Jurnal Mahasiswa Ilmu Komputer (JMIK)
Vol. 3, No. 2, Oktober 2022

IMPLEMENTASI VPN BERBASIS POINT TO POINT TUNNELING PROTOCOL (PPTP) MENGGUNAKAN LINUX UBUNTU SERVER PADA KOPERASI BUSP TULANG BAWANG LAMPUNG

Haris Perwira[1)], Mustika[2)], Arif Hidayat[3)]
[1-3)] Program Studi Ilmu Komputer, Universitas Muhammadiyah Metro

Jl. Gatot Subroto No.100, Yosodadi, Metro Timur, Kota Metro – Lampung
Email : ypain43@gmail.com[1)] ,dosen.mustika@gmail.com[2)],
androidarifhidayat@gmail.com[3)]

ABSTRAK : Koperasi Bima Utama Sakti Bratasena (Koperasi BUSB), adalah koperasi yang menjual kebutuhan rumahan, keperluan tambak udang yang dikelola oleh UUP Mandiri (Bratasena Mandiri). Dalam proses pertukaran data, UUP Mandiri dan Koperasi BUSB melakukan pertukaran data menggunakan surat elektronik (e-mail). Hasil wawancara dengan kepala IT dan karyawan Koperasi BUSB menyatakan bahwa adanya beberapa masalah mengenai kemanan, waktu, dan keutuhan data pada proses pertukaran data dikarenakan tidak adanya keamanan khusus. Dalam hal ini, penulis akan merancang jaringan pribadi (Virtual Private Network) antara Koperasi BUSB dan UUP Mandiri berbasis Point to Point Tunnelling Protocol (PPTP) dengan menggunakan sistem operasi Linux Ubuntu server yang di-install pada aplikasi Oracle VM VirtualBox. Jaringan private ini dirancang sebagai sarana yang lebih mudah, menghemat waktu serta biaya, dan lebih aman dalam mengirimkan data-data penting.

Kata Kunci: VPN, *Point to Point Tunnelling Protocol, Linux*

ABSTRACT : *Cooperative of Bima Utama Sakti Bratasena Village (BUSB Cooperative) is a cooperative that deals with household needs, shrimp farming needs which are managed by the UUP Adiwarna (Bratasena Adiwarna) and UUP Mandiri (Bratasena Mandiri). In the process of exchanging data, Mandiri UUP and BUSB Cooperative exchanged data using electronic mail (e-mail). The results of interviews with the head of IT and employees of the BUSB Cooperative stated that there were problems regarding the security, time, and validity of data in the data exchange process due to the absence of special security. In this case, the author developed a private network (Virtual Private Network) between BUSB Cooperative and UUP Mandiri with the basis of Point to Point Tunnelling Protocol (PPTP) using Linux Ubuntu Server operating system installed on Oracle VM VirtualBox application. This network was designed as means to save time and money as well as security in sending important data.*

Keywords: VPN, Point to Point Tunnelling Protocol, Linux

PENDAHULUAN

Koperasi Unit Desa Bima Utama Sakti Bratasena (Koperasi BUSB) adalah koperasi yang berjenis koperasi konsumen. Koperasi BUSB berada di desa Bratasena Adiwarna,

kabupaten Tulang Bawang, Lampung. Pada awalnya koperasi ini hanya menjual kebutuhan rumahan, tetapi semenjak tahun 2017 Koperasi BUSB juga menjual keperluan tambak udang seperti pakan dan obat-obatan untuk tambak, yang dikelola oleh sebuah Unit Usaha Pertambakan (UUP) yaitu UUP Mandiri (Bratasena Mandiri), yang berlokasi di desa Bratasena Mandiri, kabupaten Tulang Bawang, Lampung dan berjarak kurang lebih 9,5 KM dari Koperasi BUSB. Karena jaraknnya yang lumayan jauh, sebelumnya UUP Mandiri dan Koperasi BUSB melakukan pertukaran data menggunakan surat elektronik (*e-mail*) dan menggunakan data yang telah dicetak kedalam bentuk kertas. Jika menggunakan *email* UUP dan Koperasi BUSB belum bisa memastikan keamanan data yang dikirim. Jika menggunakan bentuk fisik seperti kertas, UUP Mandiri membutuhkan banyak waktu dan biaya. Dari permasalahan tersebut dalam mengakses suatu data di UUP dan Koperasi BUSB akan dibangun suatu jaringan pribadi (*private network*) yang digunakan untuk menjaga kebenaran dan keamanan data dari pihak yang tidak berwenang dan juga untuk menghubungkan jaringan UUP Mandiri dan Koperasi BUSB agar lebih mudah dalam pengiriman data. Teknologi *private network* merupakan sistem komunikasi dalam suatu jaringan pribadinya yang terpisah dari jaringan publik. Jaringan pribadi ini dinilai lebih efisien karena kecepatan transmisi data lebih tinggi daripada kecepatan transmisi data di *Internet*, serta kemampuan keamanan dijaringan pribadi dinilai lebih baik karena hanya bergerak dalam jangkauan yang terbatas. Suatu masalah timbul apabila antar lokasi pada institusi letaknya cukup jauh. *Virtual Private Network* (VPN) hadir sebagai solusi. Caesar (2014: 43) mendefinisikan ”VPN merupakan singkatan dari *Virtual Private Network* yang artinya membuat jaringan private secara virtual di atas jaringan publik (umum) seperti *internet*”. Dengan koneksi VPN, keamanan jaringan lebih mudah dikonfigurasi dan dikontrol. *Server* VPN dapat dibangun dengan menggunakan beberapa cara, salah satunya adalah dengan menggunakan sistem operasi *Linux Ubuntu, Linux* adalah sistem operasi *open source* dan gratis*. Open source* artinya *source code Linux* ini gratis dan bebas untuk dikembangkan, selain itu *linux* juga lebih stabil untuk dijadikan *server* karena *Linux* dapat jalan di komputer dengan spesifikasi yang rendah sekalipun. Ada beberapa protokol dalam penerapan VPN, protokol yang digunakan dipenelitian ini adalah *Point To Point Tunneling Protocol* (PPTP). “PPTP merupakan salah satu jenis VPN yang mempunyai konfigurasi yang mudah, yang dimana prosesnya membungkus data dan dikirimkan melalui *tunneling* lalu diteruskan”. (Rasuanda dan Haeruddin, 2020, 12)

KAJIAN PUSTAKA DAN LANDASAN TEORI

Jaringan komputer

Watmah (2020: 6) menjelaskan jaringan komputer adalah “beberapa komputer yang saling terhubung agar komputer-komputer tersebut dapat berkomunikasi, bertukar data

maupun informasi, serta berbagi sumber daya".

Virtual Private Network (VPN)

Menurut Oktivasari dan Utomo (2016: 187) *Virtual Private Network (VPN)* adalah sebuah teknologi komunikasi yang memungkinkan dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. *VPN* merupakan koneksi virtual yang bersifat private, dikarenakan jaringan yang dibuat tidak nampak secara fisik hanya berupa jaringan virtual, dan jaringan tersebut tidak semua orang dapat mengaksesnya sehingga sifatnya private. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada di dalam kantor atau *LAN* itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik.

Point-to-Point Tunneling Protocol (PPTP)

Mufida (2017: 13) menyimpulkan *Point-to-point Tunneling Protocol* (PPTP) merupakan *protocol* jaringan yang memungkinkan pengamanan transfer data dari *remote client* ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP. Pembuatan PPTP yang memakan biaya cukup kecil dan mudah untuk digunakan secara luas, menjadi sebuah solusi untuk *remote user* dan *mobile user* karena PPTP memberikan keamanan serta enkripsi komunikasi melalui PSTN ataupun *internet.*

A. Linux

Harsabat (2014: 63) mendefinisikan *Linux* adalah sistem operasi sumber terbuka (*Open Source*). Setiap *OS* berbasis *Linux* melibatkan kernel *Linux* yang mengelola sumber daya perangkat keras. *Linux* mencakup beberapa komponen inti umum, seperti *tools GNU* dan lain-lain. Alat-alat ini memberikan cara untuk mengelola sumber daya yang disediakan oleh kernel, menginstal perangkat lunak tambahan, mengkonfigurasi pengaturan kinerja dan keamanan, dan banyak lagi.

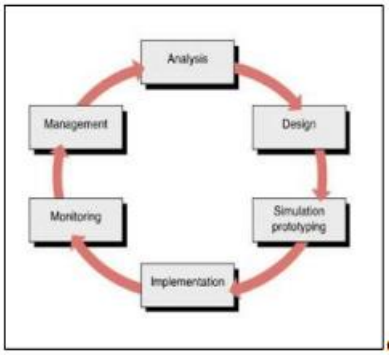
Linux Ubuntu

Harsabat (2014: 63) menjelaskan *Ubuntu* adalah sistem operasi lengkap berbasis *Linux*, tersedia secara bebas dan mempunyai dukungan baik yang berasal dari komunitas maupun tenaga ahli profesional.

METODE

Untuk memperoleh data yang dibutuhkan peneliti menggunakan teknik pengumpulan data yaitu : studi lapangan yang terbagi menjadi 3 tahap (observasi, wawancara dan dokumentasi) serta studi literatur.

Dalam metode pengembangan sistem penulis menggunakan metode *Network Development Life Cycle (NDLC)* yang merupakan suatu pendekatan proses dalam komunikasi data yang menggambarkan siklus yang awal dan akhirnya dalam membangun sebuah jaringan komputer.



Gambar 1. Metode NDLC

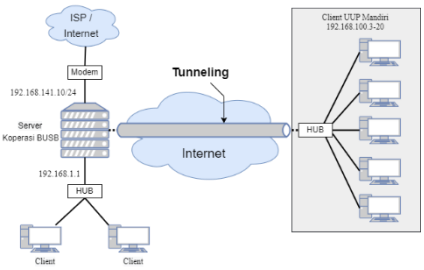
HASIL DAN PEMBAHASAN

Analysis (analisis)

Model pengembangan sistem NDLC dimulai pada fase analisis dimana pada tahap ini membahas proses analisis kebutuhan perancangan dan implementasi sistem VPN. Sebelum dilakukan pengembangan dan perancangan sistem, terlebih dahulu dilaksanakan analisis kebutuhan-kebutuhan pokok Jaringan VPN yang akan dibangun.

Design (perancangan)

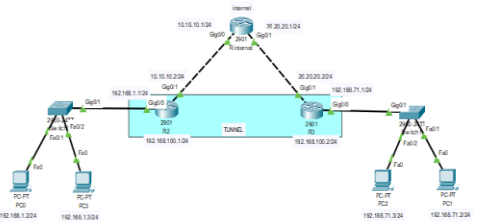
Dari data-data yang didapatkan sebelumnya tahap *design* ini akan membuat gambar desain topologi jaringan interkoneksi yang akan dibangun. Diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. Desain bisa berupa desain struktur topologi, desain akses data, desain layout perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang proyek yang akan dibangun yaitu berupa gambar-gambar topologi (*server, client*, perkabelan, titik akses dan sebagainya). Tahap *design* yang penulis gunakan ini mencakup topologi VPN yang akan dibangun dapat dilihat pada gambar 2



Gambar 2. Desain topologi VPN

Simulation Prototyping

Tahap *Simulation Prototyping* merupakan pembuatan simulasi dengan aplikasi simulator. Dimana pada tahapan simulasi ini akan membangun prototipe sistem VPN dari data yang telah didapat pada tahapan sebelumnya dengan menggunakan *software Cisco Packet Tracer* sebagai replika dari sistem yang akan dijalankan. Penulis menggunakan aplikasi *Cisco Packet Tracer* sebagai simulasi VPN yang dapat dilihat pada gambar 3.



Gambar 3. Simulasi *Cisco Packet Tracer*

Implementation

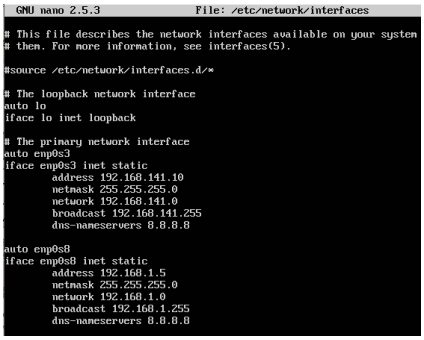
Pada tahap implementasi ini penulis akan menjelaskan beberapa konfigurasi diantaranya adalah konfigurasi *VPN linux ubuntu server* dan implementasi *VPN client*,

Kofigurasi VPN linux ubuntu server

Pada tahap ini penulis akan menjelaskan tahap-tahap konfigurasi *VPN server* pada *linux ubuntu server*.

Konfigurasi file/network/interfaces

Interfaces merupakan file yang terdapat pada folder *network.* Untuk konfigurasinya dapat dilihat pada gambar 4.



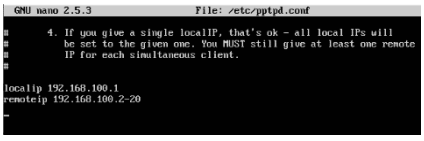
```
GNU nano 2.5.3                File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# them. For more information, see interfaces(5).

#source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet static
        address 192.168.141.10
        netmask 255.255.255.0
        network 192.168.141.0
        broadcast 192.168.141.255
        dns-nameservers 8.8.8.8

auto enp0s8
iface enp0s8 inet static
        address 192.168.1.5
        netmask 255.255.255.0
        network 192.168.1.0
        broadcast 192.168.1.255
        dns-nameservers 8.8.8.8
```

Gambar 4. Konfigurasi file *network interfaces*

Pada gambar 4, *network/interfaces* merupakan file yang digunakan untuk mengatur *IP address* adapter atau *ether* jaringan *linux ubuntu server.* Pada *linux ubuntu server* yang penulis gunakan, adapter satu secara *default* bernama *enp0s3* dan adapter dua bernama *enp0s8*. Adapter satu atau *enp0s3* merupakan IP publik yang digunakan sebagai jalur masuknya *internet. IP address* pada *enp0s3* bisa diatur dinamis dimana *IP address* secara otomatis diatur oleh sistem atau bisa juga diatur statis dimana *IP address* diatur manual oleh penguna. Jika di set secara statis maka *IP address* harus diset pada *network* yang sama dengan *IP public default* / *dhcp,* ini dimaksudkan agar *linux ubuntu server* dapat terkoneksi atau terhubung ke internet. Disini penulis menggunakan konfigurasi IP statis dengan *IP address* yang satu *network* dengan *IP dhcp* yaitu 192.168.141.x. Konfigurasi dengan IP statis dimaksudkan agar memudahkan penulis pada tahap selanjutnya.

Konfigurasi file *pptpd.conf*

File *pptpd.conf* digunakan untuk mengatur *IP address* yang akan digunakan oleh *client* VPN. Konfigurasi file *pptpd.conf* dapat dilihat pada gambar 5.

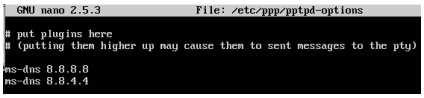


Gambar 5. Konfigurasi file *pptpd.conf*

Pada gambar 5 terdapat 2 konfigurasi tamban yaitu *localip* dan *remoteip,* dimana *localip* 192.168.10.1 merupakan *IP address VPN server* dan *remoteip* 192.168.10.3-20 merupakan *IP address* yang akan diberikan kepada *VPN client*.

Konfigurasi /ppp/pptpd-options

ppp/pptpd-options merupakan file konfigurasi untuk menambahkan DNS server. Konfigurasi *ppp/pptpd-options* dapat dilihat pada gambar 6.

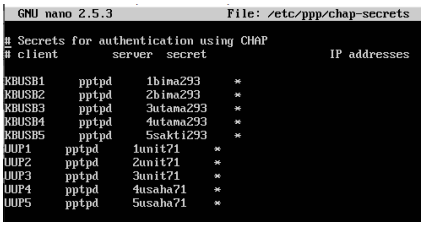


Gambar 6. Konfigurasi file *pptpd-options*

Penambahan DNS server dimaksudkan agar VPN client mendapat DNS tersebut atau client dapat terhubung ke internet.

Konfigurasi /ppp/chap-secrets

Chap-secrets merupakan sebuah file yang berisi konfigurasi manajemen akun *user* atau *client VPN*. Konfigurasi file *chap-secrets* dapat dilihat pada gambar 7.



Gambar 7. Konfigurasi file *chap-secrets*

Pada gambar 25 merupakan isi dari file *chap-secrets* yang terlihat seperti tabel. Dimana kolom pertama yaitu *client* yang merupakan nama identitas pengguna atau *user*. Kolom kedua yaitu *server* merupakan *server VPN* yang digunakan. Kemudian ada kolom *secret* yang merupakan *password* untuk *user VPN.* Lalu ada *IP addresses* yang merupakan alamat IP yang akan diberikan oleh server VPN, disini penulis memberikan simbol bintang (*) pada *IP address* semua *user* yang dimaksudkan untuk memberikan *IP address* otomatis sesuai dengan

remoteip pada konfigurasi file *pptpd.conf.*

Menambahkan rules iptables

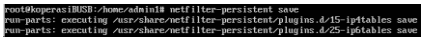
Iptables merupakan seperangkat aturan *firewall* yang secara *default* disediakan oleh sistem operasi linux. Penambahan rules iptables dapat dilihat pada gambar 8.

Gambar 8. Penambahan *iptables rules*

Pada gambar 8, penulis menambahkan baris perintah *rules iptables* yang digunakan agar *firewall ubuntu server* mengizinkan VPN dapat terhubung ke internet.

Menyimpan rules iptables

Konfigurasi iptables telah berhasil, selanjutnya adalah konfigurasi untuk menyimpan *rules iptables* yang dapat dilihat pada gambar 9.



Gambar 9. Menyimpan *rules iptables*

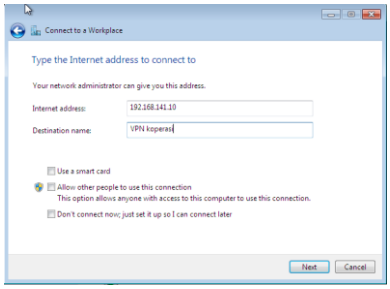
Pada gambar 9 *command* yang digunakan adalah *netfilter-persistent save*. Secara default *rules iptables* yang telah dikonfigurasikan akan hilang saat komputer di *restart/reboot.* Untuk mengatasi hal ini penulis memberikan tambahan konfigurasi *netfilter-persistent save* untuk menyimpan *rules iptables* supaya admin tidak mengonfigurasi ulang saat komputer di-*restart.*

Implementasi *VPN client*

Setelah tahap konfigurasi VPN server, tahap selanjutnya adalah meng-implementasikan VPN ke *client. Client* menggunakan sistem operasi *windows 7*. Adapun beberapa tahap dalam imlementasi pada *client* yaitu mengisi alamat IP server VPN, pengisian informasi akun VPN, dan VPN terhubung.

Mengisi alamat IP *server VPN*

Kemudian akan diarahkan untuk mengisi alamat server VPN yang dapat dilihat pada gambar 10.

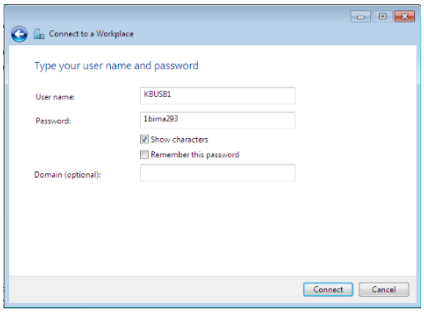


Gambar 10. Pengisian alamat IP *VPN server*

Pada gambar 10 terlihat bahwa ada permintaan untuk mengisi "*internet address"* dan *"destination name"*. *internet adress* merupakan *IP address* server yang dituju, disini penulis mengisi internet address dengan *IP address* yang dimilki oleh VPN server yaitu 192.168.141.10. kemudian pada "destination name" yang berfungsi memberikan identitas atau nama untuk koneksi VPN di dalam komputer *client*.

Mengisi username client VPN

Selanjutnya adalah pengisian akun *VPN client* yang sebelumnya telah dibuat pada tahap Konfigurasi file */ppp/chap-secrets* pada *VPN server.* Pengisian *username* pada *client* dapat dilihat pada gambar 11.



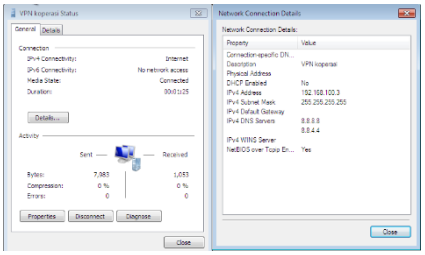
Gambar 11. Pengisian informasi akun *VPN*

Pada gambar 11 penulis menggunakan salah satu akun VPN yang telah dibuat pada tahap Konfigurasi file */ppp/chap-secrets,* yaitu *username :* KBUSB1, dan

password : 1bima293. Kemudian klik "*connect"* dan tinggal menunggu VPN terhubung.

VPN terhubung

Untuk memastikan apakah VPN terhubung atau tidak dapat dilihat pada gambar 12.



Gambar 12. Tampilan status koneksi jaringan

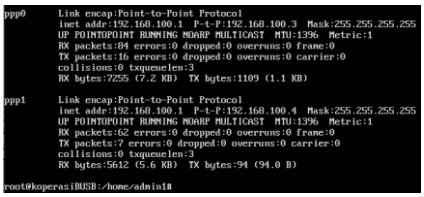
Pada gambar 12 yang merupakan tampilan status dari koneksi *VPN client* dapat dilihat bahwa VPN sudah sukses terhubung dengan IP address 192.168.100.3.

Monitoring

Dalam tahapan monitoring akan dijelaskan berberapa proses yang akan dilakukan untuk monitoring jaringan, dan monitoring inilah tahap dimana akan terlihat keberhasilan atau kegagalan dari tahapan sebelumnya, karena pada monitoring ini penulis maupun admin nantinya akan dapat mengetahui kesalahan atau keberhasil dari jaringan yang telah dibangun. Pada tahapan hasil monitoring ini akan diuraikan dalam 4 tahap yaitu : monitoring VPN *server*, monitoring koneksi *client* pada *server*, dan pengujian *file sharing*.

Monitoring VPN *server*

Monitoring pada server dimaksudkan untuk memantau *client VPN* yang terhubung menggunakan akun VPN yang telah dibuat pada konfigurasi */ppp/chap-secrets.* Gambar 13 berikut ini merupakan tampilan *server VPN* saat memantau *client VPN* yang terhubung menggunakan perintah *ifconfig*.

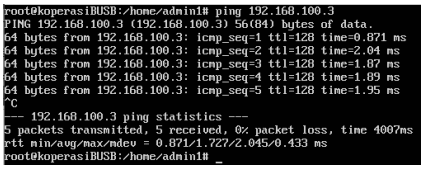


Gambar 13. Hasil monitoring *server*

Pada gambar 13, *"ppp0"* dan *"ppp1"* menandakan adanya 2 akun VPN yang terhubung ke *server.* Pada *"ppp0" address* yang terhubung ke *server* adalah 192.168.100.3, sementara pada *"ppp1" address* yang terhubung adalah 192.168.100.4. *IP client* yang terhubung tersebut berarti sudah sesuai dengan *IP address* pada konfigurasi */pptpd.conf.*

Monitoring Koneksi *client*

Pada monitoring koneksi *client* dijelaskan proses koneksi antara komputer *server* dengan *client* pada satu jaringan yang telah dirancang dan dibangun sebelumnya, gambar 14 dibawah ini merupakan tahapan pengujian antara koneksi admin dengan Client.



Gambar 14. Hasil pengujian *server* ke *client*

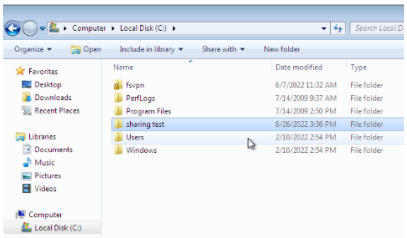
Dari gambar 14 diatas merupakan hasil pengujian kneksi jaringan yang telah berhasil dilakukan oleh *server* kepada *client* melalui satu jaringan dengan *output "64 bytes from 192.168.100.3: icmp_seq=1 TTL=128 time=0.871ms"* dan *output* tersebut menandakan bahwa VPN *server* sudah terhubung dengan *client*.

Pengujian file sharing pada client VPN.

Disini penulis berfokus pada *file sharing* yang merupakan aktifitas membagi dan menyediakan akses data untuk memudahkan pegawai Koperasi BUSB dan UUP Mandiri dalam pengiriman data. Pengujian *file sharing* ini menggunakan dua komputer yang telah terhubung menggunakan VPN.

File sharing pada VPN client 1

Disini penulis membuat sebuah folder baru yang berisi file dokumen untuk pengujian file sharing yang bisa dilihat pada gambar 15.

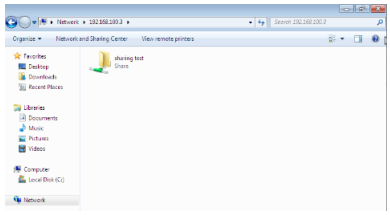


Gambar 15. Tampilan folder yang di *share*

Pada gambar 15 yang merupakan folder yang akan di-*share* oleh penulis kepada *client 2.* Folder tersebut berisi beberapa file dan terdapat di direktori *Local Disk (C:)* dan bernama "*sharing test*".

File sharing pada VPN client 2

Untuk membuka file pada *client 2* yang telah di *share* atau dibagikan oleh *client 1* dapat dilihat pada gambar 16



Gambar 16. Membuka file yang telah di *share*

Gambar 16 merupakan tampilan direktori *network* pada komputer *client 2*. Untuk mengakses file yang telah dikirim oleh client 1, client 2 memasukan alamat *IP VPN* didalam kolom pencarian lokasi folder yaitu \\192.168.100.3. Dapat dilihat bahwa file "sharing test" yang di-*share* oleh *client* 1 dapat tampil dan dapat diakses oleh *client* 2.

Management

Tahap selanjutnya adalah *management* atau pengelolaan. Tahap ini meliputi aktifitas perawatan dan pemeliharan dari keseluruhan sistem yang sudah dibangun. Tahap management ini akan dilakukan setelah sistem berjalan dengan baik. tahap pengelolaan merupakan kewenangan dari pihak Koperasi BUSB, maka penulis hanya terlibat sampai fase sebelumnya yaitu monitoring namun penulis memberikan arahan atau panduan yang terarah langsung kepada pengguna sistem kedepannya, agar mengetahui tentang bagaimana sistem ini dapat digunakan dengan baik sesuai dengan rancangan.

Penulis mengusulkan memonitor konfigurasi jaringan yang dilakukan admin sehingga dampak dari perangkat keras atau pun lunak yang digunakan jaringan Koperasi BUSB dan UUP Mandiri telah terkelola dengan baik. Hal tersebut dilakukan dengan melakukan *backup* konfigurasi, dan *maintenance* atau pemeliharaan sistem secara berkala. Dalam hal keamanan, admin harus memastikan informasi autentifikasi VPN yang tidak dapat diperoleh *client* tanpa izin. Hal tersebut dilakukan dengan cara membuat surat keterangan komitmen dan surat serah terima informasi akun yang berisi *username* dan *password* pada

masing masing *client* yang akan terkoneksi ke jaringan VPN.

KESIMPULAN

Dengan semakin berkembangnya teknologi internet banyaknya peluang untuk mencuri data dan merusak sistem keamanan untuk melakukan gangguan dengan menggunakan teknologi tersebut. Didalam perkembangannya, kebijakan keamanan merupakan langkah kritis dan penanganan yang serius dalam rangka mengamankan sistem jaringan Komputer. Berdasarkan hasil pengamatan pada tahap analisa, implementasi dan pengujian, dapat disimpulkan bahwa hasil penelitian implementasi VPN dengan metode PPTP menggunakan *Linux Ubuntu Server*, sebagai berikut:

1. Untuk membuat server VPN dengan Ubuntu Server 16.04 merupakan pilihan yang sangat baik, karena linux terkenal dengan keandalan dan kestabilan dalam sistem operasi servernya.
2. Teknologi VPN yang dibangun dapat memberikan keamanan dalam komunikasi data melalui jaringan internet serta merupakan solusi yang efisien dan ekonomis.
3. Dengan adanya user VPN yang saling terkoneksi maka tentunya dapat melakukan sharing data secara langsung,
4. Dengan implementasi VPN ini maka penggunaan *internet* akan lebih aman karena *IP address* asli tersamarkan.
5. Dengan menggunakan metode PPTP implementasi VPN di Koperasi BUSB dapat memberikan keamanan dengan adanya enkripsi disetiap komunikasi data serta memberikan *username* dan *password* sebagai pengenal untuk setiap *user*-nya.

Adapun saran yang disampaikan oleh penulis berdasarkan penelitian ini adalah : diharapkan penelitian ini nantinya dapat digunakan sebagai bahan referensi bagi mahasiswa lain yang akan menyusun penelitian berkaitan dengan *Virtual private network (VPN)* dan *linux ubuntu server*

REFERENSI

Harsabat, K. 2014. Rancang Bangun Jaringan Komputer Diskless Berbasis LTSP Dengan Sistem Operasi Linux Ubuntu 14.04 LTS di Laboratorium Teknik Elektro UNNES.*http://lib.unnes.ac.id/20915/.* 28 November 2021 (10:00).

Mufida, E. Irawan, D. dan Chrisnawati, G. 2017. 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* 16(2), h. 9-19.

Oktivasari, P. dan Utomo, A. B. 2016. Analisa Virtual Private Network Menggunakan Openvpn Dan Point To Point Tunneling Protocol. *Jurnal Penelitian Komunikasi dan Opini Publik*, 20(2), h. 185-202.

Watmah, S. W. 2020. Implementasi VPN Menggunakan Point-To-Point Tunneling Protocol (PPTP) Mikrotik Router Pada BPRS Bumi Artha Sampang. *INSANTEK-Jurnal Inovasi dan Sains Teknik Elektro*, 1(1), h. 6-12.