Research Exhibition in Mathematics and Computer Sciences (REMACS 6.0)/
ISBN: 978-629-97440-5-4

PERFORMANCE COMPARISON OF VPN TUNNELING ON GRE, IPSEC AND GRE OVER IPSEC USING GNS3

Muhammad Muazzim Mohd Safri, Rafiza Ruslan and Hafizah Hajimia
College of Computing, Informatics and Mathematics,
Universiti Teknologi MARA, Perlis Branch
2020461934@student.uitm.edu.my, rafiza.ruslan@uitm.edu.my and hafizah.hajimia@uitm.edu.my

ABSTRACT – Virtual Private Network (VPN) have become essential for secure communication over public networks. There are few protocols that can be implement in VPN, that establish a secured data communication. However, the continuous evolution of cybercriminal activities poses a significant threat to the security of sensitive data, necessitating the implementation of robust security mechanisms. Moreover, GRE is a tunneling protocol that only encapsulates packets within IP packets between network devices and does not have built-in security mechanisms. On the other hands, IPSec offers various security management capabilities and supports authentication and cryptographic key negotiation make the algorithm more complex. Besides, the performance of GRE and IPSec may degrade with an increase in the number of users and also when to scalable the network, it can leads to fragmentation issues that susceptible to certain network performance. This problem leads to the issues of network performance for both VPN protocol, thus limiting the potential used of GRE and IPSec protocol when implementing in network environment. This research simulated the performance comparison of VPN tunnelling on GRE, IPSec, and GRE over IPSec using GNS3. Simulation results of the GRE, IPSec, and GRE over IPSec VPN protocol indicates that these VPN protocol has remarkable performance in terms of its average throughput, average latency, and also average jitter in various VPN scenarios. For the future work, simulation of GRE-Based VPN tunnelling over IPSec with more additional VPN scenarios and network performance metrics can be carried out in order to gain deeper knowledges and understanding of the GRE, IPSec, and GRE over IPSec VPN protocol.

Keywords: VPN tunnelling protocol, GRE, IPSec, GRE over IPSec, GNS3

1. INTRODUCTION

The aim of this research is to simulate GRE, IPSec, and GRE over IPSec by using GNS3 network simulator tool and then compare the results of each GRE, IPSec, and GRE over IPSec performance under various different scenarios that reflects the real-time implementation of the VPN protocol. The scope of this research focused on the performance of GRE, IPSec, and GRE over IPSec protocol in network environment, and the simulation is carried out in GNS3. This research is also using Iperf-3 network monitoring tool in GNS3 that used together for simulation of each VPN tunnelling protocol.

2. METHODOLOGY

The method that was used to carry out this research is a simulation model that represents VPN network environment in between two building with different networks. The simulation model is presented in the form of a VPN network topology that consists of GRE, IPSec, and GRE over IPSec tunnelling. There is one source node, and one destination node in both buildings that are linked together in order to simulate GRE, IPSec, and GRE over IPSec VPN tunnelling protocol in VPN network environments. The whole simulation of GRE, IPSec, and GRE over IPSec is carried out under several different simulation scenarios such as MTU sizes, and encapsulation modes which are tunnel mode and transport mode. The results obtained from the simulation is then analysed in order to find the best solutions to maximize the network performance of GRE, IPsec, and GRE over IPSec tunnelling environments.

3. RESULTS AND DISCUSSION

Based on the results and analysis, there are three simulations which are GRE, IPSec, and GRE over IPSec VPN tunnelling. Firstly, for the GRE VPN performance, as the MTU size increases, performance of GRE VPN in terms of average network throughput increases and in terms of average network latency and average network jitter decreases when simulated with 1500 bytes. Secondly, for the IPSec VPN performance there will be two simulation which is in tunnel mode and transport mode. For the tunnel mode, as the MTU size increases, performance of IPSec tunnel mode in terms of average network throughput increased gradually together with average network latency and network jitter when set the maximum MTU size of 1500 bytes. For the transport mode, as the MTU size increases, performance of IPSec transport mode in terms of average network throughput decreases except when simulated with the minimum MTU size of 1000 bytes. However, the average network latency and average network jitter increases as the MTU size increases. Lastly, the GRE over IPSec performance, as the MTU size increases, performance of GRE over IPSec VPN in terms of average network throughput increases when simulated with 1500 bytes. Besides, the average network latency

and average network jitter decreases as the MTU size increased gradually. Overall, results of the analysis indicates that each of GRE, IPSec, and GRE over IPSec VPN tunnelling has optimal network performance according to the right MTU sizes and encapsulation mode.

4. NOVELTY OF RESEARCH / PRODUCT

Throughout the years, there have been several research that conducted performance analysis on GRE, IPSec, and GRE over IPSec using either GNS3, and packet tracer measuring the throughput, response time, jitter by measuring with Solar Winds such as (Ogudo., 2019; Uddin et al., 2021). There is also a previous research on the performance of GRE and IPSec that focusing on QoS VoIP and how both protocol effects the performance of network throughput, packet loss, and jitter using OPNET Moduler as a network simulation tool (Ubedilah et al., 2022). Other than that, there is also research that analysed the performance of VPN tunnelling protocol based on Application Service Requirements in terms of throughput, latency, and jitter that provided the good network performance for the application service requirements (Akter et al., 2022). Last but not least, research by Forbacha & Agwu (2023) implemented a secure Virtual Private Network over an open network (internet) measuring the throughput, bandwidth, and security implementation between multiple private networks connected to public network that is internet by implementing GRE and IPSec VPN protocol.

5. CONCLUSION

In the nutshell, it can be concluded that each of GRE, IPSec, and GRE over IPSec has remarkable performance towards the performance of the network throughput, network latency, and network jitter when the different network parameter being simulated in different scenarios.

REFERENCES

Ogudo, K. (2019). *EasyChair Preprint Tunnel comparison between Generic Routing Encapsulation (GRE) and IP Security (IPSec) Tunnel comparison between Generic Routing Encapsulation (GRE) and IP Security (IPSec)*.

Ubedilah, Budiyanto, S., & Silalahi, L. M. (2022). Analysis QoS VoIP using GRE + IPSec Tunnel and IPIP Based on Session Initiation Protocol. 2022 5th International Conference on Computer and Informatics Engineering, IC2IE 2022, 47–54. https://doi.org/10.1109/IC2IE56416.2022.9970120

Forbacha, S. C., & Agwu, M. J. A. (2023). Design and Implementation of a Secure Virtual Private Network Over an Open Network (Internet). American Journal of Technology, 2(1), 1–36. https://doi.org/10.58425/ajt.v2i1.134