Proceedings of the Second International Conference on Computing Methodologies and Communication (ICCMC 2018)
IEEE Conference Record # 42656; IEEE Xplore ISBN:978-1-5386-3452-3

VPN: a Boon or Trap?

A Comparative Study of MPLS, IPSec, and SSL Virtual Private Networks

Zhang Zhipeng (Zzhang36@nyit.edu), Sonali Chandel (schandel@nyit.edu), Sun Jingyao (jsun19@nyit.edu), Yan Shilin (syan05@nyit.edu), Yu Yunnan (yyu18@nyit.edu), Zang Jingji (jzang@nyit.edu)

School of Engineering and Computing Sciences, New York Institute of Technology, Nanjing, China

***Abstract* - In today's world, the security and privacy of data that travels through the cyberspace have become an essential concern for the individual users and the organizations. Apart from this, the government of many countries has also imposed many censorship rules on the way their citizens should use the Internet. All this has resulted in VPNs (Virtual Private Network) becoming very popular as it allows the users and organizations to secure and circumvent their Internet connection to a great extent. In this paper, we mainly study three types of most common VPNs and present a comparative study of their features, performance, security and a few other aspects. We hope that our research will offer a clear understanding of the users and will help them make their decision on choosing the correct VPN based on their need and priority regarding security, speed, and cost.**

Keywords – VPN, MPLS, IPSec, SSL, Network Security

I. INTRODUCTION

In the present times, staying connected to the Internet 24x7 has become as crucial as breathing. Our privacy and the security of our data comes under potential threat of many types as a result of being connected to the Internet all the time through multiple devices. These risks may include user's data being hacked, lost or exposed by the cybercriminals or coming under surveillance by the government or some secret services. There is another major issue that is affecting many netizens these days. Contrary to popular belief by a substantial percentage of people in the developed countries that the Internet is freely accessible for everyone around the globe round the clock, there is a considerable size of the world population that has got controlled access to the Internet, because of their location. For example, The Great Fire Wall (GFW) has been preventing Internet users in China from accessing many foreign websites ever since 2008. In the latest survey conducted by Freedom House, a US state-funded non-profit organization, China ranks worst in the world for Internet freedom. However, it is not the only country which poses strict Internet restrictions and surveillance upon its citizens. Countries like North Korea, Syria, Ethiopia, Iran, and Cuba, rank very high on this list as well.

So what is the solution to all these cyber threats and control of the cyberspace by a specific group of people who are more equipped than a general user? Use of a Virtual Private Network or VPN, in short, is the answer to all these issues to a greater extent. It not only allows better security but it can also provide anonymity and privacy to its user at any time, anywhere. There is no limit to who can use this or who cannot as there is something for everyone, ranging from students to home users to travelers to small businesses to large organizations. A VPN can cater to everyone's needs depending on what they are looking. As a result, VPN has become very popular in the last few years with an increased rate of cybercrime and government surveillance throughout the world. A VPN is a virtual encrypted tunnel between the user and a remote server operated by a VPN service. [4] All external internet traffic is routed through this tunnel, so our data becomes safe from the data hunters. On the other hand, the IP address of the VPN server becomes our IP address, enabling us to hide our actual identity.

In this paper, we have presented our research on the development, technology, and impact of VPN and Firewalls. The paper presents a brief analysis of three different VPNs namely, MPLS, IPSec, and SSL. Also, the article illustrates how these three VPNs work concerning their security, quality of service, convenience, scalability, cost-efficiency, and maintainability. By comparing the advantages and disadvantages of these algorithms, we also explain the algorithms behind these three VPNs. We have evaluated their performance regarding encryption speed, stability, availability, and security. Our study also aims to provide their security implementation modes. We have assessed the safety of these three VPNs regarding their confidentiality of connection and transmission data, the authenticity of data, source of data, and their access control methods.

II. DEVELOPMENT

In its initial days, VPNs were used to meet companies' increasing demand of providing faster and flexible networking system to its employees as modern enterprises certainly need higher efficiency in communication. In addition to that, the need for enhanced security, scalability and profit also accelerated the birth of VPN. A VPN depends on ISP (Internet Service Provider) and other NSP (Network Service Provider) to create encrypted and dedicated data communication networks as a part of public networks, namely logical Virtual Private Network. The development of VPN has been affected by two significant technologies namely, Data Compression & Package technology, and Multiline Multiplex & Smart Routing technology. The Data Compression & Package technology has introduced the concept of new redundant data by re-encrypting the plaintext packets, resulting in lowering the transmission efficiency of the VPN by 20-30% compared to that of the plaintext transmission efficiency. By compression of the application layer data and package, the transmission

performance of VPNs can be improved, and therefore make it faster than the transmission in plaintext. In present times, data reduction and packet technology have become very popular in quite a few innovative VPNs. Multiline Multiplex and Smart Routing technology have accelerated the speed of VPN networking as well. It refers to those VPN devices which can support multiple WAN (Wide Area Network) lines at the same time. By bundling multiple lines into a high-bandwidth line, multiline multiplexing technology provides users with a bandwidth guarantee. At the same time, multi-line backup technology can ensure high availability of the line, even if one or more lines fail. So as long as one line is free, the user's business will not be interrupted. [3]

III. 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.

IV. How Does VPN Work

The mainstream applications that claim to provide VPN services are using one of the following three techniques: proxy, IPSec, and SSH.

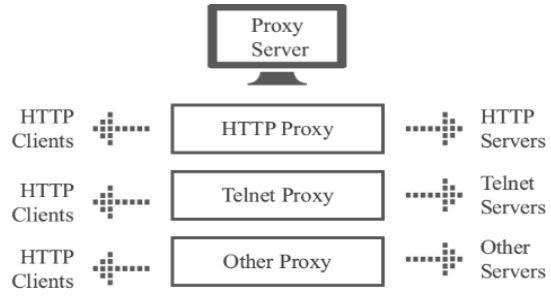

Fig 1. Proxy Server

A. Proxy Server

A proxy server is like a courier service which is responsible for nothing but transcending the message. The work of proxy servers is conducted in the HTTP layer and Socket layer in the open system interconnection model under most circumstances. Fig 1 explains how proxy server functions.

B. IPSec

IP security is the most common method used by the VPN applications. It works in the third layer of the Open System Interconnection (OSI) model, which is the Network layer.

C. SSH

It is an encrypted channel that needs to be combined with the proxy server to overcome the blocked network. Hence the tool that is used to scale the blocked network which is usually called SSH is, in fact, an SSH agent. In other words, an SSH agent equals to an agent and SSH together. It can be considered as an encrypted agent, where the package is kept in a safe case while being sent to the courier. In the TCP/IP five-tier model, SSH is the security protocol that applies to the application layer and transport layer. SSH is a remote shell, an application based on SSL. Although many people use SSH's to transmit data, they merely use the SSL proxy function of SSHD software to get this job done.

V. Analysis of Various Features of VPN

A. Security

The core function of IPSec VPN is providing the security mechanisms like data encryption, data certification, and data verification. It allows any application to make full use of its security features without modification. However, all of the access resources are available for remote users after building a tunnel between two sites in IPSec VPN, and it cannot achieve the fine-grained access control, which results in security risk. The emphasis of SSL VPN is on the protection of sensitive data, which leads to controlling the different levels of user access to the users based on their identity. The browser-based access of SSL VPN means that we can access the network resources from any computer at anywhere. It improves the working efficiency, but it also exposes the Internet to many machines with unknown security state. MPLS VPN can complete the security tunnel by using various methods such as route isolation, address and information hiding. However, it does not provide security services like encryption and

TABLE 1. COMPARISON OF DIFFERENT VPN'S PERFORMANCE

Types	IPSec VPN	SSL VPN	MPLS VPN
Security	1) High 2) Providing the security mechanisms data encryption, data certification, data verification 3) Cannot achieve the fine-grained access control	1) Higher 2) Protection of sensitive data 3) Accessing the network resources from any computer anywhere 4) Improves the working efficiency 5) Exposes the Internet to countless computers with unknown security state	1) Average 2) Completing the security tunnel by route isolation, address hiding, information 3) Cannot provide security services: encryption, certification 4) Transmitting data in plain text which may lead to some security issues
Quality of Service	1) Cannot be guaranteed 2) IPSec tunnel technology uses differentiated service model to realize the limited quality of service 3) May lose data packet seriously, even cannot work normally	1) Cannot be guaranteed 2) Improving the performance of SSL handshake protocol: Session reuse, Sache handshake protocol parameters, and Accelerators	1) Perfect 2) Providing two aspects: Predictable performance and Policy applications
Convenience	1) Must install the client software and configure it 2) Incompatible with each other	1) Directly using the Web browser 2) Need not to install the client software	1) Used in two or more local area networks 2) Need not to install the client software
Scalability	1) Average 2) Modifying data in IP header, Transmission header and Transmitting procedure 3) Cannot support expansion of complex networks	1) Good 2) Designed for mobile users and massive users 3) Any authorized users can access resources as long as the server installs SSL VPN gateway	1) Best 2) VPN providers can configure the mesh network of MPLS VPN into full mesh easily 3) Users can keep using the original tag without changes due to that addresses are taken place by tags
Cost-efficiency	1) Not so cost-efficient 2) Needing to deploy VPN gateway device between two organizations	1) Most cost-efficient 2) Only requiring to implement VPN gateway device on the server-side	1) Least cost-efficient 2) Making the cost of access reduces exponentially 3) Charging for one-access and monthly rent
Maintainability	Relatively poor	1) Best 2) Zero maintenance	1) Good 2) Only need to maintain CE router

certification. Data gets transmitted in plain text which may lead to some security issues.

B. Quality of Service

Quality of Service (QoS) is a technology used to solve problems such as network latency and congestion. IPSec VPN and SSL VPN implement encryption and authentication services, and they use IP data transmission jumping step by step, which affects the transmission speed. However, quality of service cannot be guaranteed. MPLS VPN can implement high-speed switching in the backbone network, so it has a better QoS performance.

C. Convenience

Users of IPSec VPN have to install the client software and its configuration. Different IPSec VPN's manufacturer's client software may not be compatible with each other. SSL VPN directly uses the Web browser and does not need to install the client software. MPLS VPN is mainly used in two or more local area networks. Different LAN users seem to be on the same network, and there is no need to install the client software to access it.

D. Scalability

IPSec VPN modifies data in IP header, in transmission header and even in transmitting procedure so that it works. IP packets which have been processed by IPSec do not support the expansion of complex networks. Therefore, it has overall scalability. SSL VPN is designed for mobile users and massive users. Any authorized users can access resources as long as the server installs SSL VPN gateway. Therefore, SSL VPN has good scalability. The mesh network of MPLS VPN can be configured into full mesh easily by VPN providers. The corporations link CPE (Customer Premise Equipment) to ISP and make no complicated configurations. Simple arrangements and adjustments are done between CPE and ISP when new CPE enters in. Meanwhile, users can keep using the original tag without changes. Therefore, MPLS VPN has the best scalability.

E. Cost-efficiency

SSL VPN is the most cost-efficient one because it only needs to deploy VPN gateway device on the server-side. IPSec VPN usually requires implementing VPN gateway device between two organizations which are not so cost-efficient. On the other hand, MPLS VPN may cost less than dedicated access, but it charges monthly rent for access which makes it the most expensive among the three.

F. Maintainability

From the aspect of the server maintenance, there are not many differences among these three VPNs. From the client's perspective, IPSec VPN needs to maintain client software, so its maintainability is relatively weak. SSL VPN is zero maintenance, which suggests an absolute advantage over the other two kinds of VPNs. MPLS VPN has good maintainability

as well because the users only need to maintain CE router while MPLS VPN service providers can manage the others.

VI. Pros and Cons of Using A VPN

Despite all the drawbacks of VPN, there is no denying that it can be a powerful tool in many terms. The disadvantages and advantages for users are listed in Table 2 [2] and Table 3 [5] [10].

VII. Algorithms behind These VPNs

A. Genetic Algorithm for data network planning model in MPLS VPN

A genetic algorithm (GA) is repeatedly applied to solve optimization problems (constrained and unconstrained) based on a random natural selection process and genetic search algorithm to improve a population of individual solution over a period. It puts evolution principle of "select the superior and eliminate the inferior" into optimizing the parameters of the formation of the encoded string. Using a particular function and a series of genetic screening for each individual, it succeeds in producing new groups of individuals that contains better information and new and better individuals from the previous generation. Fig. 2 shows the optimal solution for optimal parameters of the group.

B. Algorithm for IPSec VPN

It is a mixed encryption algorithm which is composed of Advanced Encryption Standard (AES) that belongs to the symmetric algorithm and Elliptic Curve Cryptography (ECC) which belongs to the asymmetric algorithm [1]. Table 4 shows a comparison of the advantages and disadvantages of AES and ECC. Data encryption uses AES to satisfy the requirements of fast and efficient processing that crypto-operations and decryption operations need. The encryption key is disposable. When VPN delivers data, the sender generates a key randomly. Then keys created according to AES are encrypted by ECC again so that processes of key exchange and administration can be simplified. In the end, VPN sends encrypted data to the receiver. Fig. 3 [1] and Fig. 4 [1] describe specific processes of the mixed encryption algorithm.

TABLE 2 THE DISADVANTAGES OF VPN

Disadvantages	Features
Not for anonymity	Was not designed at all for anonymity, it is a single, supplemental tool instead of a privacy solution
Unsafe	Some VPN does not provide peer-to-peer sharing which might turn in usernames to a copyright holder if required
Don't offer robust protection from ad tracking	Some cheap/ free VPNs do not protect against malware and ad trackers
Could put us at risk	Poor configuration of VPN could give direct access to hackers to our personal LANs
Pre-shared keys	People know the pre-shared key for the VPN and control the Wi-Fi access point can quickly attack ou VPN
Use the obsolete PPTP VPN protocol	The usage of the old protocol might put us in trouble
Data retention/logging	Local data storage/ cache data/cookies on user's computer can lead to loss of user's anonymity
Leakage	Some of the outgoing packets might miss the VPN tunnel, which could compromise their privacy
Marketing Hype	Users who cloaked their IP addresses unwillingly became VPN exit nodes or endpoints.

TABLE 3 THE ADVANTAGES OF VPN

Benefits	Features	
Cost saving	The savings of dedicated line costs	
	Savings in equipment investment	
	Support cost savings	
	Saving mobile communication costs	
The enhanced security	Data communication security	Tunneling
		Encryption & Decryption
		Key Management
		Authentication
	User authentication security technology	PAP
		CHAP
		SPAP
		MS-CHAP
		EAP
	Data encryption and ke management	MPPE
		IPSec
	Separate the highly sensitive data server data server	
Network protocol support	Support almost all kinds of network protocols	
Easy to extend	Companies can just let NSP responsible for all the work to enlarge the capacity and coverage of the VPN	
Feel free to connect with your partner with network	VPN expand and extend flexible	
Full control of the initiative	Businesses can use the facilities and services of ISP; they can also fully control their networks by using a VPN.	
Secure IP address	Users on the Internet can only see the public IP address but not the proprietary network addresses included in the packet	
Support for emerging applications	VPN can support all kinds of advanced applications	

TABLE 4 COMPARISON OF SYMMETRIC AND ASYMMETRIC ALGORITHM

Performance	Symmetric Algorithm(AES)	Asymmetric Algorithm(ECC)
Encryption Speed	Very fast	Slow
Key Relationships	Same encryption and decryption key	Different encryption and decryption key
Key Administration	Difficult	Easy
Key Delivery	Required	Not required
Digital Signature	Unworkable	Workable
Main Applications	Encryption for mass data	Encryption for files, digital signature, and authentication

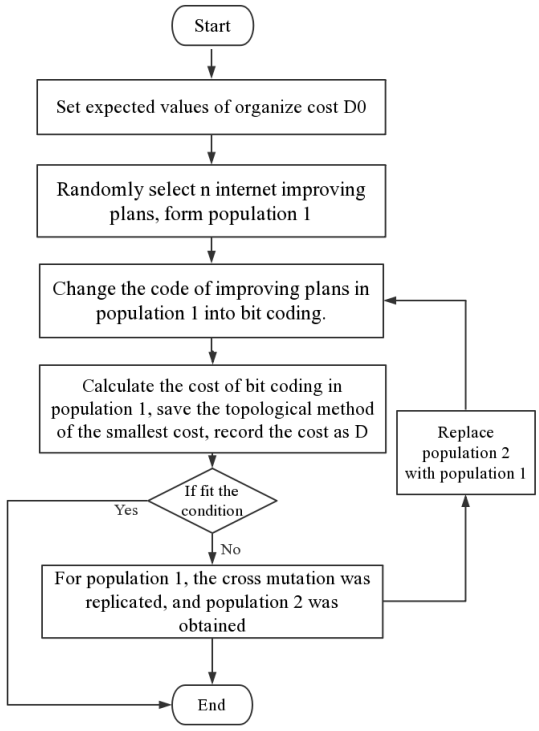

Fig. 2. Flow chart of network planning cost based on genetic algorithm.

VIII. REALIZING VPN SECURITY

There are many security issues of VPN that we have to pay attention [10]. Firstly, from the perspective of the VPN, there are two issues as VPN fingerprinting and unsecured storage of authentication credentials by VPN clients. Using the User Datagram Protocol (UDP) back off fingerprinting, most of the VPN servers can be fingerprinted. The attackers can efficiently use the known loopholes and weaknesses of the device type and software version to attack some particular products utilizing the Vendor identity (ID) fingerprinting or other fingerprinting methods. The authentication credentials that the VPN client's programs offer is the default setting which will repeat every time a new session is initiated. It will bring security risks as bring conveniently. [8] Secondly, from the perspective of the client, there also many issues. The client system becomes very vulnerable because of the presence of the unencrypted username or unencrypted username in the registry as anyone who accesses the client computer can get the access to all this information. The first target is confidentiality of connection and transmission data. It means that the network connection is invisible and hidden, and the content of the connection is unwarranted to the unauthorized user, or invisible. Only authorized users can obtain understandable raw data through password changes or other means. The authenticity of data is the second one. It means the transmission of data within itself without unauthorized generation, insertion, addition, and tampering. The authenticity of the data source is consistent with the actual sender and the claimed sender. The availability of communication resources refers to the ability of users in the

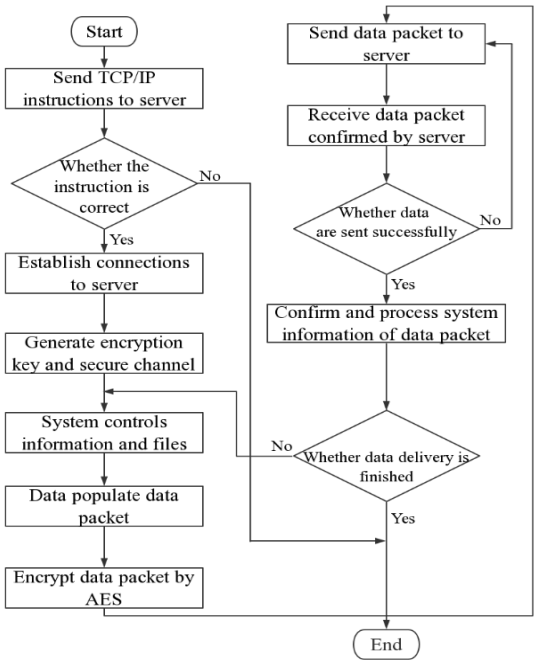

Fig. 3. Mixed Encryption Algorithm for Server-side

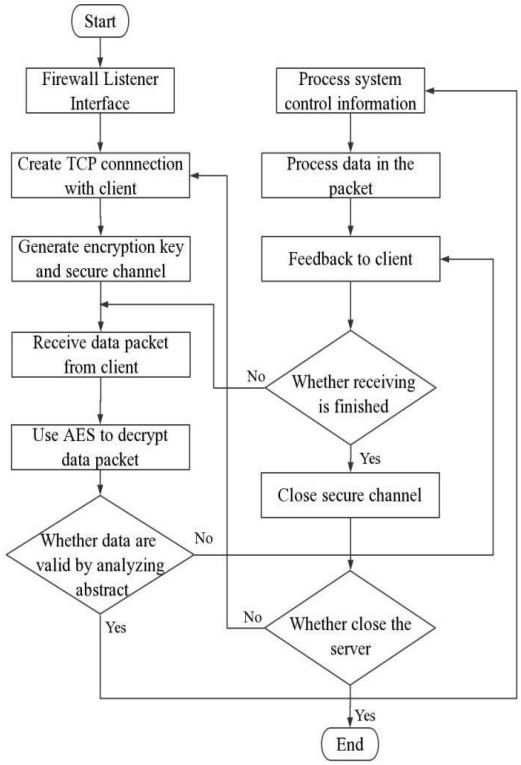

Fig. 4 Mixed Encryption Algorithm for Server-side

common body to receive services when they wish to receive services. The audibility of access is valid logging of access behavior in or outside the interest body and can be used to extract security information from these log records [11].

IX. VPN SECURITY IMPLEMENT MODE

A. Users distrust network operator

Fig. 5 shows that the user is responsible for the security of the data passed by themselves in this case. The protection of VPN data depends on the user's firewall and the safety of the tunnel protocol used by the operators. The operator is only responsible for providing send packet transmission channel at this moment, and not responsible for security. The security of tunnel data is the user's responsibility. [6][9]

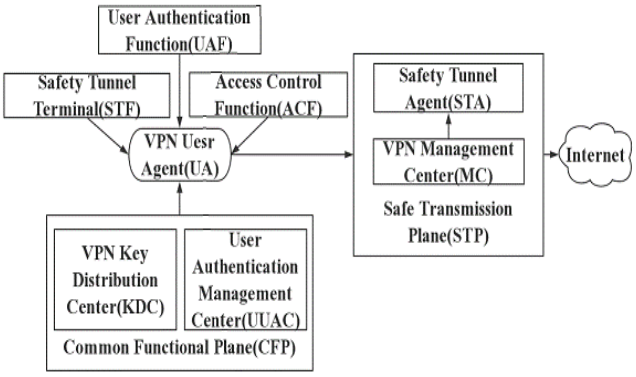

Fig.5. The management structure of VPN system

B. User trust network operators

The traditional VPN, which base on frame relay and ATM are both assume the operators are trustworthy. In this case, the provision of firewall functionality and the security guarantee for packet transmission are provided by the operator. If a VPN is based on the network, the operator is responsible for the security between the two edges (PE) of the operator, which does not include the protection of the user access link. If it is a VPN based on the user equipment (CE), the operator is responsible for ensuring the safety of CE devices to PE devices, including the security of the user access link, which is a CE based management VPN. Operators can use different levels of security on various occasions. If the operator believes that the path between CE and CE or PE and PE is inherently safe, it is not necessary to provide the tunnel security services between the backbone nodes with high-security mechanisms. If VPN data passes across multiple carriers' backbone, it is essential to use a high-level security mechanism. [6][7]

X. CONCLUSION

As a result of this study, we have concluded that it is not 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 users and their requirements regarding how much security they want and how much money are they ready to spend to get what they need in a VPN? However, leaving aside those requirements, we can conclude that IPSec VPN, is the most common VPN and it is highly secured even though it has not been able to achieve the fine-grained access control yet. However, at the same time, it can hardly be considered as extraordinary regarding the quality of services, convenience, scalability, cost-efficiency, and maintainability. SSL VPN is the most secure one among the three that we studied, but it cannot guarantee the quality of service as expected. However, there are many other advantages of SSL that outshine this defect. Not only it is ready to use, but the scalability of it is also beyond average. At the same time, it costs the least and requires almost zero maintenance. MPLS VPN is the least safe among the three VPNs, but it provides perfect service that uses two or more local area networks. The scalability of MPLS is also the best among the three, and the only part of it that needs maintenance is the CE router. However, the price of MPLS VPN is not feasible at all. In our opinion, SSL VPN is the best choice of VPN in general. The other two certainly have their places in the market to grow which leads to further options for future studies that may include whether or not we can optimize the algorithms behind these VPNs so that we can remove their weaknesses and the end user can get more value for their money or their requirements.

REFERENCES

[1] Chen Juan, Wei Yiliang. “Research on mixed encryption algorithm based on IPSec VPN data security.” *Railway Computer Application: Research and Development*, vol.19 No. 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-VPN-Disadvantages-of-early-virtual-private-networks

[3] Gupta, Himanshu, and Vinod Kumar Sharma. “Role of multiple encryptions in a secure electronic transaction”. *International Journal of Network Security & Its Applications (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 Here’s Why”. http://uk.pcmag.com/privacy/88655/feature/you-need-a-vpn-and-here, December 2017.

[6] Min, Tong, Qingrong Li and Youqun, Mo. “Security Study of VPN” *Computer Era, vol. 12*, pp.1-3, 2002.

[7] Philipp Winter, Tobias Pulls, Juergen Fuss, “ScrambleSuit: a polymorphic network protocol to circumvent censorship”, *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society, November 04-04*, 2013, Berlin, Germany

[8] Roger Dingledine and Nick Mathewson. “Design of a blocking-resistant anonymity system. Technical report”, *The Tor Project*, 2006.

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

[10] Wang, Guoqiang, “The benefits of VPN network can bring to users” (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