is mostly in Web-based remote security access. It makes sure that the users get secure remote access to the company's internal network.

C. IPSec VPN

The basis of IPSec VPN is IPSec (Internet Protocol Security) protocol, which provides the tunnel security. IPSec is an end-to-end approach designed by IETF (Internet Engineering Task Force). It uses IP communication to make sure our data is secure by providing high quality, compatible, and cryptography based security to the information that is transmitted over the network.

5. HYPOTHESIS TESTING

Hypothesis testing is a sort of statistical reasoning that includes analysing data from a sample to derive inferences about a population parameter or probability distribution. First, a hypothesis is created regarding the parameter or distribution.

This is known as the null hypothesis, abbreviated as H0. After that, an alternative hypothesis (denoted Ha) is defined, which is the polar opposite of the null hypothesis. Using sample data, the hypothesis-testing technique determines whether or not H0 may be rejected. The statistical conclusion is that the alternative hypothesis Ha is true if H0 is rejected.

For this paper,

Null hypothesis (H0): Smart devices are very secure and can be trusted with our privacy.

Alternative hypothesis (Ha): Smart devices are not secure and cannot be trusted with our privacy.

TEST (STATISTICS)

There are 3 tests available to determine if the null hypothesis is to be rejected or not. They are:

1. Chi-squared test
2. T-student test (T-test)
3. Fisher's Z test.

For this paper, we will be using a 2 tailed T-student test.

A t-test is an inferential statistic that determines if there is a significant difference in the means of two groups that are related in some manner.

- **Level of significance**

(also known as alpha or α). A significance level of 0.05, for example, means there's a 5% probability of discovering a difference when there isn't one. Lower significance levels indicate that more evidence is required to reject the null hypothesis.

- **Level of confidence**

The confidence level indicates the probability that the location of a statistical parameter (such as the arithmetic mean) measured in a sample survey is also true for the entire population.

Sr. No.	Data
1	88.1
2	85.3
3	58.7
4	37.6
5	67.9
6	71.6
7	66.1
8	84.4
9	57.8
Mean (x)	68.61111111
Standard Deviation (s)	16.20250324

Level of significance = 0.05 i.e. 5% Level of confidence = 95%

The chance of rejecting the null hypothesis when it is true is the significance level

A t-score (t-value) is the number of standard deviations away from the t-mean. distribution's.

The formula to find t-score is:

$t = (x-\mu) / (s/\sqrt{n})$

where x is the sample mean,

μ is the hypothesized mean,

s is the sample standard deviation, and n is the sample size.

The p-value, also known as the probability value, indicates how probable your data is to have happened under the null hypothesis. Once we know the value of t, we can find the corresponding p-value. If the p-value is less than some alpha level (common choices are .01, .05, and .10) then we can reject the null hypothesis and conclude that smart devices are not secure and cannot be trusted with our privacy.

Calculating t-value:

Step 1: Determine what the null and alternative hypotheses are.

Null hypothesis (H0): Smart devices are very secure and can be trusted with our privacy.

Alternative hypothesis (Ha): Smart devices are not secure and cannot be trusted with our privacy.

Step 2: Find the test statistic.
In this case, the hypothesized mean value is considered 0.

$t = (x-\mu) / (s/\sqrt{n}) = (68.61-0) / (16.202/\sqrt{9})$
$= 12.704$

t-value = 12.704

Calculating p-value:

Step 3: Calculate the test statistic's p- value.

The t-Distribution table with n-1 degrees of freedom is used to calculate the p-value. In this paper, the sample size is n = 9, so n- 1 = 8.

By plugging the observed value in the calculator, it returns a p-value. In this case, the p-value returned is less than 0.00001.

Since this p-value is less than our chosen alpha level of 0.05, we can reject the null hypothesis. Thus, we

have sufficient evidence to say that smart devices are not secure and cannot be trusted with our privacy.

6. CONCLUSION

As a result of this study, we've concluded that it isn't easy to judge one VPN against the other because each one of them has some advantages and disadvantages. It also depends on the type of druggies and their conditions regarding how important security they want and how important plutocrat are they ready to spend to get what they need in a VPN? Still, leaving away those conditions, we can conclude that IPSec VPN, is the most common VPN and it's largely secured indeed though it has not been suitable to achieve the fine-granulated access control yet. Still, at the same time, it can hardly be considered as extraordinary regarding the quality of services, convenience, scalability, cost- effectiveness, and maintainability. SSL VPN is the most secure bone among the three that we studied, but it can not guarantee the quality of service as anticipated. Still, there are numerous other advantages of SSL that outmatch this Disfigurement. Not only it's ready to use, but the scalability of it's also beyond normal. At the same time, it costs the least and requires nearly zero conservation. MPLS VPN is the least safe among the three VPNs, but it provides perfect service that uses two or further original area networks. The scalability of MPLS is also the stylish among the three, and the only part of it that needs conservation is the CE router. Still, the price of MPLS VPN isn't doable at all. In our opinion, SSL VPN is the stylish choice of VPN in general. The other two clearly have their places in the request to grow which leads to farther options for unborn studies that may include whether or not we can optimize the algorithms behind these VPNs so that we can remove their Sins and the end stoner can get further value for their plutocrat or their conditions.

7. REFERENCES

(1) Chen Juan, Wei Yiliang. " Exploration on mixed encryption algorithm grounded on IPSec VPN data security." Railway Computer Application Research and Development,vol. 19No. 3, March 2010.

(2) Chris Partsenidis, " History of VPN Disadvantages of early virtual private network, Search Enterprise WAN",
http//searchenterprisewan.techtarget.com/tip/A-history-of-VPNDisadvantages-of-early-virtual-private-networks

(3) Gupta, Himanshu, and Vinod Kumar Sharma. " Part of multiple encryptions in a secure electronic sale". International Journal of Network Security & Its Operations (IJNSA)3.6 (2011), 89-- 96.

(4) Li, Xiupeng. " Differences between Proxy, VPN, and SSH." (blog)
http//blog.csdn.net/map_lixiupeng/article/details/41695045, 2014

(5) Max Eddy. " You Need a VPN and Then's Why".
http//.December 2017.

(6) Min, Tong, Qingrong Li and Youqun,Mo. " Security Study of VPN"
Computer Period,vol. 12,pp.1-3, 2002.

(7) Philipp Winter, Tobias Pulls, Juergen Fuss, " ScrambleSuit a polymorphic network protocol to circumvent suppression", Proceedings of the 12th ACM factory on Factory on sequestration in the electronic society, November 04-04, 2013, Berlin, Germany

(8) Roger Dingledine and Nick Mathewson. " Design of a blocking-resistant Obscurity system. Specialized report ", The Tor Project, 2006.

(9) Singh, Arun Kumar, Shefalika Ghosh Samaddar, and ArunK. Misra. " Enhancing VPN security through security policy operation", 1st International Conference on Recent Advances in Information Technology (RAIT), 2012

(10) Wang, Guoqiang, " The benefits of VPN network can bring to druggies" (blog) http//blog.sina.com.cn/ s/blog_4a857b6f0100g6l5. html

(11) Zongkun, Dai. " VPN and Network Security" Academics and Technology, pp. 23-24,Feb. 2001