TEKNOKOM : Jurnal Teknologi dan Rekayasa Sistem Komputer
Vol. 4, No. 1, March 2021, pp. 30 - 36
ISSN: 2686-3219, DOI: 10.31943/teknokom.v4i1.59

VPN SITE TO SITE IMPLEMENTATION USING PROTOCOL L2TP AND IPSEC

Budi Santoso[1], Asrul Sani[2*], T. Husain[3], Nedi Hendri[4]
[1, 2]Department of Informatics, STMIK Widuri, Jakarta, Indonesia
[3]Department of Information System, STMIK Widuri, Jakarta, Indonesia
[4]Department of Accounting, Universitas Muhammadiyah Metro, Lampung, Indonesia

ARTICLE INFO
History of the article:
Received June 3, 2021
Revised June 7, 2021
Accepted June 8, 2021
Published June 9, 2021

Keywords:
VPN
L2TP
IPSec
Networking

ABSTRACT

Data exchange communication has developed, which leads to centralized communication, and to achieve this communication requires a type of data communication whose data is accommodated on the server and can be accessed by clients, such as at organization. As a company engaged in education, the development of centralized data communication by utilizing the intranet network has been formed. The use of an intranet network allows data communication that is vulnerable to wiretapping. To fix this using a VPN network. L2TP and IPsec VPNs have different performances, especially in the level of security provided. In this study, an analysis of the L2TP and IPsec VPN network performance was carried out on the SMB Server on the Ubuntu server and the Mikrotik router for its VPN configuration. In this study, the L2TP and IPsec VPN was designed by configuring the Mikrotik RB 450G router and the SMB Server configuration using Command Line Interface on Ubuntu 18.04 server. For security analysis, use hacking methods to get VPN Server login data and sniffing methods to get SMB Server login data and SMB data. For performance analysis using parameters of delay, throughput, and packet loss. Wireshark is software for checking by capturing each packet of data from an interface. The research objective to be achieved is to design a VPN technology based on L2TP & IPSec, to be able to determine the resulting performance after implementing a VPN based on L2TP & Ip Sec. The result is that VPN can connect from HO to branch one and branch two or connect from public connection to local connection. The Ubuntu server used is also running well, so it helps the VPN process properly.

Correspondence:
Asrul Sani,
Department of Informatics,
STMIK Widuri, Jakarta, Indonesia,
Email : asrulsani@kampuswiduri.ac.id

INTRODUCTION

This company was established in Jakarta in October 2019 and had several branches spread across Jakarta. The exchange of information between head offices and branches which are located far apart at this time is only through the media of telephone, e-mail or mail, however, as business processes develop and needs increase, the exchange of information between offices is indispensable, an easy, fast and safe method is needed. Basically, the process of exchanging information between regions and between countries is not much different from the exchange of information within an organization, only the media is different. This can also be done for the implementation of site-to-site VPNs in different regional conditions.

The problems that exist in the company are problems that must be resolved so that a system that supports company activities is needed to reduce the risk of delays in delivering information and a weak level of security to transfer essential company data. Currently, the company has three divisional buildings consisting of operational divisions, sales, and information technology divisions, where the distances between these division buildings are far from each other, and a private network has not yet been established. So far, data exchange between buildings is carried out, namely by using Flash Drive and e-mail, using this method is considered ineffective and efficient, especially in maintaining the confidentiality of company data. On the network currently running, there are Non-Real-Time Online applications and several servers that are used as file sharing and staging development servers, which later can be accessed by all employees between divisional buildings and employees who are outside the office (remote access) for accessing corporate networks to improve the performance and effectiveness of the use of the computer network sector and the internet [1, 2].

Currently, a new Local Area Network (LAN) has been formed at the head office, and all users are integrated with the head office and branch offices. The application of Virtual Private Network (VPN) technology serves to create a network tunnel from a local network to another local network via the internet to be connected and impressed in the same network. While the L2TP/IPSec protocol is a network security protocol that encrypts every data sent over the internet [3]. In other words, the researcher analyzes how the head office network can be connected to the branch office network using VPN technology.

The research objectives to be achieved in this study include a) Designing a Virtual Private Network (VPN) technology based on Layer 2 Tunneling Protocol (L2TP) & IPSec, which is applied in the company. b) Knowing the effectiveness and efficiency of the implementation of Virtual Private Network (VPN) based on L2TP & IPSec. c) Knowing the performance produced after the implementation of Virtual Private Network (VPN) based on Layer 2 Tunneling Protocol (L2TP) & Ip Sec.

RESEARCH METHOD

The data analysis method is a stage of the research process where the data collected is managed to be processed to answer the problem formulation. This data management and processing is called data analysis. This initial stage is carried out an analysis of needs, analysis of problems that arise, analysis of user desires, and analysis of topology/network. After everything has been analyzed, design is the next step to conceptualize needs, after design, then simulation, implementation, monitoring, and management.

The system design method used is Network Development Life Cycle (NDLC). In an NDLC cycle, there are six general stages of analysis, design, simulation, implementation, monitoring, and management [4, 5].

Material

VPN is a communication network technology that allows users to connect to a public network and connect to a local network. By utilizing the public network, users can access the local office network from anywhere, as if the user is in the office. VPN can occur between two end-systems or two PCs, or it can be between two or more different networks. VPN can be established using tunneling technology and encryption. VPN connections can also occur at all layers of the OSI protocol, so you can make VPN communication for whatever your needs. Thus, a VPN can also be categorized as an alternative Wide Area Network (WAN) infrastructure for obtaining a private point-to-point connection between two points [6, 7].

The VPN network itself has many types: OpenVPN, PPTP, L2TP, IPSec, and many more. PPTP, L2TP & IPSec are widely used because it is easier to build their infrastructure with a router to make a Vpn connection. It is different from Open VPN. Because it is required to build a server, where the server is to be the path of the local network and the public network, as if the network is the same, for Open VPN point to point the security level is very vulnerable because the encryption process is not applied, so the information exchange process is not recommended Open VPN, apart from requiring more costs, has to build a server and the encryption process is not enforced [7, 8].

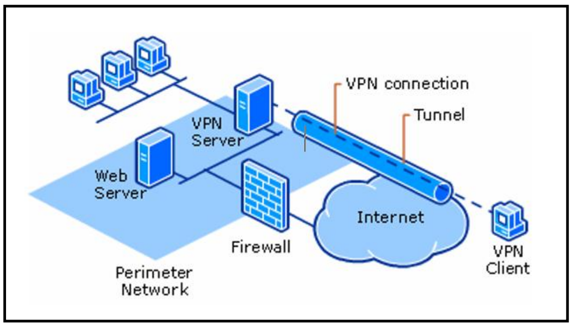


Figure 1. Virtual Private Number Model

Tunneling is the primary tunnel from the VPN to create a private network through the internet network. Tunneling is also the encapsulation or wrapping of a protocol into a protocol packet. Tunneling provides a logical point-to-point connection across a connectionless IP network. The process of transferring data from one network to another utilizes the internet network in disguise (tunneling). When the packet travels down to the destination node, it travels through a path called a tunnel. It is called a tunnel or channel because applications that use it only see two endpoints, so a packet passing through the tunnel will only make one hop or hop. Tunneling in VPN uses encryption to protect data from unauthorized parties and create a multiprotocol encapsulation if needed. It can be said that the computer used can access several computers or sites via the internet network so that the computers we use can communicate with other computers [9, 10].

L2TP is the development of PPTP, which is added with Layer Two Forwarding (L2F). L2TP has two main components: the L2TP Network Server (LNS), which functions to end and authenticate the PPP flow, and the L2TP Access Concentrator (LAC), ending a call. L2TP combines two reliable protocols: Microsoft PPTP and Cisco L2F [11]. This makes even a free L2TP VPN one of the best protocols to use. The encapsulation protocol can be IP and IPX, AppleTalk, and other protocols supported by PPP (although they are transmitted as IP packets). Just like with PPTP, L2TP does not encrypt data, nor does it authenticate individual messages. To overcome this deficiency, L2TP is often used in conjunction with IPSec. This combination provides an additional layer of authentication and encryption because L2TP packets are packaged in IPSec packets at the Network layer. L2TP operates at the Data-Link layer of the OSI model and uses UDP port 1701. There are two known tunnel models, namely Compulsory and Voluntary, the main difference between the two lies in the Endpoint Tunnel, on the Compulsory tunnel, the end of the tunnel is on the ISP, while at the Voluntary end of the tunnel at the ISP, remote client [12].

IPSec is a communication security standard over the internet with authentication and encryption for all IP packets passing through the IPSec data stream providing security at OSI layer 3, namely the network layer.

IPSec offers 3 main services, namely: authentication and data integrity, confidentiality, and key management. Authentication services, data integrity and confidentially on IPSec are provided by 2 main IPSec protocols, namely: Authentication Header (AH) and Encapsulated Security Payload (ESP) [13].

Methods

The type of research carried out is the NDLC (Network Development Life Cycle) development method, this development method is very suitable for this research, namely research related to networks that require stages of analysis, design, simulation, prototype, implementation, monitoring, and management in VPN design, based on L2TP / IPSec [14, 15].

To obtain materials as a basis for research that is useful as a reference in the design and research stage, research is carried out first, namely library research and field studies, research-based on modules, library files contained in the Mikrotik operating system, and coupled with discussions and interviews. To gain understanding and add to existing data.

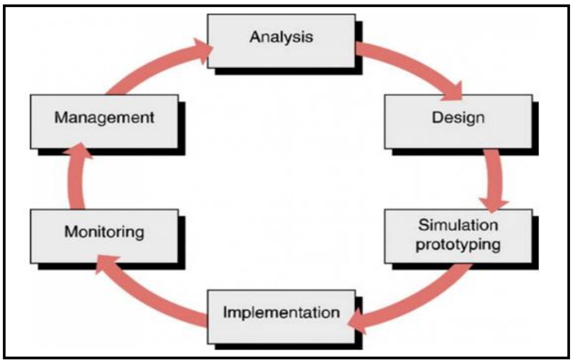


Figure 2. Network Development Life Cycle

Hardware (hardware) is an analysis of system requirements that are used to determine the devices needed to support the development process and use of the application system to be made.

A server is a specific type of service (service) in a computer network. The server is supported by a scalable processor and large RAM, with a unique operating system called a network operating system, the server is used for the Finance, Accounting, and HR, and GA divisions, to be used as server accurate and attendance management.

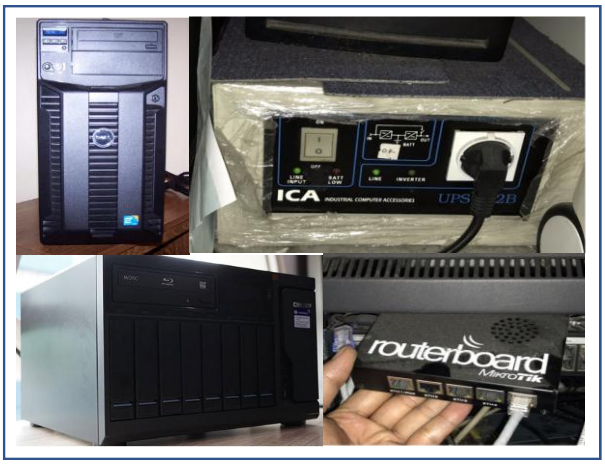


Figure 3. Hardware Requirements

UPS stands for Uninterruptible power supply to back up electricity when the PC loses energy from its primary source. The UPS works between the computer and the power outlet, from a power outlet supplied to the battery on the UPS and then stored for energy stability. The electricity stored in the battery will be used when the primary energy source of electricity is cut off.

Mikrotik is a router that regulates the entry and exit of bandwidth and data, a hardware technology supported by software and an operating system called the Mikrotik OS. This operating system is used for the administration of computer networks both on a small and large scale, the role of Mikrotik itself is to build and manage the internet network from internet providers to users or clients.

NAS stands for Network Attached Storage, a data storage device with an operating system devoted to serving data backup and sharing needs. With the completeness of open source software, NAS is a solution in data storage and file sharing, equipped with a LAN adapter, so NAS can be accessed using a computer network.

RESULTS AND DISCUSSION

In this study, the researchers designed a VPN network architecture based on the L2TP and IPSec protocols where all hardware (router, client device, and server) has been configured beforehand, the configuration must also be documented so that when there is trouble, maintenance, or device updates, there is no need to reconfigure, or you can say reinstallation and configuration backups are needed, this is based on the addition of a device, or if we change our device still has the previous configuration. When the L2TP and IPSec VPN connections are established, each local network will communicate as if it were in the same network through a tunnel. Tunneling is a technology used to form a private network connection by safely applying two or more networks because there is an encapsulation process.

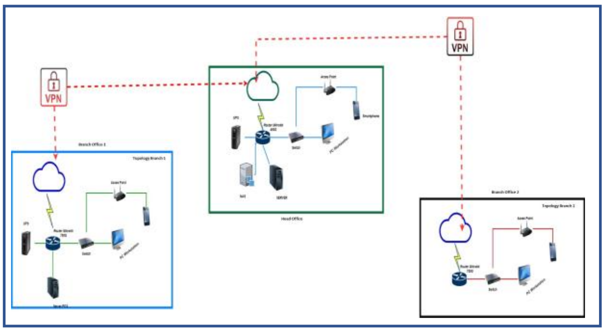


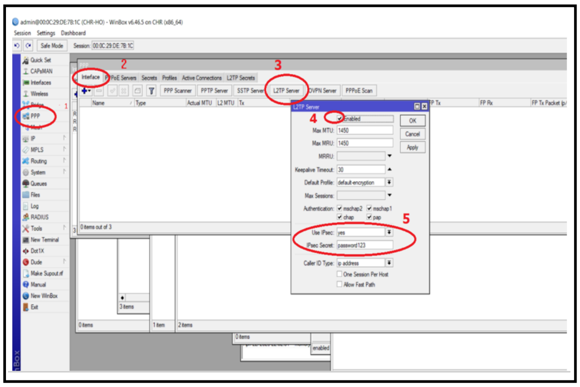
Figure 4. The Topology Proposed

Implementation is the next stage, where this stage will take time from the previous stage. The implementation stage will apply all the stages that have been planned and designed beforehand. Implementation is a very decisive stage of the success or failure of the project to be built, and the teamwork will test both technically and non-technically. To avoid many technical test errors, it is better to do virtualization in order to avoid accidental or intentional errors, usually testing using tools such as VMWare or VirtualBox, in addition to helping virtualization work, is also very much needed when a Network Engineer creates a new project with a device, and different designs, the best solution using virtualization.

After the implementation stage continues to the monitoring stage, the stage is essential so that computer and communication networks can run according to the initial wishes and goals of the user at the analysis stage, it is necessary to carry out the monitoring stage. Using this monitoring stage, most Network Engineers add configurations and tools such as MRTG, Wireshark, IPPerf, The Dude and others, to monitor network performance so that there are no problems and problems in the process. Network infrastructure development is needed to make it easier if there are network problems, both hardware, and software, the monitoring tools mentioned usually provide notices such as email, SMS, and even messages from telegram.

Configuration is the process of setting up a tool in the form of a script or digital code. In this configuration, it is done using a Graphical User Interface (GUI) or the type of user interface used on the device graphically, with this technology, the user can better understand the configuration process, besides the GUI configuration can also be done using the Command Line Interface (CLI).

After logging in to Mikrotik with winbox, there is a PPP menu then select the interface tab, then select L2TP server then check enabled, check IPSec and enter IP secret press OK.


admin@00:0C:29:DE:7B:1C (CHR-HO) - WinBox v6.46.5 on CHR (x86_64)

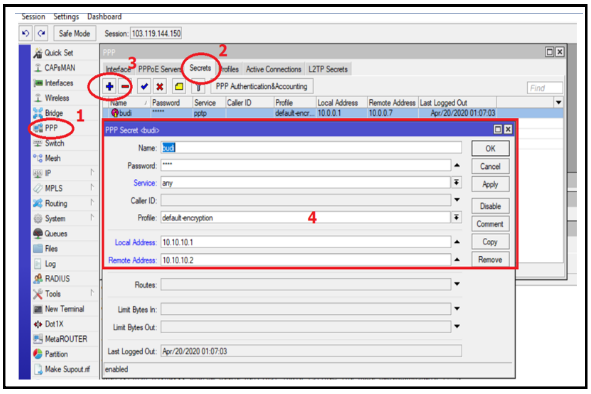
Session: 00:0C:29:DE:7B:1C

L2TP Server

4 ☑ Enabled
Max MTU: 1450
Max MRU: 1450
MRRU:
Keepalive Timeout: 30
Default Profile: default-encryption
Max Sessions:
Authentication: ☑ mschap2 ☑ mschap1 ☑ chap ☑ pap
5 Use IPsec: yes
IPsec Secret: password123
Caller ID Type: ip address
□ One Session Per Host
□ Allow Fast Path

Figure 5. The L2TP Server

The secret is an account to help log in or dial out from the client-side to be connected. Following are the steps for creating a secret that has been shown in Figure 6, by filling in the name, password, services are VPN services, use any so that at any time you change to other services. Profile input default-encryption, then add the IP address VPN local address, and remote address. This IP address will be added automatically when the VPN connection is established and serves as a data communication gateway.



Session: 103.119.144.150

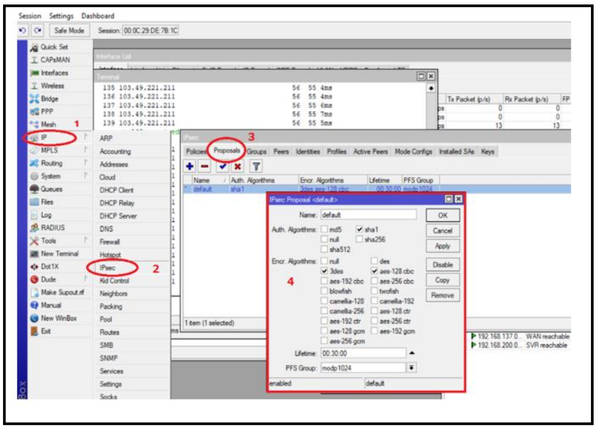
Name	Password	Service	Caller ID	Profile	Local Address	Remote Address	Last Logged Out
budi	*****	pptp		default-encr...	10.0.0.1	10.0.0.7	Apr/20/2020 01:07:03

PPP Secret <budi>

Name: budi
Password: ****
Service: any
Caller ID:
Profile: default-encryption
Local Address: 10.10.10.1
Remote Address: 10.10.10.2
Routes:
Limit Bytes In:
Limit Bytes Out:
Last Logged Out: Apr/20/2020 01:07:03
enabled

Figure 6. The Secret Server

IPSec is used to increase the level of security combining L2TP and IPSec, combining these protocols to create encryption codes so that the security level of a VPN connection is higher, in implementing IPSec the drawback is that the configuration installation to the client will take time because testing or testing is required. at both sites, it should be noted that implementing site-to-site VPN using L2TP and IPSec-based protocols is a tunneling technology that prioritizes security in the process, so it is no wonder companies use this protocol to connect every branch office and head office. Here are the steps or how to set it on the proxy router, select the IP menu then IPSec, select proposal, default, then select Authentication Algorithms, and the Encryption Algorithms continue OK.



Session: 00:0C:29:DE:7B:1C

```
135 103.49.221.211      56  55 4ms
136 103.49.221.211      56  55 4ms
137 103.49.221.211      56  55 6ms
138 103.49.221.211      56  55 7ms
139 103.49.221.211      56  55 5ms
```

Name	Auth. Algorithms	Encr. Algorithms	Lifetime	PFS Group
default	sha1	3des aes-128 cbc	00:30:00	modp1024

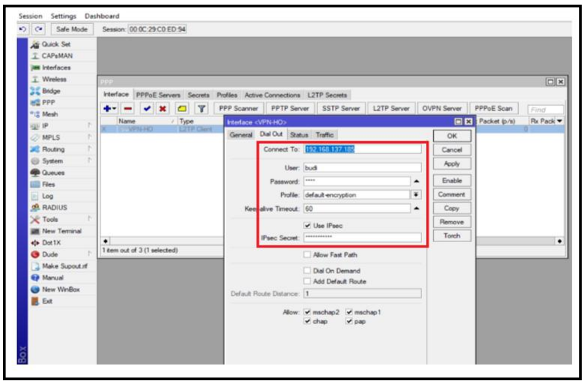
IPsec Proposal <default>

Name: default
Auth. Algorithms: □ md5 ☑ sha1 □ null □ sha256 □ sha512
Encr. Algorithms: □ null □ des ☑ 3des ☑ aes-128 cbc □ aes-192 cbc □ aes-256 cbc □ blowfish □ twofish □ camellia-128 □ camellia-192 □ camellia-256 □ aes-128 ctr □ aes-192 ctr □ aes-256 ctr □ aes-128 gcm □ aes-192 gcm □ aes-256 gcm
Lifetime: 00:30:00
PFS Group: modp1024
enabled default

Figure 7. IPSec to L2TP Server

After configuring on the server-side or head office, the next step is configuring on the client-side or branch office, activating the L2TP client, and then selecting dial out.

Dial-out connects the router server to the client router by calling the server-side public IP and then entering the username and password of the secret and then adding the IPSec secret created on the server-side.



Session: 00:0C:29:C0:ED:94

Interface <VPN-HO>

Connect To: 192.168.137.185
User: budi
Password: ****
Profile: default-encryption
Keepalive Timeout: 60
☑ Use IPsec
IPsec Secret: ************
□ Allow Fast Path
□ Dial On Demand
□ Add Default Route
Default Route Distance: 1
Allow: ☑ mschap2 ☑ mschap1 ☑ chap ☑ pap

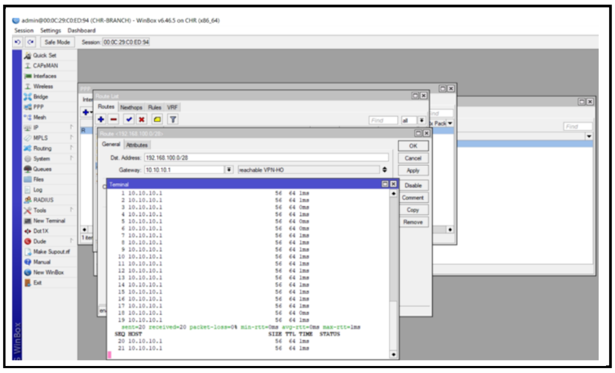
1 item out of 3 (1 selected)

Figure 8. Dial-Out L2TP+IPSec

The next step is to add the client-side IPSec settings, just like the server-side, without adding any other settings. The settings must be the same in order for the two communication processes to be connected.

Adding a static route is a link between site to site or between the source to the upstream, because the dial-out process has connected the IP public server, a dynamic route will automatically be formed, but there is a need for a static route to connect the local IP server so that it reads the ip secret in use it for VPN purposes, the IP will be routed to develop VPN L2TP and IPSec.

Up to this point, the two offices in different locations, which differ significantly in distance have been successfully connected to L2TP and IPsec VPN, which have a high level of security via the internet. IPsec configuration will not work if there is a mismatch of time information on the client and server. So make sure the time configuration is appropriate and in real-time conditions.



admin@00:0C:29:C0:ED:94 (CHR-BRANCH) - WinBox v6.46.5 on CHR (x86_64)

Session: 00:0C:29:C0:ED:94

Route <192.168.100.0/28>

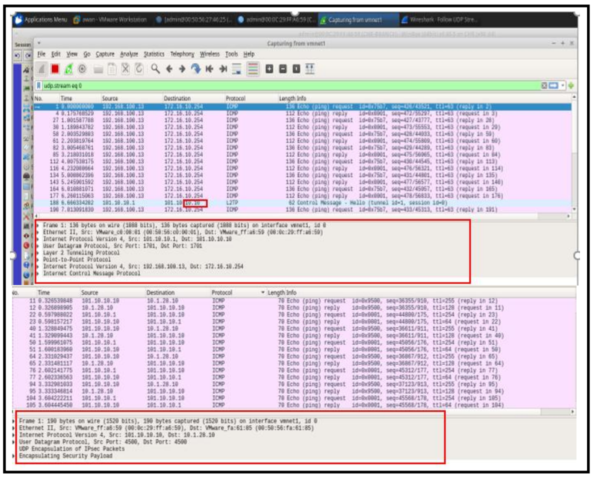
Dst. Address: 192.168.100.0/28
Gateway: 10.10.10.1 reachable VPN-HO

```
  1 10.10.10.1                                    56  64 1ms
  2 10.10.10.1                                    56  64 1ms
  3 10.10.10.1                                    56  64 0ms
  4 10.10.10.1                                    56  64 1ms
  5 10.10.10.1                                    56  64 0ms
  6 10.10.10.1                                    56  64 0ms
  7 10.10.10.1                                    56  64 1ms
  8 10.10.10.1                                    56  64 1ms
  9 10.10.10.1                                    56  64 1ms
 10 10.10.10.1                                    56  64 1ms
 11 10.10.10.1                                    56  64 1ms
 12 10.10.10.1                                    56  64 1ms
 13 10.10.10.1                                    56  64 1ms
 14 10.10.10.1                                    56  64 1ms
 15 10.10.10.1                                    56  64 1ms
 16 10.10.10.1                                    56  64 1ms
 17 10.10.10.1                                    56  64 1ms
 18 10.10.10.1                                    56  64 0ms
 19 10.10.10.1                                    56  64 1ms
    sent=20 received=20 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=1ms
SEQ HOST                                        SIZE TTL TIME  STATUS
 20 10.10.10.1                                    56  64 1ms
 21 10.10.10.1                                    56  64 1ms
```

Figure 9. Dial-Out L2TP+IPSec

Tests are carried out so that we can find out whether the L2TP and IPSec VPN services are running or not. Testing is done by sharing files between the client and server to the destination Network Attached Storage (NAS), previously from the client or branch side, they could not access the NAS at the head office or server, therefore testing was carried out so that we know whether the L2TP VPN service and this IPSec is running.

Performance testing A VPN's performance based on the L2TP and IPSec protocols is carried out by transferring files to measure the time it takes for a packet to reach its destination. This test is carried out in 2 stages: using the L2TP protocol only and combining L2TP and IPSec [16].



Applications Menu
awan - VMware Workstation
Capturing from vmnet1
Wireshark · Follow UDP Stre...
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.stream eq 0

```
No.   Time           Source           Destination     Protocol  Length Info
    1 0.000000000    192.168.100.13   172.16.10.254   ICMP      136 Echo (ping) request  id=0x75b7, seq=426/43521, ttl=63 (reply in 2)
    4 0.175768529    192.168.100.13   172.16.10.254   ICMP      112 Echo (ping) reply    id=0x0001, seq=472/55297, ttl=63 (request in 3)
   27 1.001587788    192.168.100.13   172.16.10.254   ICMP      136 Echo (ping) request  id=0x75b7, seq=427/43777, ttl=63 (reply in 28)
   30 1.189843782    192.168.100.13   172.16.10.254   ICMP      112 Echo (ping) reply    id=0x0001, seq=473/55553, ttl=63 (request in 29)
   58 2.003529803    192.168.100.13   172.16.10.254   ICMP      136 Echo (ping) request  id=0x75b7, seq=428/44033, ttl=63 (reply in 59)
   61 2.203819764    192.168.100.13   172.16.10.254   ICMP      112 Echo (ping) reply    id=0x0001, seq=474/55809, ttl=63 (request in 60)
   82 3.005468761    192.168.100.13   172.16.10.254   ICMP      136 Echo (ping) request  id=0x75b7, seq=429/44289, ttl=63 (reply in 83)
   85 3.218031018    192.168.100.13   172.16.10.254   ICMP      112 Echo (ping) reply    id=0x0001, seq=475/56065, ttl=63 (request in 84)
  112 4.007530175    192.168.100.13   172.16.10.254   ICMP      136 Echo (ping) request  id=0x75b7, seq=430/44545, ttl=63 (reply in 113)
  116 4.232080664    192.168.100.13   172.16.10.254   ICMP      112 Echo (ping) reply    id=0x0001, seq=476/56321, ttl=63 (request in 114)
  134 5.008862396    192.168.100.13   172.16.10.254   ICMP      136 Echo (ping) request  id=0x75b7, seq=431/44801, ttl=63 (reply in 135)
  143 5.245001592    192.168.100.13   172.16.10.254   ICMP      112 Echo (ping) reply    id=0x0001, seq=477/56577, ttl=63 (request in 140)
  164 6.010881071    192.168.100.13   172.16.10.254   ICMP      136 Echo (ping) request  id=0x75b7, seq=432/45057, ttl=63 (reply in 165)
  177 6.260115063    192.168.100.13   172.16.10.254   ICMP      112 Echo (ping) reply    id=0x0001, seq=478/56833, ttl=63 (request in 176)
  188 6.666334282    101.10.10.1      101.10.10.10    L2TP       62 Control Message - Hello (tunnel id=1, session id=0)
  190 7.013091830    192.168.100.13   172.16.10.254   ICMP      136 Echo (ping) request  id=0x75b7, seq=433/45313, ttl=63 (reply in 191)
```

```
▸ Frame 1: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface vmnet1, id 0
▸ Ethernet II, Src: VMware_c0:00:01 (00:50:56:c0:00:01), Dst: VMware_ff:a6:59 (00:0c:29:ff:a6:59)
▸ Internet Protocol Version 4, Src: 101.10.10.1, Dst: 101.10.10.10
▸ User Datagram Protocol, Src Port: 1701, Dst Port: 1701
▸ Layer 2 Tunneling Protocol
▸ Point-to-Point Protocol
▸ Internet Protocol Version 4, Src: 192.168.100.13, Dst: 172.16.10.254
▸ Internet Control Message Protocol
```

```
No.   Time           Source          Destination     Protocol  Length Info
   11 0.326539848    101.10.10.10    10.1.28.10      ICMP      70 Echo (ping) request  id=0x9500, seq=36355/910, ttl=255 (reply in 12)
   12 0.326898905    10.1.28.10      101.10.10.10    ICMP      70 Echo (ping) reply    id=0x9500, seq=36355/910, ttl=128 (request in 11)
   22 0.597988022    101.10.10.1     101.10.10.10    ICMP      70 Echo (ping) request  id=0x0001, seq=44800/175, ttl=254 (reply in 23)
   23 0.598157217    101.10.10.10    101.10.10.1     ICMP      70 Echo (ping) reply    id=0x0001, seq=44800/175, ttl=64 (request in 22)
   40 1.328849475    101.10.10.10    10.1.28.10      ICMP      70 Echo (ping) request  id=0x9500, seq=36611/911, ttl=255 (reply in 41)
   41 1.329099443    10.1.28.10      101.10.10.10    ICMP      70 Echo (ping) reply    id=0x9500, seq=36611/911, ttl=128 (request in 40)
   50 1.599961075    101.10.10.1     101.10.10.10    ICMP      70 Echo (ping) request  id=0x0001, seq=45056/176, ttl=254 (reply in 51)
   51 1.600183960    101.10.10.10    101.10.10.1     ICMP      70 Echo (ping) reply    id=0x0001, seq=45056/176, ttl=64 (request in 50)
   64 2.331029437    101.10.10.10    10.1.28.10      ICMP      70 Echo (ping) request  id=0x9500, seq=36867/912, ttl=255 (reply in 65)
   65 2.331481117    10.1.28.10      101.10.10.10    ICMP      70 Echo (ping) reply    id=0x9500, seq=36867/912, ttl=128 (request in 64)
   76 2.602141775    101.10.10.1     101.10.10.10    ICMP      70 Echo (ping) request  id=0x0001, seq=45312/177, ttl=254 (reply in 77)
   77 2.602336563    101.10.10.10    101.10.10.1     ICMP      70 Echo (ping) reply    id=0x0001, seq=45312/177, ttl=64 (request in 76)
   94 3.332981033    101.10.10.10    10.1.28.10      ICMP      70 Echo (ping) request  id=0x9500, seq=37123/913, ttl=255 (reply in 95)
   95 3.333346814    10.1.28.10      101.10.10.10    ICMP      70 Echo (ping) reply    id=0x9500, seq=37123/913, ttl=128 (request in 94)
  104 3.604222211    101.10.10.1     101.10.10.10    ICMP      70 Echo (ping) request  id=0x0001, seq=45568/178, ttl=254 (reply in 105)
  105 3.604445450    101.10.10.10    101.10.10.1     ICMP      70 Echo (ping) reply    id=0x0001, seq=45568/178, ttl=64 (request in 104)
```

```
▸ Frame 1: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits) on interface vmnet1, id 0
▸ Ethernet II, Src: VMware_ff:a6:59 (00:0c:29:ff:a6:59), Dst: VMware_fa:61:85 (00:50:56:fa:61:85)
▸ Internet Protocol Version 4, Src: 101.10.10.10, Dst: 10.1.28.10
▸ User Datagram Protocol, Src Port: 4500, Dst Port: 4500
  UDP Encapsulation of IPsec Packets
▸ Encapsulating Security Payload
```

Figure 10. Ping using L2TP and IPSec site to site

In the last stage, we tried to check the security of the L2TP and IPSec VPN concepts by providing ping packets and transferring files from the branch office to the head office. The test is carried out in 2 stages, namely the first testing using the L2TP protocol and the second using 2 L2TP and IPSec protocols in this way, we can find out that this VPN protocol can work without fear of data being stolen or manipulated by irresponsible parties.

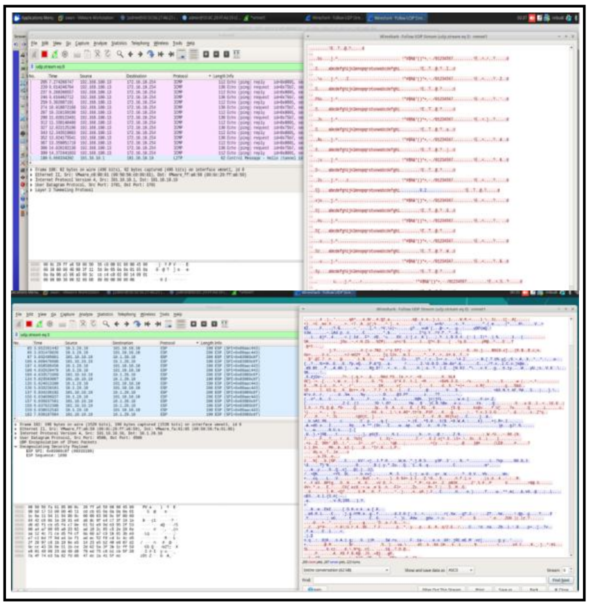


Figure 11. UDP Stream L2TP and IPSec Test

CONCLUSION

Based on the results of experiments that have been carried out using the Samba Server service using Ubuntu Server 16.04, it can be said that the interconnection in each branch is essential to support secure and fast communication in the company. Based on the tests conducted, the researchers concluded a) need a VPN connection at each branch to connect to the head office, b) VPN connects from HO, branch 1 and branch 2 or connects from a public connection to a local connection, as if in one network, c) Ubuntu Server 16.04 and Samba servers were chosen for testing because of the data load, so that we can conclude the VPN's capabilities.

Furthermore, as a consideration for the next research, it is necessary to make a Standard Operating Procedure (SOP) which is useful for optimal use and utilization of the network, besides that it can be helpful if there is further research, the use of VPNs based on the L2TP and IPSec protocols can be developed at other device vendors besides Mikrotik, and can also be developed with the L2TP / IKEv2 encryption method.

REFERENCES

[1] E. Mufida, D. Irawan, and G. Chrisnawati, "Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus Pada Yayasan Teratai Global Jakarta," *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer,* vol. 16, no. 2, pp. 9-19, 2017.

[2] A. Hidayat, "Analysis And Distance Access Design Far With Vpn Technology In Bmt Office. Mentari East Lampung," *IJISCS (International Journal of Information System and Computer Science),* vol. 3, no. 2, pp. 64-71, 2019.

[3] V. Bollapragada, M. Khalid, and S. Wainner, *IPSec VPN Design*. Cisco Press, 2005.

[4] H. Sujadi and A. Mutaqin, "Rancang Bangun Arsitektur Jaringan Komputer Teknologi Metropolitan Area Network (MAN) Dengan Menggunakan Metode Network Development Life Cycle (NDLC)(Studi Kasus: Universitas Majalengka)," *J-ENSITEC,* vol. 4, no. 01, 2017.

[5] R. T. Prabowo and M. T. Kurniawan, "Analisis dan Desain Keamanan Jaringan Komputer dengan Metode Network Development Life Cycle (Studi Kasus: Universitas Telkom)," *JRSI (Jurnal Rekayasa Sistem dan Industri),* vol. 2, no. 01, pp. 1-7, 2015.

[6] F. Hauser, M. Häberle, M. Schmidt, and M. Menth, "P4-IPsec: Site-to-Site and Host-to-Site VPN with IPsec in P4-Based SDN," *IEEE Access,* vol. 8, pp. 139567-139586, 2020.

[7] P. Arora, P. R. Vemuganti, and P. Allani, "Comparison of VPN Protocols–IPSec, PPTP, and L2TP," *Department of Electrical and Computer Engineering George Mason University, Project Report ECE,* vol. 646.

[8] R. Arlan, R. Munadi, and N. Andini, "Implementasi Dan Analisis Sistem Keamanan Ip Security (ipsec) Di Dalam Multi Protocol Label Switching-virtual Private Network (mpls-vpn) Pada Layanan Berbasis Ip Multimedia Subsystem (ims)," *eProceedings of Engineering,* vol. 3, no. 3, 2016.

[9] D. E. Kurniawan, H. Arif, N. Nelmiawati, A. H. Tohari, and M. Fani, "Implementation and analysis ipsec-vpn on cisco asa firewall using gns3 network simulator," in *Journal of Physics: Conference Series*, 2019, vol. 1175, no. 1, p. 012031: IOP Publishing.

[10] H. Pratama and N. F. Puspitasari, "Penerapan Protokol L2TP/IPSec dan Port Forwarding untuk Remote Mikrotik pada Jaringan Dynamic IP," *Creative Information Technology Journal,* vol. 7, no. 1, pp. 51-62, 2021.

[11] A. Haider and M. Houseini, "The Difference Impact on QoS Parameters between the IPsec and L2TP," *International hournal of Innovative n Advanced Engineering (IJIRAE),* vol. 11, no. 3, pp. 31-42, 2016.

[12] M. I. Majid, S. Ashraf, and H. Ghouri, "Using L2TP Protocol in Cloud Infrastructure with IoT for Secure and Robust Communication," *IEEEP New Horizons Journal,* pp. 34-37, 2018.

[13] M. Elezi and B. Raufi, "Conception of Virtual Private Networks using IPsec suite of protocols, comparative analysis of distributed database queries using different IPsec modes of encryption," *Procedia-Social and Behavioral Sciences,* vol. 195, pp. 1938-1948, 2015.

[14] T. Hidayat, "Encryption Security Sharing Data Cloud Computing by Using AES Algorithm: A Systematic Review," *TEKNOKOM,* vol. 2, no. 2, pp. 11-16, 2019.

[15] P. D. Arnesia and A. Aqim, "Rancang Bangun Jaringan VPN Berbasis IPSec Menggunakan Microtic Routerboard pada PT. Zahir nternational," *Prosiding SeNTIK,* vol. 3, no. 1, 2019.

[16] F. Arafat, A. Sani, N. Wiliani, and A. Budiyantara, "Optimalisasi Jaringan Wireless Dengan Metode Wireless Distribution System (WDS)," *BRITech, Jurnal Ilmiah Ilmu Komputer, Sains dan Teknologi Terapan,* vol. 1, no. 2, pp. 11-16, 2020.