Virtual private network impacts on the computer network performance with different traffic generators

Zaman Nagy¹, Asst. Prof. Dr. Mousa K. Wali²
¹²Department of Computer Engineering, College of Technical Electrical Engineering, Middle Technical University, Baghdad, Iraq.
Email: zamannajii362@gmail.com, drmusawali4@gmail.com

Abstract: Virtual private network (VPN) is providing a solution of security to the network nodes. This can be performed by applying tunnels on the link connecting the hosts. However, VPN connection may impact the performance of network according to the traffic density. In this paper, three types of network seniors were tested in presence of VPN connection. A 200 Mbps VPN connection was made between a pair of nodes and performance of this connection is examined by monitoring the time delay and throughput. Network traffic seniors were changes between CRB, HTTP and FTP protocols. Results shown that throughput is not affected when using HTTP-UDP topology. While, throughput is increased when HTTP-TCP topology is used. The time delay is generally increasing in case of HTTP-UDP and HTTP-TCP as compared with other traffic generators.

Keywords: HTTP, DDP, FTP, VNAT, VPN, Security.

1. Introduction
VPN are a topology developed to enforce security for the network connections. This is mainly aimed to separate the unauthorized hosts to get access into the network. Networks are firstly made to enable set (group) of computers to share some peripheries such as printers and fax machines [1]. The networks are further extended and improved by the time. Servers are made with supper computers and hence other host computers are connected to the servers. Those types of networks are used to share the data and information apart from the office machinery amongst the users [2].

Henceforth, internet networks are evolved to act as larger data exchange network; this promoted large number of individuals to communicate through this wide span network. With development of communication systems such as mobile technology and wireless applications, the number of networks applicants is dramatically increased [3]. The involvement of individuals in the networks especially the internet network has enforced new challenges. The network management and traffic control are one of those challenges. Networks are keen on quality of service esurience which involves a low time delay and high throughput [4].

Different type of networks is operating using the internet with support of particular network protocols. Those protocols enable the computers to perform particular tasks such as file transfer, remote control remote access, voice over internet protocol (VoIP), video conferences, live broadcasting and many more applications [5]. With this expansion of the network services, the second major challenge is the security. Security of networks have become more challengeable especially when the hacking activity are realized. The network involved more personalized data which required a strong privacy network [6].
Virtual private network shown in fig. 1 is proposed a state of the art for network security. This kind of security is impended by using the tunnels in form of connection. Those tunnels are established between those connections which are said to be private and no other third party is permitted to get access [7].

Using the virtual private network has a good impact on the privacy enforcement of the network connections. The problem is again raised when different types of network activities are performed over this private connection. The real-life experiments show that network can draw different performances over the virtual private connection [8,9].

Virtual private network is set the requirement of the enterprise security and privacy agreement which is known four key privacy agreement namely: compatibility, availability, security and manageability [10,11]. The first insight of virtual private network has come from the intranet. This is inspired by the way that intranet performs. It is made by connecting some computers inside an organization which only can share some service and no other computers can access from other network [12,13].

In this paper we demonstrated the response of the virtual private network for various types of network activities and operations. The performance of the network is examined using the time delay and throughput metrics.

2. Virtual Private Network

The ordinary network as known as public network of the internet are meant for exchanging the data with various privacy levels among large scale of individuals and organizations. As an attempt to secure those communications, tunneling technology is established to secure the public network connections and virtual private networks are one most usable technique. With help of efficient protocols of virtual private network, VPN is success to provide the security for public network as well as the small-scale network such as home network. From the other hand, networks a like industrial or corporation networks are also being severed by virtual private network.

From the organizations point of views, two protocols are usually used for security connection over the virtual private network namely: SSL and IPSec. Those protocols as well as many other protocols are being used depending on their ability of cost cutting (adaptation) and also some advantages and disadvantages of their technical perspectives.

Figure 1. Overview of the underlaying structure of VPN network.

Internet protocol security is one of the preferred virtual private network protocols in the organizational level due to the cost cut and the productivity which improves the point to point communication through the internet.

3. Empirical model

In this paper, we are interested to examine the virtual private network performance as compared to another network running without the virtual private network. Since the virtual private network is
established so that all the data exchanged between pair of nodes to be directed into private tunnel in order to enforce the security and prevent the malicious activities [10,11,14,15]. However, the empirical model is made in two scenarios more likely first scenario is network consisting of two nodes linked by wire connection without introducing any virtual private network in between. The second scenario involves four nodes which represents two hosts nodes and two intermediate nodes represents the virtual private network routers. The first scenario is depicted in figure 2 while the second scenario is depicted in figure 3.

Figure 2. A demonstration of two nodes connected without a virtual private network.

Figure 3. A demonstration of four nodes connected in a virtual private network.

The network is examined with different traffic generator applications. However, three traffic applications are incorporated with the nodes namely: FTP, HTTP and CBR. Network performance is examined in case of each protocol and results are recorded.

Network simulator NS2 running in virtual machine is used to perform this experiment. The results are taken in each scenario using the trace file which made to provide a complete information about the networking operations during each time slot of the simulation time.

4. Results and Discussion
The seniors are made as first baseline (benchmark) technology which states permitting the transmission without using the virtual private network, while the other scenario is doing same but with presence of virtual private network. The performance is tested using the throughput and time delay measurements. Figure 4 demonstrates the throughput measure for both cases with and without virtual private network in case of CBR traffic condition. This Figure states that for different packet sizes e.g. 512, 1024 and 2048 the throughput for VPN and non-VPN shows no difference. In other word, no visible impact of VPN on the network throughput. However, the throughput keeps raising with more and more data rate as depicted in the Figure 4. Similarly, the throughput is measured for FTP and HTTP traffic and the results are demonstrated in the Figures 5 and 6 respectively indicating the throughput was found decreasing in case of FTP and HTTP traffic For different packet sizes while the throughput was found constant in case of CBR whether the network is running a virtual private connection or not.

Figure 4. VP vs none VPN throughput condition in CBR traffic.
In order to evaluate the network conditions further, time delay is tested for each traffic generator CBR, FTP and HTTP in figures 7, 8, and 9 respectively indicating VPN has only explicit impact on the network performance as it cause more time delay of the packets transferring between pair of nodes. Figure 9 shows the HTTP traffic is realized to be most robust traffic as not fluctuation in the performance with changing the packet size.
5. Conclusion
In this paper, we examined the network performance in presence of virtual private connection. Two network scenarios are implemented using the network simulator version 2. The first scenario is consisting of two nodes without involving the so-called virtual private network and the second scenario is consisting of two nodes (same as previous) with adding two more nodes that act as routers for performing the virtual private connection operations. Hence, network is established, every scenario is examined by varying the traffic generator application. Three different traffic generators are used in each scenario namely CBR, FTP and HTTP. During each paradigm first scenario and second scenario performances are examined using the throughput and time delay calculations.
For different packet sizes the throughput was found constant in case of CBR whether the network is running a virtual private connection or not. While The throughput is observed decreasing in case of FTP and HTTP traffic. On the other hand, time delay is inspected for each scenario and the results found that time delay is increasing at any time if the traffic generator is changed.

Therefore, virtual private network has only explicit impact on the network performance as it causes more time delay of the packets transferring between pair of nodes. This can be explained as more hops will take place between the nodes so the delay will be increased. While throughput is only affected in case of FTP and HTTP traffic. The HTTP traffic is realized to be most robust traffic as not fluctuation in the performance with changing the packet size.

References
[1]. Lim L K, Gao J, Ng T S E, Chandra P, Steenkiste P and Zhang H 2017 Customizable Virtual Private Network Service with QoS, Computer Networks, pp.137-151.
[2]. Malik A, Verma H K and Pal R. 2012 Impact of Firewall and VPN for securing WLANI
International Journal of Advanced Research in Computer Science and Software Engineering
2 (5), pp. 407-410.
[3]. Parmar M S and Meniya A. D 2018 Imperatives and Issues of IPSEC Based VPN International
Journal of Science and Modern Engineering (IJISME) I (2), pp. 38-41.
[4]. Venkateswaran R 2017 Various Services and Implementation Scenarios Virtual Private
Networks, Institute of Electrical and Electronics Engineers (IEEE) Potentials.
[5]. Cryptography and network security, William Stallings 2013 Voice Security in Virtual Private
Network Deep Shikha Computer Science and Engineering AT& T Research.
[6]. L.S. Buriol, C.C. Ribeiro M.G.C. Resende, and M. Thorup 2013 A hybrid genetic algorithm for
the weight setting problem in ospf/is-is routing Technical Report TD-5NTN5G (AT&T) Labs
Research.
[7]. U-T, Geneva, Switzerland 2018 Wideband embedded extension for G.711 pulse code
modulation.
[8]. Pylarinos, S.Louvros, K.IoannouA.Garmpis and S.Kotsopoulos 2015 Traffic analysis in
GSM/GPRS networks using voice pre-emption priority World Scientific and Engineering
Academy and Society, pp.120-123.
[9]. M. Ericsson, M. G. C. Resende, and P. M. Pardalos 2012 A genetic algorithm for the weight
setting problem in ospf routing, J. of Comb. Opt., 6, pp. 299–333.
[10]. Ayan B 2015 Generalized Multi-protocol label switching: An overview of signaling
enhancements and recovery techniques IEEE Communications Magazine, 39, pp.144-151.
[11]. Rosen E, Rekhter Y 2016 RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs)(S) IETF.
[12]. Thomas Berger University of Salzburg 2006 Analysis of Current VPN Technologiests
Proceedings of the First International Conference on Availability Reliability and Security
(ARES’06) IEEE.
[13]. Ming-Song Sun, Wen-Hao Wu 2012 Engineering Analysis and Research of MPLS VPN
Network Information Center, Harbin University of Science and Technology IEEE.
[14]. Luca Cittadini Giuseppe Di Battista Maurizio Patrignani, L. Cittadini, G. Di Battista, M.
Patrignani 2013 MPLS Virtual Private Networks Advances in Networking.
[15]. Muhammad Ikram, Narseo Vallina Rodriguez, Suranga Seneviratne1, Mohamed Ali Kaafar1
and Vern Paxson 2016 An Analysis of the Privacy and Security Risks of Android VPN
Permission-enabled Apps, Berkeley, ACM. ISBN.