Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks

Si Thu Aung
University of Computer Studies, Yangon
cthuaung@gmail.com

Thandar Thein
University of Computer Studies (Maubin)
thandartheinn@gmail.com

Abstract

Nowadays, many companies have branch offices and connect those offices to the main office over the Internet using a site-to-site Virtual Private Network connection. Most of these connections have always operated at Layer 3 of the OSI network model. In recent years, there has been a growing requirement to extend links at Layer 2, which allows broadcast traffic to be forwarded between sites. Depending on inter-site connection medium, different technologies are utilized. This paper compares and analyses site-to-site Layer 2 VPN technologies, which include layer 2 tunneling protocol (L2TP), and point to point tunneling protocol (PPTP), OpenVPN, Ethernet over IP (EoIP), and MPLS/VPLS to choose the right VPN for the organization. This is done by means of performance measurement and packet analysis. In order to provide fair comparable results, all technologies are tested in the same manner.

Keyword: *PPTP, L2TP, OpenVPN, EoIP, VPLS, Virtual Private Network*

I. INTRODUCTION

While VPNs were commonly planned for individual clients, demand is likewise expanding in business. Organizations presently use VPNs to verify their office systems, business PCs, and Internet connection while others use VPNs to remotely access network resources that are not near them geologically. In the course of the most recent couple of years, VPNs have turned strongly to be one of the most well-known and irreplaceable tools for every privacy-conscious consumer. Globally, the Internet handles around 71,131 GB of traffic for each second, including 2,790,265 emails and 73,849 Google searches for every second [1]. All the company's communications and employees searching for business-related information help to make up those numbers. Furthermore, a breach or leak of the business's data transmitted over the Internet could cost people millions. This raises alarms because, according to a Ponemon Institute survey [2], 67% of SMBs admitted to being attacked in 2018. Large businesses with massive investment may be in a better position to deploy a range of IT security solutions; small businesses need to be more vigilant. The most effective way to prevent the data from reaching the wrong hands is through the use of a VPN service that makes the Internet usage fully private and secure. Businesses may also find different reasons for using a VPN. To fill this gap, there are many kinds of VPN technologies such as IPSec, GRE and SSL. Most of them are Layer 3 VPNs, and it fulfills most of the business requirements. With Layer 3 VPNs, exchange emails and accessing internal servers are easy to use and secure. However, it is not possible to use some software for LAN between two sites, although they are connected by Layer 3 VPN, for example, printer sharing, some database protocols, CRMs, and other applications that are developed for LAN specified purpose. If people want to use LAN applications, a single Ethernet segment needs to be constructed.

Imagine the situation of three remote sites; Yangon, Mandalay and MauBin, and every site have an Ethernet switch. It is a big challenge to connect Ethernet network cables between them. To lay the cable between different offices in different cities is expensive as well as time-consuming. The Internet cannot become an alternative to Ethernet because even if both sites are connected to the Internet, two sites do not construct the single Ethernet segment at all. Layer 2 "Site-to-Site VPN" tunnels the Internet and establish a VPN Session between remote sites with full capabilities to transmit any Ethernet frames. Layer 2 VPN has unlimited protocol transparency, which is identical to physical Ethernet segments. Many protocols such as IPv4 (TCP, UDP, ICMP, ESP, GRE), IPv6, PPPoE, RIP, STP, and others can be used on Ethernet. Any legacy and latest protocols can be used within the Layer 2 VPN sessions. Although provider provisioned Layer 2 VPN solutions such as MPLS/VPLS can be purchased from ISPs, most of these services are monthly payment basis, and the price is not cost-effective.

Not only are these restrictions, but also different IP subnets on each site need to be built. A site's IP subnet cannot overlap with other sites. Moreover, a number of subnets have to be managed in order to prevent any other subnets from colliding. Adopting the Layer 3 VPN for creating site-to-site VPN requires special pain to satisfy the demands of legacy VPNs. However, when we use Layer 2 VPN to link up the site-to-site VPN, it is very straightforward and reduces the effort to coop against several troublesome errors which might occur when Layer 3 VPNs are used. Designing and architecting networks with layer 2 VPNs can be as simple as designing traditional Ethernet network topology with hub-and-spoke mode. Connecting VPN Sessions between sites is possible instead of using physical Ethernet network cables.

All kinds of server and inter-client-PC-communication applications will work well, with no difference between inside the same site and beyond the distance. It is the main reason that the decision to carry out a performance comparison of Layer 2 VPNs is made.

In this paper, the impact of Layer 2 VPNs and performance analysis of five different VPNs, namely, PPTP, L2TP, OpenVPN with BCP, EoIP and MPLS/VPLS are discussed and presented. However, this paper does not provide explicit suggestion on which technology is to be preferred. The rest of this paper is organized as follows: Section II presents related work. Section III explains the characteristic of VPN, and Section IV provides the testbed setup. The experiment results are discussed in section V and draw conclusions in section VI.

II. Related Work

Singh and Gupta [3] proposed Multi-phase encryption and payload encryption; it was applied to the data inside the IP packet of the encapsulated tunnel packet. They discussed the traditional security measures of VPN and a whole new approach for VPN security by using a multi-phase encryption technique. I. Kotuliak, P. Rybár, and P. Trúchly [4] analyzed OpenVPN and IPSec based VPN; they compared those technologies based on parameters such as throughput, the response time of each protocol. They chose OpenVPN due to its simplicity and fast and straightforward implementation.

Chawla et al. [5] explained the architecture and protocols of IPSec and SSL VPN technologies, including their advantages and disadvantages for real kinds of applications. Qin et al. [6] studied IPSec and SSL VPN in detail, and the scope of application, security, scalability, and other aspects are analyzed and compared, advantages and inadequacy are summarized. Zhang Zhipeng et al. [7] presented three types of common VPNs and explained a comparative study of their features, performance, security, and cost-efficient.

None of the related works compared to the performance of Layer 2 VPNs. In this paper, we concentrate on the performance of Layer 2 VPNs.

III. Characteristics and Models of VPNs

A plethora of methods is used to model and characterize VPNs. The purpose of this section is to introduce and explain each of these models and characterizations.

A. Service Provider and Customer Provisioned VPNs

VPNs that are configured and managed by a service provider are service provider provisioned VPNs. VPNs that are configured and managed by the customer itself are called customer provisioned VPNs. Examples of service provider provisioned, and customer provisioned VPNs are shown in Table 1.

TABLE 1. Service Provider and Customer Provisioned VPNs

Provider Provisioned	Customer Provisioned
VPWS, VPLS, IPLS	PPTP, L2TP, OpenVPN
BGP/MPLS, IPSec, GRE, IP-in-IP	IPSec, GRE, EoIP

B. Site-To-Site and Remote Access VPNs

Whether provider or customer provisioned, VPNs fall into one of two broad categories: site to site or remote access. Site-to-site VPNs allow connectivity between an organization’s geographically dispersed sites (such as a head office and branch offices). Fig 1 illustrates a typical site-to-site VPN.

Remote access VPNs allow mobile or home-based users to access an organization’s resources remotely. Fig. 2 illustrates typical remote access VPNs.

C. Protocol Background

This section presents protocols used in Layer 2 VPN technologies.

1)PPTP: The Point to Point Tunneling Protocol (PPTP) is one of the oldest protocol. PPTP uses the TCP port 1723 for remote access over the Internet. The data packets transmitted through the tunnel are

encapsulated. It is suitable for applications where speed is important, such as streaming and gaming.

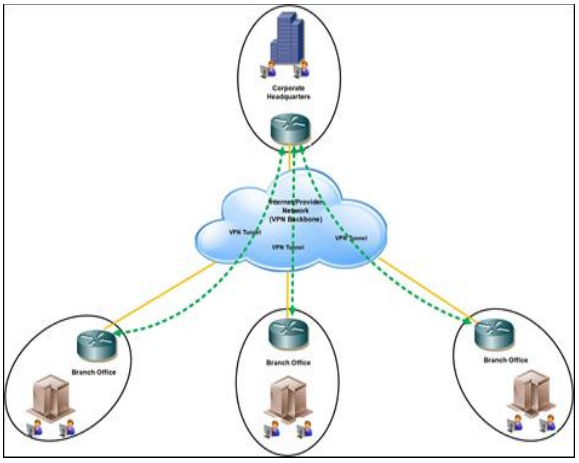

Figure 1. Typical site-to-site VPN

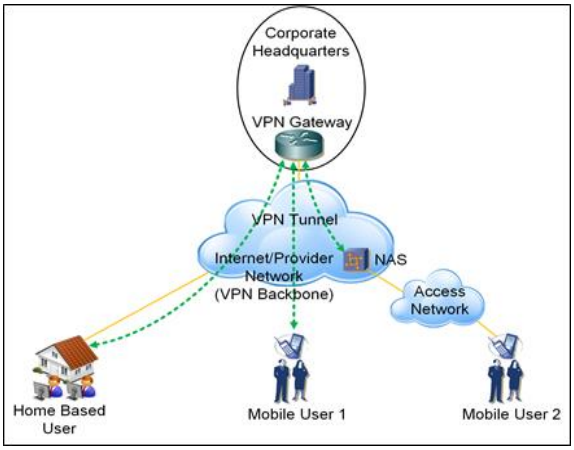

Figure 2. Remote Access VPNs

2)L2TP with IPSec: L2TP stands for Layer 2 Tunneling Protocol and does not provide any encryption on its own. L2TP usually uses IPSec (Internet Protocol Security) authentication protocol. The data transmitted through the L2TP / IPSec protocol is usually authenticated twice. Each data packet transmitted through the tunnel includes L2TP headers. One of the many reasons why L2TP is a common protocol is that there are no known vulnerabilities.

3)OpenVPN: OpenVPN is often referred to as an SSL-based VPN because it uses the SSL/TLS protocol for secure communication. The control channel is encrypted and protected using SSL/TLS while the data channel is encrypted using a custom encryption protocol. OpenVPN's default protocol and port are UDP and port 1194.

4)PPP Bridging Control Protocol: BCP allows bridging the Ethernet frame through the PPP link. Established BCP is an integral part of the PPP tunnel. The Bridging Control Protocol (BCP) is responsible for configuring, activating and disabling the bridge protocol modules at both ends of the point-to-point link. PPTP, L2TP, and OpenVPN protocols can carry only the upper layer of Layer 3 and more. However, with the support of BCP, they can work as Layer 2.

5)EoIP with IPSec: IP protocol 47/GRE allows tunnel creation by encapsulating Ethernet frames in IP packets and forwarding them to another router. Ethernet over IP (EoIP) establishes an Ethernet tunnel on top of an IP connection between two routers. All Ethernet traffic will be bridged, just as if there is a physical interface.

6)MPLS VPLS: Virtual Private LAN Service (VPLS) offers multipoint Ethernet-based connectivity over IP or MPLS networks. It enables geographically dispersed sites to share an Ethernet broadcast domain by linking sites through pseudowires. It is often used for extending LAN services over a network given by a service provider.

IV. Testbed Setup and Performance Parameters

This section describes how to setup testbed to measure performance and to analyze security.

A. Testbed Setup

There are two laptop computers and three desktop computers in this setup. WAN Emulator [8] is running on a desktop computer. RouterOS [9] is running on two computers to create a tunnel between these two desktop computers. Two laptops are running iPerf software to test throughput. In testbed example, the iPerf client send the 100MB of data to the iPerf server, and the output are saved in CSV file. Our testbed setup is as shown in Fig. 3 and their hardware and software specifications are shown in Table 2.

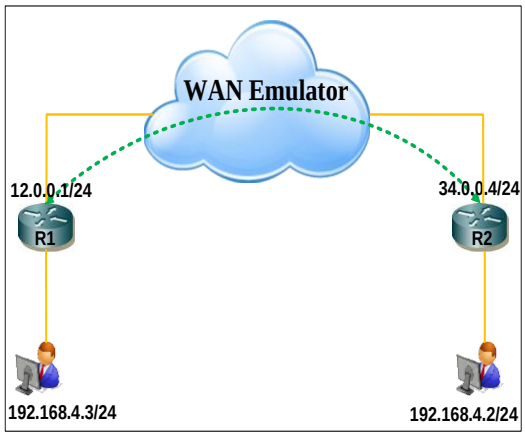

Figure 3. Testbed setup

TABLE 2. Hardware and Software Specification

Type	Description
Laptop x 2	Intel(R) Core(TM) i5-7200 CPU @ 2.50GHz(4CPUs), ~2.7GHz, 8GB memory
Desktop x 3	Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz(4CPUs)
WANem	Wide Area Network Emulator v3.0 Beta 2 released
VirtualBox [10]	Oracle VirtualBox 6.0 hypervisor software
RouterOS	6.46.1 (Stable) release

In this paper, WANEM is used to emulate to define QoS parameters such as packet loss, jitter, and delay. Packet loss has a direct impact on the stability of the VPN. Packet loss occurs when the network is congested.

TABLE 3. QoS Parameters

Parameters	Value
Bandwidth Limit	50 Mbps
Delay	20ms, 40ms, 60ms
Jitter	2ms
Packet Loss	0.1%

Delay is the amount of time a packet travels from its source to destination. Jitter is the changing rate of delay across a network, and is measured in milliseconds and it has a great impact on live streaming application such as video and VoIP. To be similar with real network, QoS values are defined as shown in Table 3.

B. Measurement Tools

Assessing the performance of Layer 2 VPN requires the use of several measurement tools for generating, measuring, and monitoring network traffic. The tools used in this work are Wireshark [11] and iPerf3 [12]. Wireshark is a network protocol analyzer with a rich feature set for capturing and analyzing network traffic. iPerf3 is a network testing tool for active measurements of the maximum achievable bandwidth on IP networks.

V. Experimental Results and Discussion

Experimental results are based on the different parameters for the different VPN technologies. This section shows the performance of seven different methods of Layer 2 VPNs in terms of throughput and protocol analysis.

A. Throughput

Throughput is measured in bits per second. By analyzing the results, throughput varies depending on protocol nature and encryption method. For throughput measurement, iPerf3 is used to exchange traffic between two laptops. For all VPN technologies, the same amount of traffic (100MB) is exchanged and tested three times with three different delays; 20 milliseconds (ms), 40 ms, and 60 ms. The results are documented in Table 4, and Fig. 4 shows the throughput comparisons.

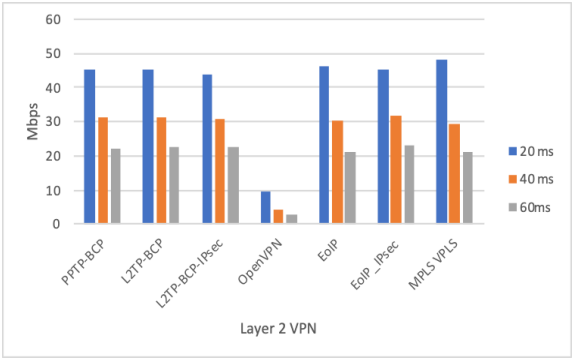

Figure 4. Throughput comparison

TABLE 4. Throughput Comparison with Different Delays

VPN	Delay 20 ms	Delay 40 ms	Delay 60 ms
PPTP-BCP	45.1 Mbps	31.4 Mbps	22.2 Mbps
L2TP-BCP	45.2 Mbps	31.4 Mbps	22.6 Mbps
L2TP-BCP-IPSec	44 Mbps	30.8 Mbps	22.7 Mbps
OpenVPN	9.6 Mbps	4.16 Mbps	2.6 Mbps
EoIP	46 Mbps	30.4 Mbps	21.2 Mbps
EoIP_IPSec	45.1 Mbps	31.8 Mbps	23.1 Mbps
MPLS VPLS	48.1 Mbps	29.4 Mbps	21.3 Mbps

TABLE 5. Throughput and Loss Comparison between Non-VPN Traffic and VPN Traffic at 20ms delay

VPN	Non-VPN Throughput	VPN Throughput	% of Loss
PPTP-BCP	50 Mbps	45.1 Mbps	9.8%
L2TP-BCP	50 Mbps	45.2 Mbps	9.6%
L2TP-BCP-IPSec	50 Mbps	44 Mbps	12.0%
OpenVPN	50 Mbps	9.6 Mbps	80.8%
EoIP	50 Mbps	46 Mbps	8.0%
EoIP_IPSec	50 Mbps	45.1 Mbps	9.8%
MPLS VPLS	50 Mbps	48.1 Mbps	3.8%

All VPN tunnels can degrade performance because of the overhead and encryption methods they use. The amount of throughput loss is due to the trade-off between network performance and security. Generally, the more secure tunnel may result in poor throughput, while less secure tunnel may have better throughput. Table 5 shows the loss of throughput when traversing a tunnel.

B. Packet Analysis

Wireshark protocol analyzer captures the traffic and analyze while two computers ping each other inside Layer 2 VPN tunnels.

1)PPTP with BCP: Fig. 5 shows the packet analysis for the PPTP with BCP, and it can be seen clearly that two computers ping each other since there is no encryption with PPTP.

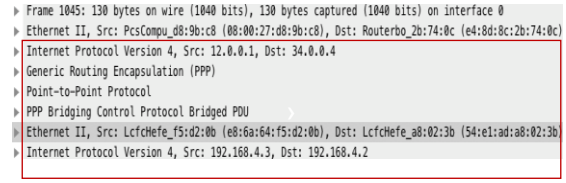

Figure 5. PPTP with BCP

2) L2TP with BCP: When analyzing the packets transmitted through L2TP with BCP tunnel, it is observed that which protocols, along with which source addresses and destination addresses that are being used can be sniffed.

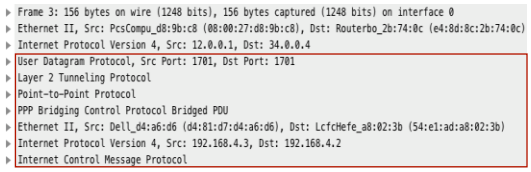

Figure 6. L2TP with BCP

3) L2TP with IPSec with BCP: When analyzing the packets transmitted through L2TP with BCP tunnel with IPSec encryption, only the information of encapsulated payload can be sniffed.

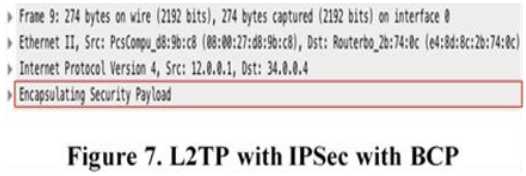

Figure 7. L2TP with IPSec with BCP

4) OpenVPN: Due to its secure encryption methods used, packets that are transmitted through OpenVPN display only the OpenVPN protocol with no other additional information.

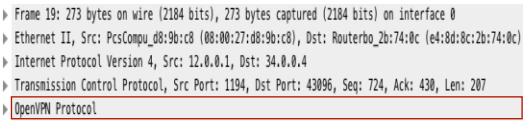

Figure 8. OpenVPN

5) EoIP: Similar to unencrypted L2TP and PPTP tunnels, EoIP also shows protocol and addresses of both source and destination when analyzed by a packet sniffer.

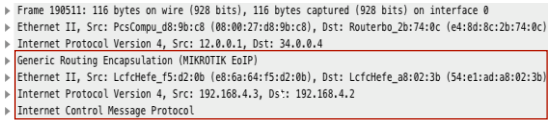

Figure 9. EoIP

6) EoIP with IPSec: EoIP with IPSec no longer displays which protocols along with source and destination addresses accessed in packet analysis if it is properly encrypted by IPSec.

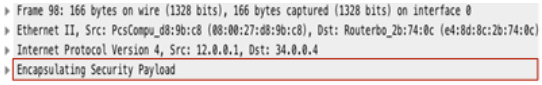

Figure 10. EoIP with IPSec

7) MPLS VPLS: When examine the packets transmitted with MPLS VPLS, it is observed which protocols can be sniffed along with the source addresses and destination addresses used.

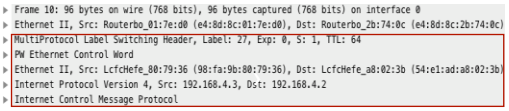

Figure 11. MPLS VPLS

TABLE 6. Comparison Matrix of Authentication and Encryption

VPN Type	Encryption	Authentication	Can be bridge
PPTP	MPPE128	Username Password	With BCP
L2TP	IPSec	Username Password	With BCP
OpenVPN	TLS (AES/BF)	TLS	With BCP
EoIP	IPSec	No	Yes
MPLS/ VPLS	No	No	Pseudowires & Control Word

C. VPN Selection

This section discusses the use of each VPN based on the various throughput performance test and packet analysis conducted in previous sections. Packet analysis describes that OpenVPN, L2TP IPSec with

BCP, and EoIP with IPSec are good for security. The throughput result shows that MPLS VPLS is 48.1 Mbps at 20 ms. EoIP with IPSec is 31.8 Mbps at 40 ms, and 23.1 Mbps at 60 ms. Although the result of EoIP is good at 40 ms and 60 ms, it is not widely used in the industry because it is not mature yet and still vendor dependent. As mentioned in section III, MPLS/VPLS is a provider provisioned VPN, and customer cannot manage themselves. L2TP IPSec with BCP should be considered in term of performance and security perspective for enterprise networks which need Layer 2 VPN connections. The pros and cons of each VPN on various aspects can be observed in Table 7.

TABLE 7. Pros and Cons of Different VPNs

	Security	QoS	Scalability	Cost
PPTP-BCP	Low	No	Good	Low
L2TP-BCP	Low	No	Good	Low
L2TP-BCP-IPSec	High	No	Good	Average
OpenVPN	Higher	No	Good	Average
EoIP	Low	Yes	Average	High
EoIP_IPSec	High	Yes	Average	High
MPLS VPLS	Average	Yes	Best	Higher

VI. CONCLUSION

The main purpose of this paper is to analyze and compare site-to-site Layer 2 VPNs. The experimental results are achieved with different throughputs from five different VPN technologies. They are monitored and captured by Wireshark network protocol analyzer so as to see what protocols and overheads are added to the original frame inside layer 2 tunnel. It is easy to see that Layer 2 VPN carries Ethernet frame that can raise the overhead compared to Layer 3 VPN. As a result of this study, it is not easy to recommend one VPN against to the other because each one of them has advantages and disadvantages in term of security and performance. VPN protocol's encryption capabilities are paramount important because it determines the level of privacy and protection, however, this should not be only one reason to choose the VPN for organization. Therefore, organization should consider VPN technology that can balance performance as well as security.

REFERENCES

[1] Internetlivestats. Accessed: Dec 20, 2019. [Online]. Available: https://internetlivestats.com

[2] Ponemon-Report. Accesed: Dec 20, 2019. [Online]. Available: https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

[3] Kuwar Kuldeep Veer Vikram Singh and Himanshu Gupta "A New Approach for the Security of VPN" in Proc. ICTCS 2016, doi:10.1145/2905055.2905219

[4] I. Kotuliak, P. Rybár and P. Trúchly "Performance Comparison of IPSec and TLS Based VPN Technologies," ICTEA 2011, Slovakia, Oct 2011, pp. 217-221, doi: 10.1109/ICETA. 2011.6112567

[5] Baljot Kaur Chawla, O.P. Gupta, B. K. Sawhney "A Review on IPsec and SSL VPN," International Journal of Scientific & Engineering Research, Volume 5, Issue 11, November-2014 pp. 21-24

[6] Huaqing MAO, Li ZHU and Hang Qin "A comparative research on SSL VPN and IPSec VPN," in proc. ICTCS 2012

[7] Zhang Zhipeng Et al "VPN: a Boon or Trap? A Comparative Study of MPLS, IPSec, and SSL Virtual Private Networks," in Proc. ICCMC 2018, pp. 510-515

[8] WANEM, wide area network emulator. Accessed: Dec 20, 2019 [Online]. Available: http://wanem.sourceforge.net/

[9] RouterOS, operating system for routerboard. Accessed: Dec 20, 2019 [Online]. Available: https://mikrotik.com/software

[10] VirtualBox, open-source hosted hypervisor. Accessed: Dec 20, 2019, [Online]. Available: https://www.virtualbox.org/

[11] Wireshark, packet analyzer. Accessed: Dec 20, 2019 [Online]. Available: https://www.wireshark.org/download.html

[12] iPerf, network measurement tool. Accessed: Dec 20, 2019 [Online]. Available: https://iperf.fr/