Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 343-353 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Application of IP Security and Mac Address Filtering Authentication Methods to Build Encrypted Interconnection Networks

[1]Mochamad Akbar Fajar Hidayat Putra, [2]Ucuk Darusalam, [3]Andri Aningsih

Program Studi Teknik Informatika,
Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional, Jl.Sawo Manila, Pasar Minggu, Kota Jakarta Selatan, Daerah KhususIbukota Jakarta 12520

Email: [1]akbarfajar1302@gmail.com, [2]ucuk.darusalam@civitas.unas.ac.id, [3]andrianingsih@civitas.unas.ac.id

ARTICLE INFO

Article history:
Received: 04/14/2020
Revised: 04/28/2020
Accepted: 05/01/2020

Keywords:
Authentication,
Interconnection,
IP Security,
Security,
Mac Address Filtering.

ABSTRACT

The development of the industry is happening very fast, Making the company must improve its resource capabilities, one of which is the technology used to be able to contribute to the company. Security issues become very important at this time, especially for companies that already have many branches in different locations that require high-performance security systems, because the network interconnections that occur between the head office and branch offices are very vulnerable to attacks from irresponsible parties, The use of IP Security and MAC Address Filtering authentication methods on network devices is very useful to be able to protect, verify and filter company data from enemies on the internet. IP Security authentication provides integrity between connections, then Filtering MAC Address can help the router task to be able recognize users on the network, So that expected the combination between IP Security and Mac Address Filtering will provide security for every transfer and receive data from Headquarter to branch office, then the company doesn't have to worry about data package being robbed or manipulated by the irrensponsible parties

1. Introduction

Sending data and storing data through electronic media requires a process that can guarantee the security and integrity of the data sent. network security means ensuring that the data in hardware, software and network systems is protected, not damaged, unchanged for any reason and the system runs continuously without any interruption in service [1]. The data must remain confidential during transmission and reception, to fulfill this, the encryption (decryption and decryption) process of the data to be transmitted is carried out. Encryption is done at the time of delivery by changing the original data into confidential data while decryption is done at the time of receipt by changing confidential data into original data [2]. So the data sent during the sending process is confidential data, so that the original data cannot be known by unauthorized parties. Original data can only be known by recipients who have agreed keys.

Because of the need to improve security on a network, an interconnection network requires IPSec to be able to increase that security. Internet Protocol Security (IPsec) is a collection of protocols used to secure Internet Protocol (IP) communication with authentication and encryption on each packet data stream IP [2]. Mac address is a unique hardware address that is determined for identity on a network, each mac address is not the same as the others because it has been regulated for use by IEEE, by allocating Mac addresses to 48bit in hexadecimal. The first 24 bits represent company-specific code, while the remaining 24 bits represent the card number [3], an example of a mac address is as follows D0-C5-D3-96-C7-7F. Filtering is a method to determine what addresses / devices are allowed or prohibited to be able to carry out certain processes [4]. So the router will do a scan on each client to be able to determine which mac address can have access to the server connection.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 343-353 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

2. Research methods

A. Waterfall Model Method

In this study the waterfall model method used is depicted in Figure 1.The stages of the waterfall method model already reflect a complete process, including:

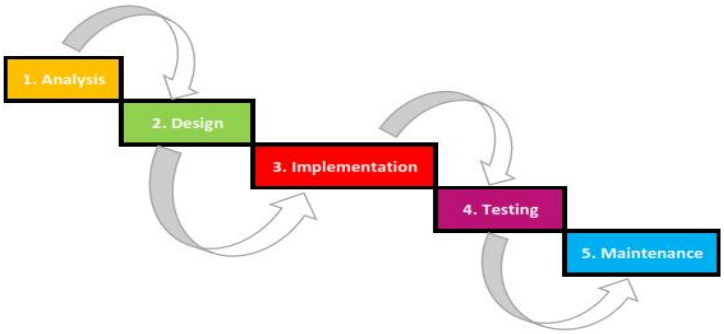

Fig 1. The Waterfall Method Model

1) Analysis, this stage is needed to understand the needs needed by the user.
2) Design, at this stage will be determined overall system specifications and architecture.
3) Implementation, at this stage the overall system design that has been made previously will be changed to a system topology which will later become an appropriate system.
4) Testing, at this stage the system configuration that has been made in the implementation phase will be tested to test the suitability of the system that has been designed.
5) Maintenance, the final stage in this method is the system will be run and carried out maintenance to correct system errors that were not found in the previous step.

B. Internet Protocol Security (IPSec)

IP Security (IPSec) is a set of network security protocols that are standardized byInternet Engineering Task Force(IETF) which functions to authenticate and encrypt data packets, IPsec uses cryptographic security services to protect communications over the network, This protocol will be implemented at the internet and transport layers in the OSI model layer [5] - [6].

In IPSec there are 2 security protocols, namely Authentication Header (AH) and Encapsulating Security Payload (ESP) which provide security mechanisms, while the Internet Key Exchange (IKE) key management protocol allows two nodes to negotiate the key of all parameters. AH is a procedure provided to ensure data integrity and authentication, by adding an authentication header that is inserted between the IP header and data transport [5]. The AH function is based on the HMAC algorithm, HMAC is a security algorithm used to ensure the authentication and integrity of data in computer networks [7]. The AH function will look like the one illustrated in Figure 2.

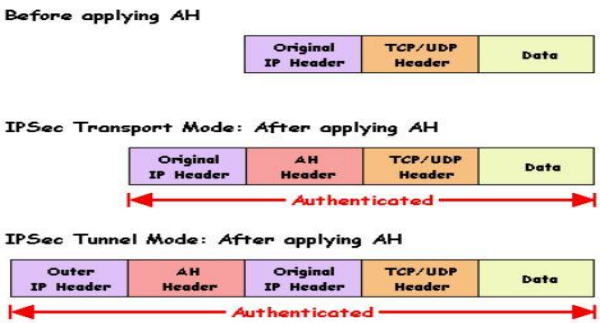

Fig 2. Authentication Header Function

While the Encapsulating Security Payload (ESP) main goal is to provide confidentiality by encrypting data by adding headers to the data before the data is sent to the destination, so the data will be

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 343-353 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

surrounded by security mechanisms [4]. In Figure 2 shows the ESP datagram structure, which shows how the original data will be covered by the ESP header on the front, ESP Trailer and ESP Authentication on the back, after that if using tunneling to send data, the header will also be added to tunnel mode header so that it does not easily identified by others who do not have a key that has been adjusted between the server and client on IPSec.

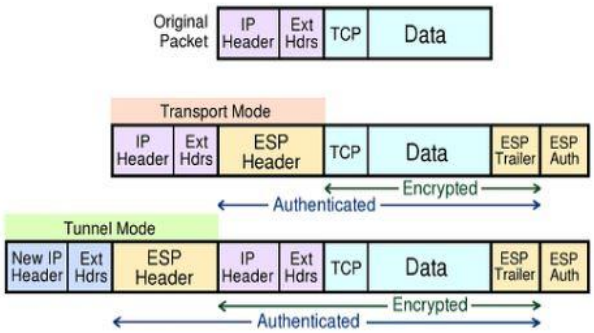

Fig 3. Encapsulating Security Payload function

C. Layer 2 Tunneling Protocol

Tunneling is a method for transferring data from one network to another network by utilizing the internet network in disguise [8]. The L2tp server will identify the l2tp client by matching the security and authentication types that have been set on the server, so that if the security and authentication types on the client are compatible with the server, then the l2tp connection will be established. Layer 2 Tunneling Protocol (L2TP) is one of the standard protocols to provide tunneling services that have a better level of security than before [8], to enhance higher security, this L2TP is usually added by using certain encryption that features in IPSec [9].

D. Quality of Service

QoS (Quality of Service) is defined as a mechanism that allows services to operate according to their characteristics [10]. To do QoS analysis on the network, the authors use the wireshark application. Wireshark is an open source packet analyzer, this tool is often used to find problems with networks, software development and communication protocols [11]. The author takes several parameters including [12]:

a) The time taken for a recipient to arrive (throughput).
b) Difference in arrival intervals between packets at the destination terminal (delay / latency).
c) The number of packets lost during the process of transmission to the destination (packet loss).
d) The number of bits received successfully per second through a system (jitter).

E. Design for IP Security and Mac Address Filtering Implementation

The next step is making a flowchart that will be presented in Figure 4.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 343-353 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

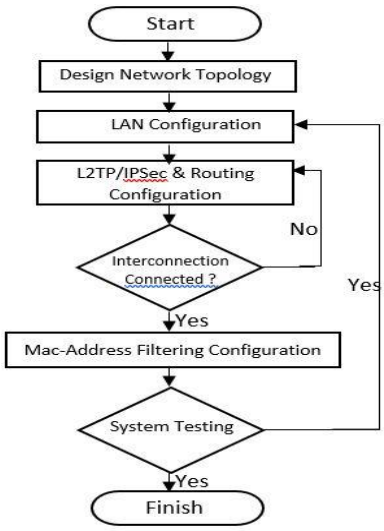

Fig 4. Design and Implementation flowchart

In Figure 4 it is explained that the first stage is the creation of the network topology of each of the Headquarters and Branch Office offices, after the topology design is made and then each local area network will be configured to connect to the internet, after the local network connection is connected, the next step is to configure L2TP / IPSec VPN and Routing Static to connect each of these offices, if the connection between offices is not established then more detailed checks must be made in the configuration, but if the interconnection is connected, the next step is to configure the Mac Address filtering on each router to determine which users can access the interconnection, so not all users can connect to that interconnection,then testing the system using the Wireshark application and command prompt on the computer to test the security and connections between the offices, if the results are what you want then, the implementation process has been completed and can be used by each user in the office.

3. Results and Discussion

A. Needs Analysis

The author has done an analysis for various types of devices needed and configuration of the IP address for each device as shown in table 1 and table 2. In the WAN IP Address router I use a Public IP not to protect the privacy of the Public IP that I have, to do the testing, it can still be done using the actual ip address with a few hidden IP Address.

Table 1
Hardware Specifications

No	Hardware	Component	Type	Quantity
1	Devices	Router	Mikrotik RB 750 R2	2 pcs
		Switch	TP-Link TL-SG1008D	2 pcs
		Access Point	TP-Link TL-WR845N	2 pcs
2	PC Server	Prosessor	XEON	2 pcs
		RAM	8 GB	2 pcs
		Harddisk	1000 GB	2 pcs
3	PC Client	Prosessor	Intel Core I5, Windows 10	2 pcs
		RAM	4 GB	2 pcs
		Harddisk	500 GB	2 pcs
4	Laptop Client	Prosessor	Intel Core I5, Windows 10	2 pcs
		RAM	4 GB	2 pcs
		Harddisk	500 GB	2 pcs
5	Tools	Crimping tools	Port RJ-45	1 pcs
		UTP Cable	Cat 5E	100 meter

Table 2

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 343-353 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

IP Address

No	Device	Interface	IP Address	Gateway	Location
1	Mikrotik Router	WAN	123.123.123.2/30	123.123.123.1/30	Headquarter
		LAN	192.168.1.1/24		
2	Access Point	LAN (Bridge Mode)	192.168.1.2/24	192.168.1.1/24	
3	PC Server	Eth0	192.168.1.254/24	192.168.1.1/24	
4	PC Client	Eth0	192.168.1.3/24	192.168.1.1/24	
5	Laptop Client	WLAN Card	192.168.1.4/24	192.168.1.1/24	
6	Mikrotik Router	WAN	124.124.124.2/30	124.124.124.1/30	Branch Office
		LAN	192.168.0.1/24		
7	Access Point	LAN (Bridge Mode)	192.168.0.2/24	192.168.0.1/24	
8	PC Server	Eth0	192.168.0.254/24	192.168.0.1/24	
9	PC Client	Eth0	192.168.0.10/24	192.168.0.1/24	
10	Laptop Client	WLAN Card	192.168.0.11/24	192.168.0.1/24	

B. Design Topology

The author makes the topology design described in Figure 5 below, the author makes 2 network schemes each for the head office and branch offices, with a local area network design that has the same topology but different IP address configurations.

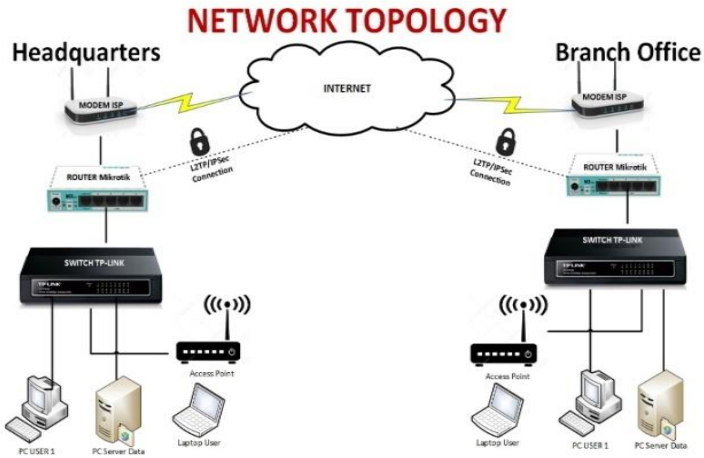

Fig 5. Network Topology

C. Device Configuration

After making the network topology design as needed, the next step is to configure the Mikrotik Router.

1) Mikrotik Headquarter Configuration Stage

a) WAN Interface Configuration is on the menu:
New terminal -> add command:

```
#ip address add address = 123.123.123.2 / 30 network = 123.123.123.0 interface =
ether1-WAN
```

b) LAN Interface Configuration is on the menu:
New terminal -> add command:

```
#ip address add address = 192.168.1.1 / 24 network = 192.168.1.0 interface = ether5-
LAN
```

c) Configuring L2TP Server, It's on the menu: PPP -> Interface Tab -> L2TP Server. with Secret IP: C0nn3ctS3rv3r

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 343-353 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

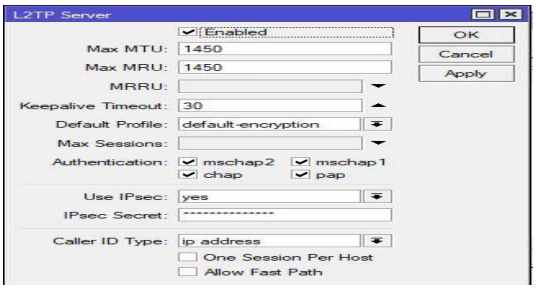

Fig 6. L2TP Server Interface

d) Create a Secret User,It's on the Menu: PPP -> Secret. Select the Secret Tab -> Click Add [+]. With Password: 5erverL2Tp

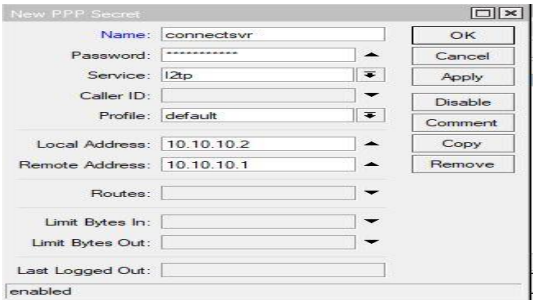

Fig 7. Secret L2TP Server settings

e) IP Security configuration, thereon the Menu: IP ->IPSec. Select IPSec Proposal Tab -> Click Add.

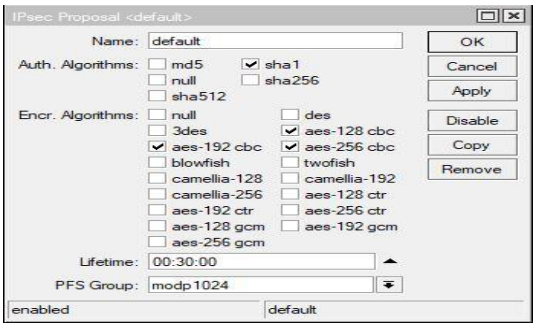

Fig 8. IPSec Server Settings

2) Branch Office Microtic Configuration Stage

a) WAN Interface Configuration is on the menu:
New terminal -> add command:

```
#ip address add address = 124.124.124.2 / 30 network = 124.124.124.0 interface =
ether1-WAN
```

b) LAN Interface Configuration is on the menu:
New terminal -> add command:

c)
```
#ip address add address = 192.168.0.1 / 24 network = 192.168.0.0 interface = ether5-
LAN
```
h
c
Headquarters.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 343-353 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

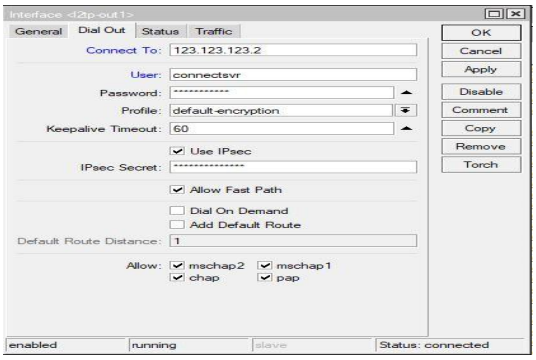

Fig 9. L2TP Branch Office

d) IP Security configuration, must be adjusted to the IPSec Server configuration, the configuration is there On the Menu: IP ->**IPSec**->IPSec Proposal tab -> Click Add.

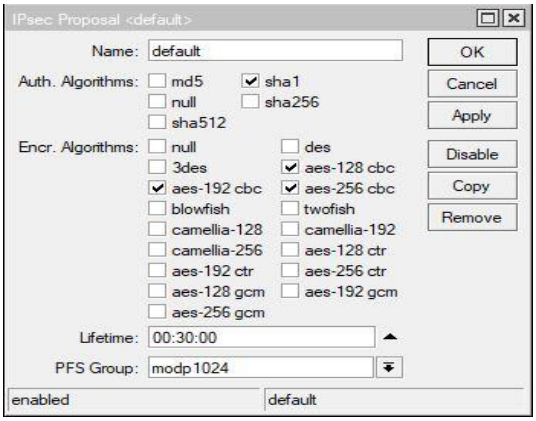

Fig 10. Sec IP Client

3) Configuring static routing for Router HQ, in the new terminal menu -> add command:

```
# ip route add gateway = 10.10.10.2 dst-address = 192.168.0.0/24 check-gateway = ping
type = unicast distance = 1 scope = 30 target-scope = 10
```

Then add routing for Branch Office, the same menu as the add command:

```
# ip route add gateway = 10.10.10.1 dst-address = 192.168.1.0/24 check-gateway = ping
type = unicast distance = 1 scope = 30 target-scope = 10
```

4) Configuring MAC-Address Filtering for Router HQ and Branch Office, is on the IP menu -> Firewall

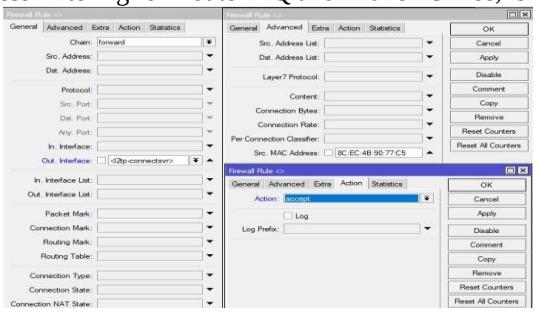

Fig 11. Mac-Address settings that are allowed access

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 343-353 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Also can enter the command in the proxy terminal by typing:

```
# ip firewall filter add chain = forward out-interface = "l2tp-connectsvr" src-mac-
address = 8C: EC: 4B: 90: 77: C5 action = accept.
```

Then for mac-address, enter the mac-address that is allowed to be able to access the data server on the vpn, then block all unauthorized users by entering the command:

```
# ip firewall filter add chain = forward out-interface = "l2tp-connectsvr" action =
```

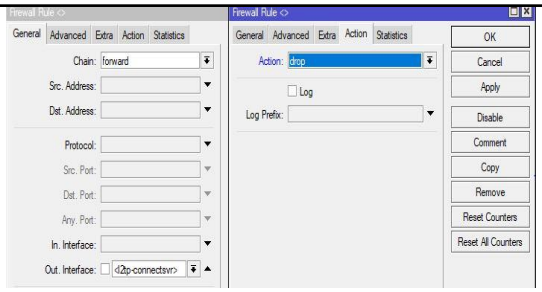

Fig 12. Block all VPN connections to the server

Then configure the Branch Office proxy, in the same way, can enter through the terminal on the proxy then type the command:

```
# ip firewall filter add chain = forward out-interface = "Connect To HQ" src-mac-
address = 00: 06: 19: 08: 00: 2D action = accept.
```

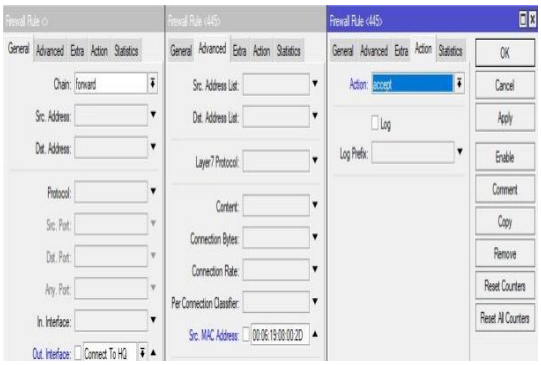

Fig 13. Mac-Address settings access to the HQ server

Then block all unauthorized users by entering the command:

```
# ip firewall filter add chain = forward out-interface = "Connect To HQ" action =
```

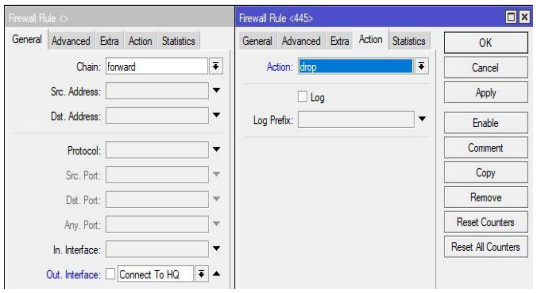

Fig 14. Block all VPN connections to the HQ server

4. System Configuration Testing

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 343-353 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

A. Test Inter-Office Connections

In this test, testing will be carried out on each router to see whether the connections between office routers are connected or not, using the PING and TRACEROUTE tools on the router.

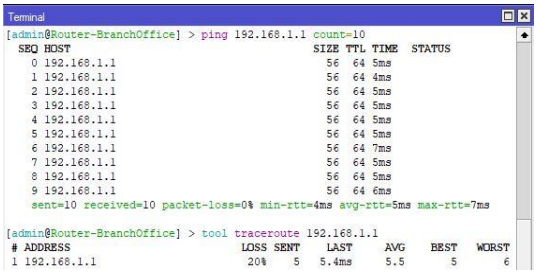

Fig15. PING & Tracert on Router Office Branch to Router-HQ

In figure 15, it can be concluded that the connections between offices are already connected because they are able to reciprocate ping and traceroute sent from each router.

B. Measurement of Quality of Service Analysis

The author tests by sending data from the Branch Office to the Headquarters by sending data of 15 Mbps and 10 Mbps with a bandwidth of each office of 10 Mbps using the Wireshark application for monitoring on each pc in the office, the following results of QoS analysis:

Table. 3
Quality of Service Analys

No	Description	Traffic Load	Parameter Quality of Service			
			Packet Loss	Delay (ms)	Jitter (kbps)	Throughput (kbps)
1	Headquarters -> Branch Office	File Data 15 Mbps	0%	0.001	0.001	9341k
2	Branch Office -> Headquarters	File Data 10 Mbps	0%	0.001	0.001	2652k

In the above data it can be concluded that the QoS results meet a good rating because the data sent does not have any damage / failed delivery because it produces 0% packet loss and good value of delay, jitter and throughput even though the location of sending and receiving data is different, it is also influenced by the amount of bandwidth available at each location, so that it only provides a very minimal delay to be able to send files of that size.

C. Test Mac-Address Filtering

In this test, the MAC-Address Filtering configuration will be tested, so only mac-addresses that have been registered to the router can access the data server via the VPN, other than that it is not permitted to be able to access the server.

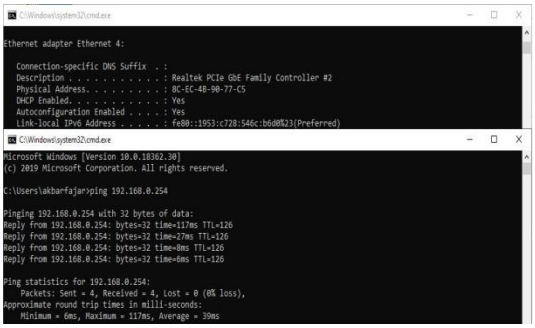

Fig 16. Mac-address that has been registered

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 343-353 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

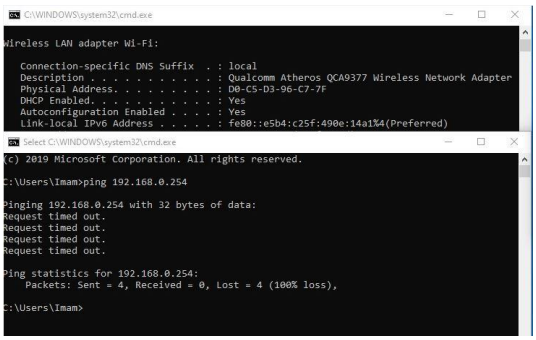

Fig 17. Mac-addresses that have not been registered

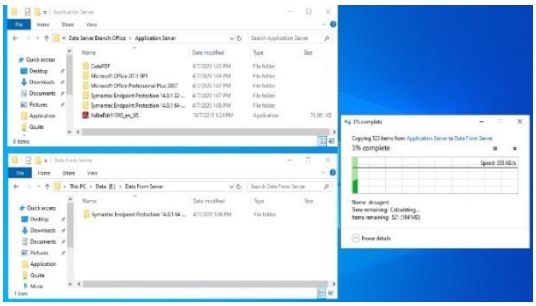

Fig 18. Data Transfer from HQ Offices to Branch Offices

In Figure 16, it is explained that the mac-address computer that is already registered can PING to the destination Server, then for Figure 17, it cannot ping the destination server because the mac-address has not been registered on the router. Figure 18 explains the file transfer process between client computers that can already access the server, by testing the copy of data software from the server computer to the client computer.

D. Test Data Security

In the same test when measuring QoS using wireshark, wireshark can also identify packet data that passes through the network, by reading every detail of the sending process from the sender and receiver, as shown in Figure 19.

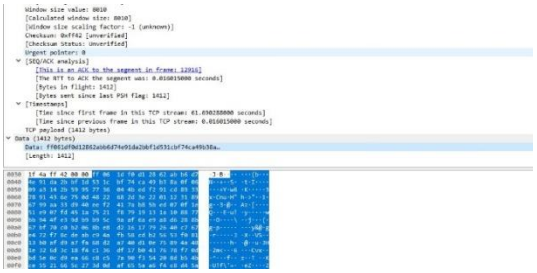

Fig 19. Wireshark Data Monitoring

In figure 19 it is explained that the data packet through the network connection between the Headquarter Office and Branch Office uses encryption data consisting of letters, numbers and symbols provided by IPSec in the form of an ESP header.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 343-353 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

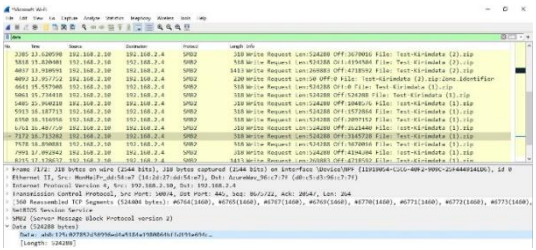

Fig 20. Wireshark Data Monitoring (2)

In Figure 20, it is explained that sending data between the local area network, between the client computer in Headquarter and the server, the data transmission is not encrypted by IPSec so that the name of the folder / file name is identified by WireShark.

5. Conclusion

In this study it has been proven that data security is very important at this time, because data is a very important information for a company / personal, therefore the application of MAC Address Filtering and IP Security on interconnection networks, has an impact to be able to minimize the occurrence attacks from irresponsible parties to be able to access / manipulate data on the network, because the router must ensure / register the user's mac address to be able to access data on the server, the use of IP Security also makes the data transferred between the sender and receiver to have hmac encryption to ensure that only the party who has the cryptographic key can open the data access, in this case the proxy router in the Branch Office.

6. Reference

[1] A. Gani, Aplikasi Pengaruh Quality of Service (QoS) Video Conference Pada Trafik H.323 Dengan Menggunakan Metode Differentiated Service (Diffserv), Universitas Syiah Kuala, 2010.
[2] Abdullah A. Al-khatib and Rosilah Hassan," Impact of IPSec protocol on the performance of network Real-Time Applications," Research center of Software Management and Technology, International Journal of Network Security, July 2017 19(01 1):800-808.
[3] Alfred Tan Yik Ern, "Network Security," Thesis at Asia Pasific University of Technology and Innovation, November 2019 DOI : 10.13140/RG.2.2.19900.59526.
[4] B. H. Kang and M. O. Balitanas, "Vulnerabilities of VPN using IPSec and Defensive Measures," International Journal of Advanced Science and Technology, vol. 8, no. 7, pp. 9-18, 2009.
[5] Mohannad Najjar, "d-HMAC — An improved HMAC," International Journal of Computer Science and Information Security, vol. 13, no. 4, 2015.
[6] Monika Asija, "Mac Address," IRA-International Journal of Technology & Engineering, volume 03, Issue 1, April 2016 ISSN 2455-4480.
[7] Muhammad Fiqri Muthohar. 2009. Studi Penerapan beberapa Algoritma Kriptografi pada IPSec. Diunduh dari https:// informatika.stei.itb.ac.id
[8] Rachmat Adi Purnama," Optimalisasi Keamanan Jaringan Wireless Menggunakan Firewall Filtering MAC Address," Indonesian Journal on Networking and Security, Volume 8, No 4 - 2019 ISSN 2354-6654.
[9] Rajeev Goyal and Samta Jain Goyal, "A Review On Layer 2 Tunneling Protocol," International Journal of Application and Innovation in Engineering Management, vol. 3, Issue. 10, October 2014 ISSN 2319-4847.
[10] Rika Wulandari,"Analisis QoS (Quality of Service) Pada Jaringan Internet (Studi Kasus : UPT Loka Uji Teknik Penambangan Jampang Kulon - LIPI," JURNAL Teknik Informatika dan Sistem Informasi, Volume 2, No. 2 Agustus 2016, ISSN 2433-2229.
[11] Sridevi, "L2TP/IPsec Interworking", IJSRInternational Journal Of Scientific Research, Volume 2, Issue 8, 2013, pp 89-91.
[12] U. Lamping , R. Sharpe dan E. Warnicke, "Wireshark User's Guide for Wireshark 2.1," [Online]. Available: https://www.wireshark.org/download/docs/userguide.pdf. [Diakses 5 Mei 2020].