Performance Comparison of Encryption IPsec VPN Encryption Techniques

Nur Hasyimah Mohd Ridzuan, Assoc. Prof. Ruhani Ab Rahman
Faculty of Electrical Engineering
Universiti Teknologi MARA
40450 Shah Alam, Selangor , MALAYSIA
hasyimahridzuan@gmail.com , ruhani467@salam.uitm.edu.my

Abstract –Internet Protocol Security (IPSEC) is one of the protocol implements in VPN site to site tunnels network. Where Virtual Private network (VPN) is a technology that used to transmit information via insecure regions such as internet from one office on one geographical area to another geographical area. IPSEC protocol network setup encrypt the overall IP traffic packets before being transferred from source to destination in order to secure the tunnels. This paper presents the implementation of site to site VPN tunneling using a network simulator. By varying the combination of encryption algorithm 3DES and AES 256 with two hashing type SHA-1 and MD5, the performance of each algorithm was compared and analyzed via Window 7 environment. The implementation of IPSEC protocol via Cisco equipments was introduced. Results indicate different algorithms (with and without encryption), hashing method and packet length have influence on Round Trip Time (RTT).

Keywords – *Virtual Private Network, Security, tunneling, Encryption Algorithm, Windows 7, Round Trip Time and IP Security.*

I- INTRODUCTION

Nowadays, there is an increasing demand to connect to internal network from instant area and location. User often intent to connect to internal private network over unsecure network such as Internet from hotel, airports, office branch, mobile and other external network. Due to that reason, other than security, performance is the one major consideration when employee or vendors require connect to internal network from other external location.

Virtual Private Network (VPN) technology offers a solution to protect data that being transfer over an Internet. It allows sender to establish virtual private tunnel securely enter the network and securely transmit data, accessing the data and communicate via unsecured Internet network [1][3][4]. VPN use encryption method in order to provide

the data confidentiality [1][2][4][5]. Figure 1 shows an example of VPN network establish between several network branch offices with head quarter office.

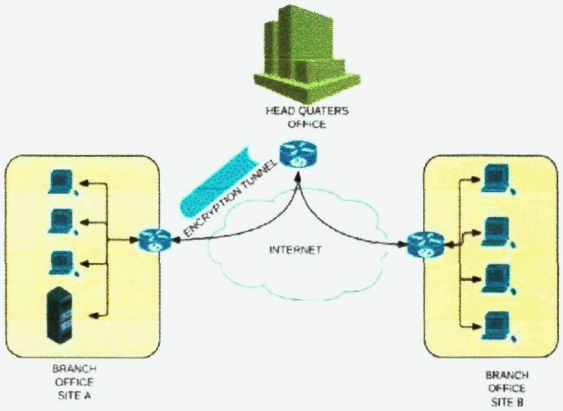

Figure 1: Virtual Private Network Environment

VPN has four types of tunnneling protocol which are point-to-point tunneling protocol(PPTP), IP Security Protocol(IPSec), the Layer 2 Tunneling Protocol (L2TP) and the Protocol for sessions traversal across firewall securely (SOCKS v5) [8][9][10]. The above protocols is run at different protocol layer and with its strengh and weakness of the performance. The benefit of applying the concept of VPN is act a as solution in order to establish long distance data transfer with secure network connections. It also can eliminated the company cost without using the conventional method which is a leased line approach. Hence, several encryption algorithm method exist in current environment such as Blowsish, DES, 3 DES, AES, RC6 and RC2.

Since VPN was contribute to an importance study of current VPN technologies, study related to implementation of VPN based on IPsec protocol was conducted [9]. The anaylsis of performance on Window 2003 environment was describe based on four protocol tunneling. The result conclude that VPN establish a secure connection to user,ensure the data secure transmisson and reduce the user cost. Besides, the smilar research was conducted via Window 2003 envorinment too, but the method approach are differ. Analyze throughput result obtained by varying protocols, algorithm, window size and CPU usage[8]. More study has been performed on previous

paper which focused on Window Vista environment by the test bed setup accumulated with testing method of combination of encryption algorithm, different file size effect on throughput and different protocols applied[3].

This paper presented the observation of site to site VPN tunneling on test bed. By varying the combination of encryption algorithm 3DES and AES 256 with two hashing type SHA-1 and MD5, the performance of each algorithm was compared and analyzed via Window 7 environment. The implementation of IPSEC protocol via Cisco equipments was introduced.

II- EXPERIMENTAL SETUP

The simulation model was developed based on small network sizes of site to site VPN network. The environment consists of six Cisco C3600 equipment named from R1, R2, R3, R4, R5 and R6. Router R1 and R6 was present as a gateway router for each site and configured with IPSec protocols. The scenarios used emulate network environment with real time traffic generated using a VPN protocol known as IPSEC. From Figure 2, it shows that R1 and R6 will establish encryption tunnel to allow the data transfer securely between two sites. Both R1 and R6 were connected to Virtual Machine PC (VMware Player) using the Fast Ethernet cables which Host PC1 and Host PC2 act as workstations. The VMware Player is running using the operating system Window Ultimate 7 and installed with Wireshark system as a monitoring agent. While the routing protocols RIP version 2 was configured on routers R2, R3, R4 and R5. The overall setup can be visualized as in testing environment on Figure 2. The technical hardware specification details of each equipment and software device attached in Table 1.

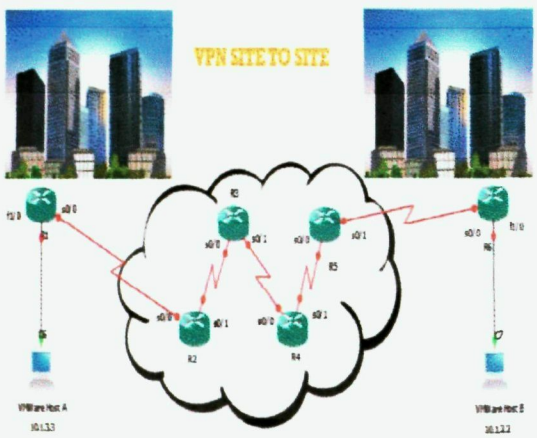

Figure 2: Testing Environment

PC Host Site A	
a.	Processor : Intel® Core ™ i7-3612QM CPU @2.10GHz RAM: 1.00 GB Operating System: Window 7 Ultimate NIC: Intel ® PRO/1000 MT Network Connection Monitoring Agent: Wireshark
PC Host Site B	
b.	Processor :Intel® Core ™ i7-3612QM CPU @2.10GHz RAM: 1.00 GB Operating System: Window 7 Ultimate NIC: Intel ® PRO/1000 MT Network Connection Monitoring Agent: Wireshark
Cisco Routers	
c.	Model: 3640 IOS Image : 3600 Software (C3640- JK903S-M) Version , 12.4 (5a) Fast Enthernet Interface: NM-1FE-TX Ethernet Serial Interface: NM-4T Serial
Channel Capacity	
d.	Fast Inthernet : 100Mbps Serial : 1.58 Mbps

Table 1: Hardware Technical Setup

The testing environment has been setup using 5 different scenarios as listed in Table 2. The main purpose of this experiment is to observe the performance on IPSEC VPN site to site tunneling mechanism with different encryption and authentication algorithms. Although the configuration of encryption is different, the device and equipment used are remain the same. This is to ensure the network platform is maintained and RTT result captured able to compare under different scenario. The scenarios tested in this experiment are:

NO.	ENCRYPTION	HASH
1st Scenario	None	None
2nd Scenario	AES 256 bit	SHA-1
3rd Scenario	AES 256 bit	MD5
4th Scenario	3DES	SHA-1
5th Scenario	3DES	MD5

Table 2: Scenario based on different selection of algorithm

The model was designed with IPSEC cipher specifications which are 3DES and AES256 as the encryption algorithm, SHA-1 and MD5 as the hashing integrity mechanism and authentication of IPSEC was establish with pre-shared key between R1 and R6 as a router gateway to peer. Below is a step by step by step required to establish IPSEC VPN tunnel and encryption algorithm setup:

- Define and configured IP address for all routers under internal and external network. Site 1 was configured with internal network of 10.1.3.0/24, while Site 2 is configured with internal network 10.1.2.0/32. The goal is to allow full communication between both networks without

any obstacle and securely connect both LAN networks.

Figure 3: Configuration internal network for each site

- Rip version 2 routing protocols was setup for internet router (R2, R3, R4 and R5).

```
Router (config)# router rip
Router (config)# version 2
Router (config-router)# network ip-address
Router (config-router)# no auto-summary
```

- Create ISAKMP policy and enable it. The below command define as:
  - AES 256 bits : encryption used
  - SHA-1 : The hashing algorithm
  - Pre-share : used pre shared key as authentication method
  - Group 2: Diffie Hellman to be used
  - 86400 : session key lifetime

```
Router (config)# crypto isakmp policy 10
Router (config-isakmp)# authentication pre-share
Router (config-isakmp)# encryption aes 256**
Router (config-isakmp)# group 2
Router (config-isakmp)# hash sha**
Router (config-isakmp)# lifetime 86400
```

** *will be changed based on scenario chosen.*

- Then, define the pre-shared key for authentication process with peer. The peer`s pre shared key is set to 0 and its peer public IP address is 10.1.1.14. Every time R1 try to establish the VPN tunneling with R6, this pre-shared key will be used. The command as follow:

```
Router(config)# crypto isakmp key 0 cisco address10.1.1.14
```

- Then, create IPSEC with the following steps:
  - Create Access List(ACL) to permit IP and ICMP traffic at R1 and R6 routers. Traffic was defining to pass through the VPN tunnel from one network to another.

```
Router (config)# access-list 101 permit ip 10.1.3.0
0.0.0.255 10.1.2.0 0.0.0.255
```

  - Configure IPSEC Transform set used to protect data.

```
Router (config)# crypto ipsec transform-set CISCOSET
esp-aes esp-sha-hmac
```

  - Set the crypto map named as S1S2 (referring to site 1 to site 2). The ipsec-isakmp will inform the router that this crypto map is IPsec crypto map. There is possible to have multiple peers set within a given crypto map. However, for this experiment, only one peer (10.1.1.14) was set.

```
Router (config)# crypto map S1S2 10 ipsec-isakmp
Router(config-crypto-map)# set peer 10.1.1.14
Router(config-crypto-map)# set transform-set
CISCOSET
Router(config-crypto-map)# match address 101
Router(config-crypto-map)#exit
```

  - Applied the S1S2 crypto map with public interface S0/0 and enable it.

```
Router(config)# int S0/0
Router(config-int)# crypto map S1S2
```

- Once R1 and R6 was successfully configured, ping command from inside node (PC1 or PC2) to trigger the tunnel.
- Finally, every scenario was repeatedly run 10 times for each encryption. Data simulation was capture and analyze follow the flowchart of the experiment presented in Figure 4.

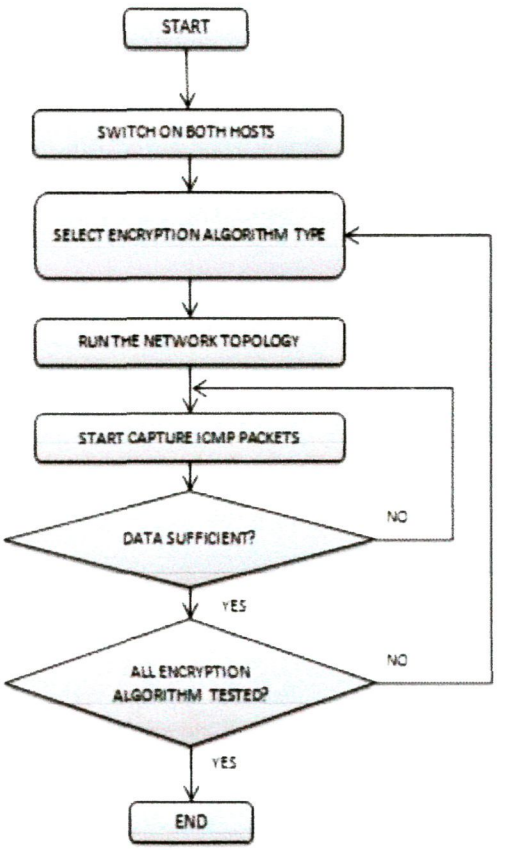

Figure 4: Flowchart of Experiment

III- FINDING ASSESSMENT

The project finding was presented on this section. Each scenario was implemented with different algorithm encryption and packet length was observed. The results of round trip time (RTT) was discussed and analyzed.

The ICMP protocol has been used to test connectivity across an IP network. In this experiment, the ping command was executed from VMware PC1 to VMware PC2. It works by PC1 sending ICMP "echo request" packet to PC2 and listening to ICMP "echo respond" replies from PC2. Ping result estimated the round trip time (RTT) in milliseconds (ms).

The RTT results achieved from this experiment based on comparison of site to site VPN with encryption method applied and without encryption. The analyze result shown in Figure 5. This graph indicate that the IPSec VPN tunneling configured with encryption has produced a slightly greater round trip time(RTT) as compared to none encryption VPN tunneling. By referring to Table 3, the data was generated based on average of repeatedly data taken on RTT results. The table shows that none encryption result mostly captured the average RTT of 192.5ms while the encryption algorithm captured the maximum average reading of RTT is 238.6 ms.

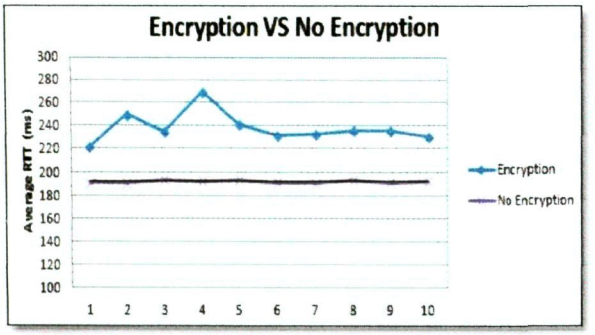

Figure 5: Performance of RTT for encryption and none encryption

Test scenario	Encryption	Hashing	Avg RTT (10x data taken)(ms)
1st Scenario	None	None	192.5
2nd Scenario	AES 256	SHA-1	216.9
3rd Scenario	AES 256	MD5	210.3
4th Scenario	3DES	SHA-1	238.6
5th Scenario	3DES	MD5	224.8

Table 3: Average RTT data based on scenario

Figure 6 shows the overall performance results obtained when all five scenarios was tested. The range of RTT results based on different encryption and authentication applied.

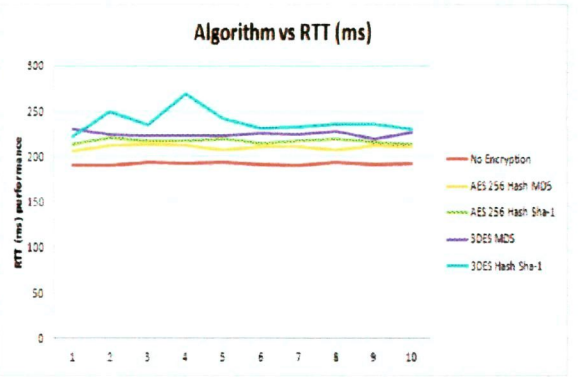

Figure 6: Overall performance encryption algorithm versus RTT

While for Figure 7, 8,9 and 10, each of encryption algorithm was tested with different packet length. The data taken was simulating with different packet length when ping command execute to 10 Bytes, 100 bytes and 1000 Bytes. The simulation result was taken repeatedly and performance graph as follow:

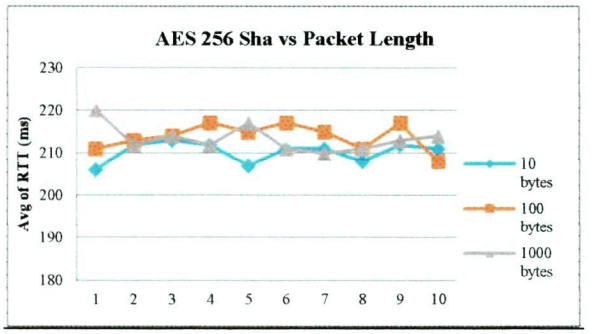

Figure 7: AES 256 hash SHA-1 with different packet length

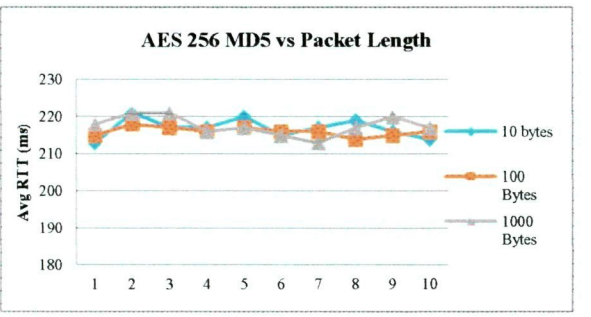

Figure 8: AES 256 hash MD5 with different packet length

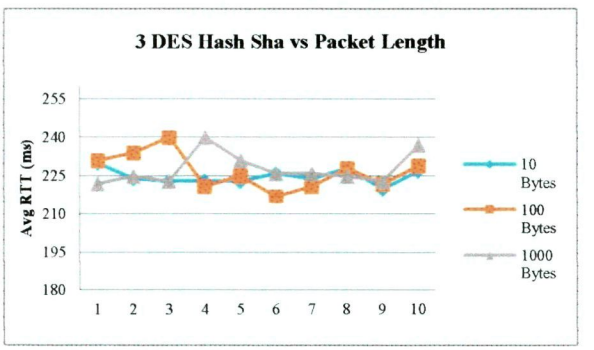

Figure 9: 3DES hash SHA-1 with different packet length

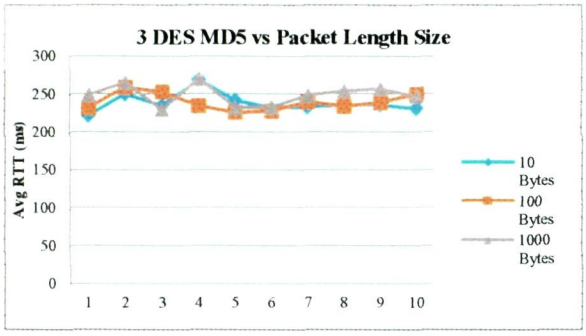

Figure 10: 3DES hash MD5 with different packet length

IV- DISCUSSION AND RESULTS

Tabulated data and graph was analyzed and discussed. Results observed that when performing ping command from PC 1 to PC2, the response time contribute to higher round trip time (RTT) when VPN tunneling implemented with encryption command. The main reason behind the scenario is due to encryption process introduce the overhead while transmit the data. The overhead data was included with AH and ESP headers which cause the process of response time is higher compare to non encrypted network [6]. The percentage of RTT value was increasing almost 10-20 % when encryption applied depending on type of encryption and authentication algorithm.

Based on table 3, the average value was calculated for every scenario. Hash algorithm has been analyzed based on the data captured. Even though both hashing algorithm are from same source, MD4 algorithm [3][5], however from Table 3 it can be seen that SHA-1 perform slower compared to MD5 based on average RTT value presented [3]. This is due to MD5 produce message has a hash size of 128 bits (16 bytes) and SHA-1 produce message has a hash size of 160 bits (20 bytes)[6][3]. Furthermore, the reason why MD5 is faster than SHA-1 is because the SHA-1 has 80 times iteration round while MD5 is only has 64 times of iteration round. This means that it conclude that MD5 digest and execute faster but less secure than SHA-1[5]. Larger digest message produce by SHA-1, the stronger the network against multiple of attack [7].

From figure 6, the better encryption applied on site to site tunneling is AES 256 compared to others 3DES encryption. When encryption applied, the range of RTT data transferred was faster than 3DES encryption which is similar to previous result obtained by other researcher [1][2].This is due to the algorithm applied is the same, just the encryption techniques applied triple times security in comparison to DES in order to increase level of security. Hence three execution times on 3DES will consume higher CPU usage and response time is slower since 3DES required a lot of bits manipulation.

Figure 7, 8 9 and 10 represents the combination of encryption algorithms when varying the packet length size from 10, 100 to1000 Bytes. Results can be seen that the average of round trip time (RTT) was maintain on different packet size length (either 10 bytes, 100 Bytes and 1000 Bytes) since the packet size transferred was within the Maximum Transfer Unit (1500 Bytes) and the value tested is small. Hence, the changed on packet length size was not effect on RTT result.

V- CONCLUSION

This paper focused on performance analysis of site to site IPSEC network with real time traffic via Window 7 environment. Performance comparison has been done for five different scenarios (without encryption algorithm, with AES 256 SHA-1, with AES 256 MD5, with 3DES SHA-1 and with 3DES MD5). The performance was compared by varying the combination of encryption algorithm and varying the packet length send via ICMP command. In the end, the result conclude that there is degradation of performance speed of round trip time(RTT) when the VPN tunneling set to be encrypted with IPsec protocol encryption. The highest RTT value recorded for 3DES encryption and follow by AES 256 and none encrypted network. Furthermore, the comparison between hash algorithms concludes that the SHA-1 is faster than MD5. A proposed for future project, analysis performance can be discuss in greater depth especially in terms of security and overall performance of an algorithm needs to be measured.

ACKNOLEDGEMENT

It is a pleasure to acknowledge my supervisor, Associate Professor Ruhani Ab Rahman for her kindness, important advice, support and guidance throughout project preparation and implementations. I also would like to express my gratitude to my colleague in involving sharing ideas and technical suggestion to smoothen the project. Not to forget my beloved husband and family members for encouragement and support .Last but not least a lot of thanks to Allah Al-Mighty for all the success, health, time and opportunity that He gave to me in order to complete this project.

REFERENCES

[1] H. O. Alanazi, B. B. Zaidan, A. A. Zaidan, H. A. Jalab, and M. Shabbir, "New Comparative Study Between DES , 3DES and AES within Nine Factors," vol. 2, no. 3, pp. 152–157, 2010.

[2] A. V. Uskov, "Information Security of IPsec-based Mobile VPN: Authentication and Encryption Algorithms Performance," *2012 IEEE 11th Int. Conf.*

Trust. Secur. Priv. Comput. Commun., pp. 1042–1048, Jun. 2012.

[3] M. Hafiz, M. Zaharuddin, R. A. Rahman, and M. Kassim, "Technical Comparison Analysis of Encryption Algorithm on Site-to-Site IPSec VPN," no. Iccaie, pp. 641–645, 2010.

[4] D. S. A. Elminaam and R. City, "Performance Evaluation of Symmetric Encryption Algorithms," pp. 58–64, 2009.

[5] A. Agung, P. Ratna, A. Shaugi, and M. Salman, "Analysis and Comparison of MD5 and SHA-1 Algorithm Implementation in Simple-O Authentication based Security System," pp. 99–104, 2013.

[6] J. Hisham and B. Osman, "SSL VPN Performance Evaluation," no. July, 2008.

[7] K. Suthar, "Analytical Comparison of Symmetric Encryption and Encoding Techniques for Cloud Environment," vol. 60, no. 19, pp. 16–19, 2012.

[8] S. Narayan, S. S. Kolahi, K. Brooking, and S. De Vere, "Performance Evaluation of Virtual Private Network Protocols in Windows 2003 Environment," *2008 Int. Conf. Adv. Comput. Theory Eng.*, pp. 69–73, Dec. 2008.

[9] J. Wu, "Implementation of Virtual Private Network based on IPSec Protocol," pp. 138–141, 2009.

[10] T. Berger, "Analysis of Current VPN Technologies," 2006.