Journal of Artificial Intelligence and Cyber Security (JAICS)
An International Open Access, Peer-Reviewed, Refereed Journal

Virtual Private Network (VPN)

[1] Mr. P. T. Talole Sir, [2]Vinesh Chavhan, [3] Rushikesh Kanfade, [4] Vaibhav Wanere

[1] *Head of Department , Information Technology ,Anuradha Engineering College, Chikhali* [2,3,4] *Under Graduate Student, Department of Information Technology, Anuradha Engineering College, Chikhali, Maharashtra, India.*

[1]pramod.talole@aecc.ac.in, [2]vineshchavhan7499@gmail.com ,
[3]rushikeshkanfade123@gmail.com , [4] vaibhavwanere777@gmail.com

ABSTRACT: This study aimed to identify the differences between state of the art VPN solutions on different operating systems. It was done because a novel VPN protocol is in the early stages of release and a comparison of it, to other current VPN solutions is interesting. It is interesting because current VPN solutions are well established and have existed for a while and the new protocol stirs the pot in the VPN field. Therefore a contemporary comparison between them could aid system administrators when choosing which VPN to implement. To choose the right VPN solution for the occasion could increase performance for the users and save costs for organizations who wish to deploy VPNs. With the remote workforce increasing issues of network reliability also increases, due to wireless connections and networks beyond the control of companies. This emands an answer to the question how do VPN solutions differ in performance with stable and unstable networks?

This work attempted to answer this question. This study is generally concerning VPN performance but mainly how the specific solutions perform under unreliable network conditions. It was achieved by researching past comparisons of VPN solutions to identify what metrics to analyse and which VPN solutions have been recommended. Then a test bed was created in a lab network to control the network when testing, so the different VPN implementations and operating systems have the same premise. To establish baseline results, performance testing was done on the network without VPNs, then the VPNs were tested under reliable network conditions and then with unreliable network conditions. The results of that were compared and analysed,

Keywords: Virtual Private Network, VPN, Wire-Guard, IPSec, OpenVPN, Performance, Unreliability, Packet Loss, Delay. Introduction

I. INTRODUCTION

A Virtual Private Networks (VPN) is a way to extend a private network through a public network such as the Internet. Users may then use the VPN to access data on the private network through the Internet as if they are directly connected to the private network. It is understood that using a VPN may reduce performance of the network connection, due to the fact that VPN adds encryption overhead which will increase the latency. The performance is sacrificed to achieve a higher degree of privacy. By examining different VPN implementations, we can find out how much the performance degrades. According to a study by two companies Flex Jobs and Global Workplace Analytic in 2017, more and more

employees are working from home: Between 2005 and 2015 telecommuting grew by 115%. An on-site user that is working on corporate network infrastructure, which is controlled and maintained by the corporation will likely have a more stable connection than the remote worker. A remote worker may use different types of connections that are not managed by the remote workers company. This could lead to an unstable network connection as it is not controlled by professionals directly, as they preferrably are on-site. Considering this scenario, VPN can potentially differ in performance if the connection is unreliable. The fact that the amount of remote workers is increasing and that VPN is a multi-billion-dollar industry, which is also projected to grow further according to Khan et al. (2018), begs the question to be answered; how does the performance of certain VPN implementations differ? This project compares state-of-the-art VPNs and how they differ in performance under normal and unreliable network conditions on different operating systems (OSs). The performance is measured in throughput and degradation is measured in how much, if any, performance was lost after the connection unreliability were introduced. The results are intended to be used as an aid to system administrators when to evaluate the options for which VPN solution to deploy. The results can be used as a steppingstone to create other VPN experiments and to avoid pitfalls that were discovered in this study. If a system administrator intends to use the same configuration as in this study, then the results can be beneficial without having to do their own testing.

II. HISTORY OF VPN

The technology for implementing VPNs has been in existence for some time. Their origins can be found in the Virtual Circuit. Virtual circuits are easy to implement in highly connected networks as well as being cost effective. We will see that these benefits also apply to VPNs. The virtual circuit was originally produced in the late seventies and early eighties. The basic structure of the virtual circuit is to create a logical path from the source port to the destination port. This path may incorporate many hops between routers for the formation of the circuit. The final, logical path or virtual circuit acts in the same way as a direct connection between the two ports. In this way, two applications could communicate over a shared network. Virtual circuit technology progressed with the addition of encryption equipment to router systems. This new equipment enciphered information between the ports of the virtual circuit. This meant that attackers would not be able to access information in transit between the communicating entities. Later, other security technologies were added such as token authentication. The communication lines were, unfortunately, still open to attack and this lead to the development of secure communication over a public network, a VPN. [6]

III. What is VPN?

A VPN is a supplement of an enterprise's private Internet across a public network such as the Internet, creating a secure private connection, essentially through a private tunnel. VPNs securely convey information across the Internet connecting remote users, branch offices, and business partners into an extended corporate network as shown on figure 1. It will help the users to understand the concepts discussed in this thesis to summarize and return to the basic concepts that distinguish VPN from other components of a networking infrastructure as well as from mere application security solutions:

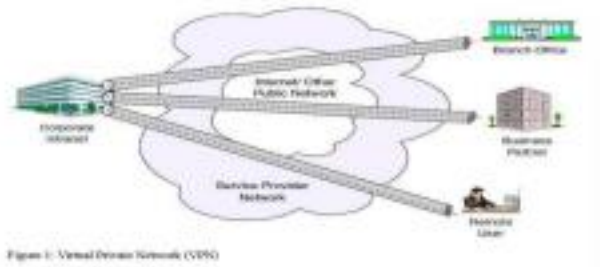

Fig no.1

It is virtual: This means that the physical infrastructure of the network has to be transparent to any VPN connection. In most cases it also means that the physical network is not owned by the user of a VPN but is a public network shared with many other users. To facilitate the necessary transparency to the upper layers, protocol tunnelling techniques are used. To overcome the implications of not owning the physical network, service level agreements with network providers should be established to provide, in the best possible way, the performance and availability requirements needed by the VPN. It is private: Private as a term in the VPN context refers to the privacy of the traffic that is to flow over the VPN. As mentioned before, VPN traffic often flows over public networks (hence the confusion with the world „private") and therefore, precautions must be met to provide the necessary security that is required for any particular traffic profile that is to flow over a VPN connection. Those security requirements include: data encryption, data origin authentication, secure generation and timely refresh of cryptographic keys needed for encryption and authentication, protection against replay of packets and address spoofing. It is a network: Even though not physically existent, a VPN must effectively be perceived and treated as an extension to company's network infrastructure. This means that it must be made available to the rest of the network, to all or a specified subset of its devices and applications, by regular means of topology such as routing and addressing.[2]

IV. Types of Virtual Private Network (VPN) and its Protocols

A. OpenVPN

OpenVPN has become the de facto standard in VPNs today with more than 50 million downloads since its release in 2001 (OpenVPN, 2019). It uses SSL/TLS for key exchange and encryption. OpenVPN is open source, it is secure by the extensive scrutiny it gets by being accessible to anyone who wishes to review the code. In 2017 an independent review of OpenVPN was performed by Cryptography Engineering (Hopkins and Green, 2019), the results found no major vulnerabilities. It supports both TCP and UDP but defaults at UDP. UDP is faster but does not perform error correction as TCP. OpenVPN is fully functional on Windows, macOS and Linux. There is plenty of ciphers and encryption methods to choose from It can be used to connect multiple different networks together in a site-to-site setup.

B. Layer 2 Tunnelling Protocol (L2TP)

The Layer 2 Tunnelling Protocol (L2TP) is one of the emerging techniques for providing a remote connection to the corporate intranet. The L2TP protocol has been developed merging two different protocols: the Point-to-Point Tunnelling Protocol (PPTP) and Layer 2 Forwarding (L2F).

The remote dial-in user scenario is the most common situation for using L2TP. Remote users do not need to make a long-distance call or use a toll-free number to connect directly to the corporate servers but cost constraints suggest the use of ISPs' points of presence (POPs) as a more cost-effective solution. In this case the dial-in user connects to the nearest POP provided by the ISP and then the session is routed through the ISPs and/or the Internet cloud to reach the corporate LAN access. This environment has more than one point of critical security and reliability issues. L2TP provides a technique for building a Point-to-Point Protocol (PPP) tunnel connection that, instead of being terminated at the ISP's nearest POP, is extended to the final corporate intranet access gateway. The tunnel can be initiated either by the remote host or by the ISP's gateway access. L2TP provides a reliable way of connecting remote users in a virtual private network that can support multiprotocol traffic, that is, all the network layer protocols supported by the PPP protocol. Moreover, it provides support for any network layer private addressing scheme for the connection over the Internet.

C. Wire Guard

Wire Guard is the name of a new VPN that aims to replace two of the most widely used VPN solutions, namely OpenVPN and IPSec (Donenfeld, 2018). It claims to be more useful than IPSec while avoiding the complexity of it and by

having better performance than OpenVPN. It was originally written for Linux systems but is now available across more platforms. It is also open source like OpenVPN and IPSec so it also benefits of being open to view for anyone with the knowledge to audit it. It is a design goal to have an overall straight forward configuration like SSH, i.e asymmetric key cryptography.

Wire-Guard also uses state-of-the-art cryptographic algorithms and protocols such as NOISE, BLAKE2 and Curve25519. All this while only being under 4000 lines of code at the time of the whitepaper release (this is excluding cryptographic primitives). According to the official white paper, Wire-guard is currently UDP only (Donenfeld, 2018). Wire-Guard has been sent out for review to be added in the Linux kernel (currently V. 5.0.8 as of writing this). One of the reasons why it was not added before has been addressed by the WireGuard developers. The Linux kernel developer Linus Thorvalds has been praising the quality of WireGuard in the Linux kernel mailing list (2018). That could mean that there is a chance that it will be part of the Linux Kernel soon. However, WireGuard is very young, it was announced as a pre-release in 2018 but already its beginning to draw much positive attention, this could imply that this novel VPN will be true to its claims that it is "faster, simpler and leaner" than the other VPN solutions

D. Remote access VPN

A remote access VPN connection is made by a remote access client. A remote access client is a single computer user who connects to a private network from a remote location. The VPN server provides access to the resources of the network to which the VPN server is connected. The packets sent across the VPN connection originate at the VPN client. The VPN client authenticates itself to the VPN server and, for mutual authentication, the VPN server authenticates itself to the VPN client. Site-to-site VPN: A site-to-site VPN connection connects two portions of a private network or two private networks. For example, this allows an organization to have routed connections with separate offices, or with other organizations, over

the Internet. A routed VPN connection across the Internet logically operates as a dedicated Wide Area Network (WAN) link. [5]

E. Site-to-site VPN

A site-to-site VPN connection connects two portions of a private network or two private networks. For example, this allows an organization to have routed connections with separate offices, or with other organizations, over the Internet. A routed VPN connection across the Internet logically operates as a dedicated Wide Area Network (WAN) link. [5]

F. Point-to-Point Tunnelling Protocol (PPTP)

One of the more "established" techniques for remote connection is the Point-to-Point Tunnelling Protocol (PPTP). PPTP is a vendor solution that meets the requirements for a VPN. PPTP is an extension of the basic PPP protocol (see Figure). It is due to this fact that PPTP does not support multipoint connections, connections must be point-to-point. PPTP does not change the PPP protocol. PPTP only defines a new way, a tunnelled way, of transporting PPP traffic. PPTP is currently being replaced by implementations of L2TP. However, some vendors are still developing solutions with PPTP.[4]

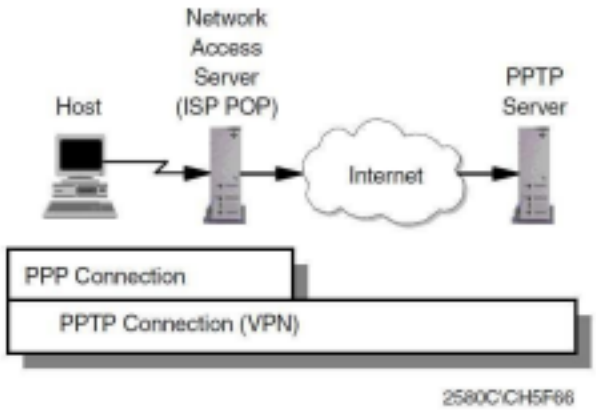

Fig no.2

G. Internet Protocol Security (IPSec)

IPSec offers encryption with the Encapsulating Security Payload (ESP) protocols and uses the Internet Key Exchange (IKE) protocol for key generation and refresh. ESP provides encryption per packet as long as a session is active and offers a choice of low, medium, strong and very strong encryption algorithms, ranging from 40-bit DES to 192-bit triple DES. IKE authenticates the parties that need to exchange secret information based on strong authentication algorithms and also encrypts the key refresh messages. The keys generated by IKE are then used by ESP (and also by AH). ESP optionally provides authentication per packeted replay protection. This makes IPSec encryption much more flexible and secure than traditional PPP authentication options, but it incurs a higher processing overhead at the performing devices. IPSec is the recommended security protocol for L2TP and can be used with L2F and theoretically with PPTP as well. For more information on IPSec AH

and ESP.

V. HOW DOES IT WORK?

A virtual private network is a way to simulate a private network over a public network, such as the Internet. It is called "virtual" because it depends on the use of virtual connections that is, temporary connections that have no real physical presence, but consist of packets routed over various machines on the Internet on an ad hoc basis. Secure virtual connections are created between two machines, a machine and a network, or two networks. Using the Internet for remote access saves a lot of money. It should be done to dial in wherever user Internet service provider (ISP) has a point-of-presence (POP). If an ISP is choosen with nationwide POPs, there's a good chance LAN will be a local phone call away. Some ISPs have expanded internationally as well, or have alliances with ISPs overseas. Even many of the smaller ISPs have tollfree numbers for their roaming users. At the time of this writing, unlimited access dial up PPP accounts, suitable for business use, are around $25 per month per user in America. At any rate, well-chosen ISP accounts should be cheaper than setting up a modem pool for remote users and paying the long-distance bill for roaming users. Even toll-free access from an ISP is typically cheaper than having your own toll-free number, because ISPs purchase hours in bulk from the long-distance companies. In many cases, long-haul connections of networks are done with a leased line, a connection to a frame relay network, or ISDN. It has been mentioned the costs of leasing a "high cap" leased line such as a T1. Frame relay lines can also give to user high speeds without the mileage charges. A connection is bought to a frame cloud, which connects user through switches to destination. Unlike a leased line, the amount that is paid is based more on the bandwidth that's committed to circuit than distance. Frame connections are still somewhat expensive, however. ISDN, like the plain old telephone system, incurs long distance charges. In many locations, the local telephone company charges per minute even for local calls, which again runs expenses up. For situations where corporate office networks are in separate cities, having each office get a T1, frame relay, or ISDN line to an ISP's local POP would be much cheaper than connecting the two offices using these technologies. A VPN could then be instituted between the routers at the two offices, over the Internet. In addition, a VPN will allow user to consolidate Internet and WAN connections into a single router and single line, saving money on equipment and telecommunications infrastructure.[1]

VI. Why we use VPNs?

The major benefit of VPNs, from the consumer's point of view, is that they are considerably cost effective. The alternative to using VPN technology is the high-speed leased line. These lines are expensive, difficult to administrate, and difficult to maintain. Additionally, consider what happens when a leased line fails. The communication between the two parties also fails until the appropriate authorities can repair the line. With Virtual Private technology however, if a node in the path or line between routers goes down, the logical path between the parties is simply changed transparently to the user. Using the Internet as the backbone for communication guarantees reliability of service. The Internet provides further benefit for VPN users. Even extremely remote locations have access to the Internet via dial-up modems. VPNs guarantee secure communication for dial-in users. Mobile users cannot possibly use leased lines for their communication with the corporate site and so VPN technology is the only real solution to this problem. Additionally, with user-based authentication, discussed later,

companies can keep a closer watch on the information their employees are accessing and thus limit internal fraud. VPNs use the Internet for communication. The Internet does not provide the highest performance solution, but they allow users to use the Internet as their own private networks. This gives users access to the wealth of information available, while allowing reliable, secure communication channels between parties at low cost. Companies have several strong motivations for building VPNs; they provide § a uniform corporate computing environment that is transparent to users, secure communications, & the cost efficiencies of using a common public infrastructure versus building and operating a private WAN. While many networking technologies have not lived up to their initial hype, this is not the case for VPNs, which are being widely deployed and appear to be earning the nickname —very profitable networks. A VPN not only drastically decreases cost but also increases flexibility because corporations can establish or release global Internet connections on demand. They can also initially pay for low bandwidth and increase bandwidth as demand grows. Internet connectivity is also a VPN's major disadvantage: Guaranteeing quality of service (QoS) over the Internet is difficult because aggregate traffic flows can be unpredictable. Service-level agreements (SLAs) between Internet service providers (ISPs) and corporations are an evolving contractual solution designed to guarantee QoS based on throughput, availability, and/or response time thresholds. [3]

VII. CONCLUSION

VPN allows users or companies to connect to remote servers, between departments, or to other factories over a public network, as providing secure communications. In these cases, the secure connection occurs to the user as a private network communication although the fact that this communication appears over a public network. VPN technology is designed to address issues surrounding the current business trend toward increased telecommuting and widely distributed global operations, where workers must be able to connect to central resources and communicate with each other. This thesis contains some basic information about VPN, then it is mentioned about VPN technologies, such as firewalls, encryption and

authentication. After that there is focused on security and risks in VPN deeply. IKE and ISAKMP are shown as the best ways to protect the data. Beside these there are discoursed about three types of VPN designs which are small, medium, and large VPN designs, also their design gridlines, identity, security, scalability, routing, performance, and alternatives are shown respectively. Moreover, VPN protocols are approached as the main topic, since they cover all of other sections in this dissertation. These VPN protocols are explained in chapter 2 in detail: L2TP, PPTP, L2F, Layer3, IPSec, MPLS, and IP-in-IP. Layer 2 solutions are in some ways more flexible particularly in terms of the higher layer protocols used in the VPN. Layer 3 VPNs can have advantages in terms of management. PPTP is an technique that for remote connections. L2F is a developing protocol of PPTP. L2F can make more than one connection, a limitation of PPTP. MPLS is useful mainly within an autonomous system, however it can be used across autonomous system if their directors agree and coordinate labels. From these protocols, IPSec is indicated as the best one, since its advantages. The main and the most important benefit of IPSec is that it is a universal protocol. IPSec is an international standard because of the flexibility and power of IP. It can provide security and communicate with a variety of different networks from around the world. Through IP, IPSec can be applied in networks of all sizes including LAN‟s to global networks. Because of these advantages IPSec is recommended as the future of VPN protocols in our opinion.

REFERENCES

[1] Charlie Scott, Paul Wolfe and Mike Erwin," Virtual Private Networks", Second Edition January 1999.

[2] Martin W. Murhammer, Orcun Atakan, Zikrun Badri, Beomjun Cho Hyun Jeong Lee, Alexander Schmid, "A Comprehensive Guide to Virtual Private Networks, Volume III: CrossPlatform Key and Policy Management", November1999.

[3] Shashank Khanvilkar and Ashfaq Khokhar, ―Virtual Private Networks: An Overview with Performance Evaluation‖, University of Illinois at Chicago, IEEE Communications Magazine, October 2004.

[4]Virtual Private Networks by Shamod Lacoul http://www.slidefinder.net/V/Virtual_Private_Networks_Shamod_Lacoul/32104518

[5] Yurcik and W. Doss, ―A planning framework for implementing VPNs‖, Volume: 3 Issue: 3, May-June 2001.

[6] Reuven Cohen and Gideon Kaempfer, ―On the Cost of Virtual Private Networks‖, IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 8, NO. 6, DECEMBER 200