Performance Evaluation of IPSec VPN Modes

Jorge Medina, Monica Tamanampudi, Nasirali Kovvuru, Wlodek Kulesza
School of Engineering
Blekinge Institute of Technology
Karlskrona, Sweden
jamedina@gmail.com, nasirali.nnn@gmail.com, monicachandhu753@gmail.com, dek.kulesza@bth.se

***Abstract*— Site-to-site VPNs have become a cheaper and a popular choice for companies to communicate their remote headquarters using the Internet network as the vehicle to convey their data. Since site-to-site VPNs rely on a public network, security mechanisms should be employed to avoid data breaches as possible; fortunately, there is a variety of VPN and encryption protocol flavors that when combined together provide the required security mechanisms. Additionally, the concept of data convergence should be examined, as data needs to be prioritized based on the service offered. This paper is an evaluation of IPSec modes of operations to determine, via measurement of network indicators, the one with better performance while keeping a balance between quality and security.**

Keywords*— *GRE encapsulation, IPSec Modes, QoS VPN, site-to-site VPN

I. INTRODUCTION

Originally to establish a private network connection between two remote sites, we were dependent on service network providers. To solve this problem VPN technology came into existence, but later due to the wide usage of internet WAN technology, enterprises chose to have their tunnels, logical connections, on the Internet, such that they can communicate with all their branch offices throughout the globe. Here the tunnel provides different encryption algorithms to establish a secure connection between the peers so that enterprises can provide confidentiality, data integrity and authentication to their clients. This logical connection is created by using different tunneling protocols, being IPSec one of the most common and used, offering three modes of operations: IPSec tunnel mode without IP GRE tunnel, IPSec tunnel mode and IPSec transport mode, both with an encrypted IP GRE tunnel.

This Paper is an evaluation of the three modes of operations mentioned above, with four combinations of IPSec phase2 transformation sets: 3DES-MD5, 3DES-SHA, AES-MD5 and AES-SHA to determine which combination gives better performance via network indicators such as throughput via Round-Trip-Time RRT and packet loss via a priority traffic class, Low Latency Queuing LLQ.

Based on the simulation of IPSec VPN using GNS3, it can be concluded that IPSec transport mode over GRE tunnel provides the lowest RTT for almost all the combination sets. Better performances are observed with the sets: AES-MD5, AES-SHA, 3DES-MD5 for IPSec tunnel mode with no GRE, IPSec tunnel mode with GRE and IPSec transport mode with GRE, respectively.

II. SURVEY OF RELATED WORKS

There are different protocols associated with VPNs site-to-site, for instance: GRE and IPSec protocols.

The study of those protocols is critical when designing VPNs because service applications demand different throughput, bandwidth and delay requirements. From [1] it was seen that GRE provides greater throughput than IPSec. However, GRE lacks security mechanisms to protect data.

Then if security is a must, IPSec must be chosen. With it, we have the flexibility to select the hash and encryption algorithms to implement in the VPN. In [2] authors compare the performance in terms of throughput of four pairs of encryption-hash algorithms for IPSec tunnel mode without GRE. The results show that when sending HTTP or FTP traffic the encryption algorithms AES performs better than 3DES algorithm. It is also key due to the convergence of traffic, video, voice and data, to analyze throughput in relation to the encryption algorithm selected as well as the packet size [3].

III. PROBLEM STATEMENT AND MAIN CONTRIBUTION

It is interesting to know how the selection of a transform-set in particular, provides better performance when applied to every mode of operation with and without GRE tunnel. IPSec is enabled with GRE tunnel to support multicast because by itself would only support unicast at layer3.

We hypothesis that the sets with AES encryption would perform better because AES tends to be faster than 3DES.

IV. PROBLEM SOLUTION

A. *Evaluation Method.*

The proposed model for this study is depicted in Fig.1. The model consists of:

- Main Office (192.168.0.0/24): consists of two hosts, 1 and 2, one switch and a router, sw1 and R1 respectively.
- Office Branch (192.168.1.0/24): consists of two hosts,3 and 4, one switch and a router, sw2 and R3 respectively.
- Main and office branch networks connected logically via VPN tunnel, between R1 and R3, and physically through the internet represented by R2.

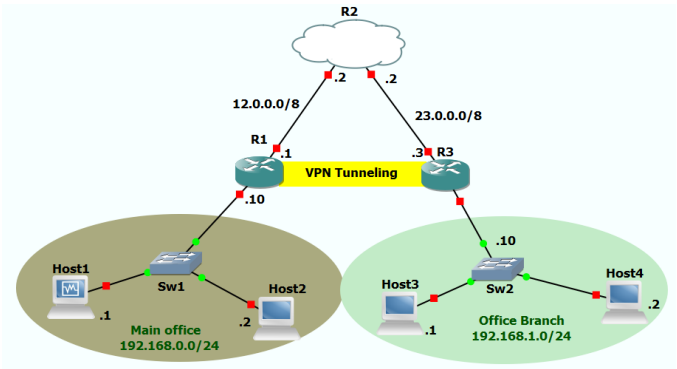

Figure 1. Proposed Model.

B. *Implementation and Results*

This study is executed using GNS3 emulator, which provides the tools necessary to obtain the data as close as possible to real implementations. ICMP traffic will be sent in order to measure the network metrics that will help at the end to compare security and QoS in the modes of operation.

For security analysis four IPSec phase2 transformation sets are going to be analyzed and network metrics, throughput via round-trip time, to be collected.

The four pairs, encryption and hash algorithms, selected:

- ESP-3DES-MD5-HMAC
- ESP-3DES-SHA-HMAC
- ESP-AES-MD5-HMAC
- ESP-AES-SHA-HMAC

Each of these combinations will be implemented in the three modes of operations.

For QoS analysis, the percentage of packet loss will be measured in the different modes by configuring an LLQ priority class on R3 for traffic coming from host1 to the branch office. The marking of differentiated traffic on the main office is set in R1 via policy-map class and access list.

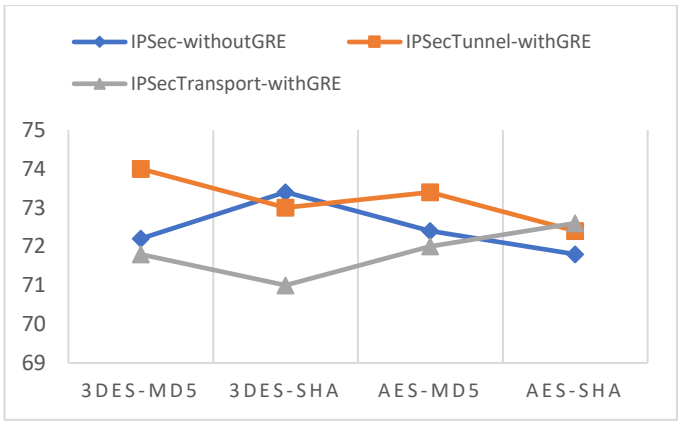

Figure 2. Average Round Trip Time (RTT) [ms]

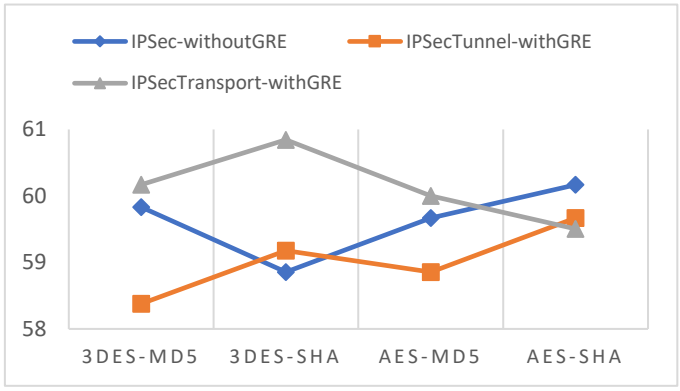

Figure 3. Average Throughput [kbps]

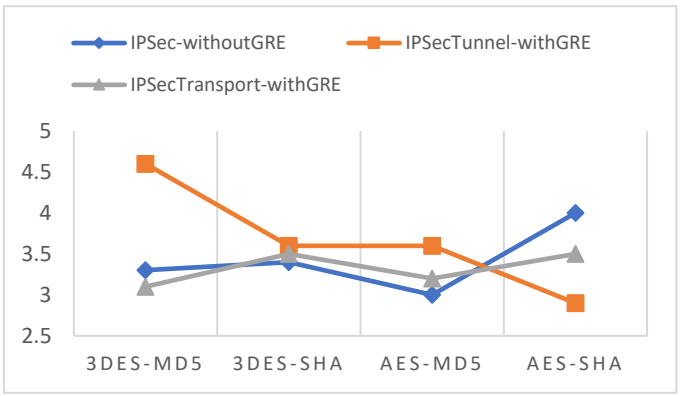

Figure 4. Average Packet Loss percentage.

In general, we can observe in Fig.2 that IPSec transport mode, will offer the lowest RTT among the three modes. This is due to the fact that it has the lowest overhead in terms of encapsulation.

From Fig.3, we can observe that better throughput is obtained for IPSec without GRE tunnel for the transform set AES-SHA. In the case of IPSec tunnel mode with GRE for the transform set AES-SHA and for IPSEC transport mode with GRE for 3DES-SHA.

From Fig.4, less packet loss is seen when implementing the transform sets: AES-MD5 in the case of IPSec tunnel mode without GRE, AES-SHA for IPSEC tunnel with GRE and 3DES-MD5 for IPSec transport mode with GRE.

V. CONCLUSION

Site-to-site VPN has become the solution to establish private communication over remote sites for companies via a virtual tunnel through the internet. When configuring an IPSec VPN site-to-site in terms of security matters, we are presented with various type of encryption and hash algorithms to choose from. In this paper, the encryption algorithms 3DES and AES and hash algorithms SHA and MD5 are selected to be applied in the three modes of IPSec operation.

To keep a good trade between throughput and quality, high throughput while keeping low packet loss percentage, we can observer that, the transform-set AES-MD5 for IPSec tunnel mode without GRE, the transform set AES-SHA for mode IPSec tunnel over GRE and finally the transform set 3DES-MD5 for mode IPSec transport over GRE are preferred.

Finally, we can conclude that IPSec transport mode with an encrypted IP GRE tunnel offers better throughput and less RTT for most of the transform-sets selected. For a future evaluation performance, a measurement of network indicator using VOIP, as very sensitive traffic data, would be worthy to further study.

REFERENCES

[1] S. Jahan, M. S. Rahman, and S. Saha, “Application specific tunneling protocol selection for Virtual Private Networks,” presented at the Proceedings of 2017 International Conference on Networking, Systems and Security, NSysS 2017, 2017, pp. 39–44.

[2] M. H. M. Zaharuddin, R. A. Rahman, and M. Kassim, “Technical comparison analysis of encryption algorithm on site-to-site IPSec VPN,” presented at the ICCAIE 2010 - 2010 International Conference on Computer Applications and Industrial Electronics, 2010, pp. 641–645.

[3] D. Lacković and M. Tomić, “Performance analysis of virtualized VPN endpoints,” presented at the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings, 2017, pp. 466–471.

Biographies

Jorge Medina. was born Tegucigalpa, Francisco Morazán, in 1988. He received the B.Sc. in electrical industrial engineering from La Universidad Nacional Autonoma de Honduras, Tegucigalpa, Honduras, in 2012 and currently studying his M.Sc. degrees in telecommunication systems in The Blekinge Institute of Technology, Karlskrona, Sweden.

From 2008 to 2012, he was an Instructor in the Physics Department in the UNAH, from 2012 to 2015 he worked for the telecommunication company TIGO as a Value-Added Service Support Engineer and from 2015 to 2016 he worked as Quality Core Engineer for the same company mentioned.

Mr. Medina's awards and honors include the participation in the Global Exchange Program, UGRAD, in The North Dakota State University, getting recognition from the Electrical Engineering Department, scholarship for the Intensive English Program in The University of Alabama in Huntsville, medals of recognition for best student from Instituto Tecnico Honduras, award of best student in the Electrical Engineering Department in promotion held in 2012.

.

Kovvuru Nasirali was born in Kalikiri village, Andhra Pradesh in 21-05-1996. He received the B.Tech in Electronics and Communication Engineering from the Jawaharlal Nehru Technological University, Kakinada, in 2016. He is currently perusing MSc degree in Telecommunication Systems at BTH, Karlskrona.

He has completed summer internship at Convergence Labs in Telecom Protocol developing and testing , his research interests include Telecommunications, IOT, Network Security, 5G, cloud computing and Network Management, he has good knowledge in Linux, programmng, TCP/IP, configuration of network and firewalls, Intrusion Detection systems, web development, DNS, DHCP, SNMP.

Kovvuru Nasirali is member of IETE and LEO club Kakinada.

.

Monica Tamanampudi was born in Tanuku city, India, on 07-02-1996 . She received the B.tech. degree in electronics and communication engineering from JNTUK university, Kakinada, India in 2016.She is currently pursuing M.Sc degree in Telecommunication at Blekinge Institute of Technology , Karlskrona ,Sweden.

She worked as a supporting front end developer for her project called 'Internet whiteboard'. Her interests include cloud computing, network management, Wireless Communications, Game development.

Ms. Monica is a member of IETE and LEO club of Kakinada