JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -

PENGAMANAN AKSES JARAK JAUH JARINGAN INTERNET RUMAH DENGAN TEKNOLOGI VPN BERBASIS VPS

Domo Pranowo Kuswandono[1], Zaenal Mutaqin[2]

[1] Universitas Bani Saleh, domo@ubs.ac.id
[2]Universitas Bani Saleh, zaenalms@ubs.ac.id

ABSTRAK

Teknologi informasi dan komunikasi data berbasis internet telah berkembang dengan pesat. Akses dan pemanfaatannya berkembang untuk melakukan transfer data tanpa harus memiliki IP public sendiri (dedicated) terhadap server fisik di rumah. Dengan berkembangnya sistem komputasi awan (virtual cloud system) dibutuhkan akses data jarak jauh yang aman. Sedangkan untuk mengakses jaringan yang ada dirumah dibutuhkan IP public. IP Public yang diberikan ISP (Internet Service Provider) kepada pelanggan pribadi biasanya menggunakan IP public dinamic sehingga tidak mudah untuk melakukan akes koneksi yang tetap. Mempertimbangkan hal diatas perlu adanya jalur khusus yang digunakan untuk mengamankan data yang penting atau bersifat pribadi melalui jaringan internet dengan IP public stastis, melalui pemanfaatkan teknologi VPS (virtual Private server) untuk membangun jalur pribadi rumah. Dalam penelitian ini penulis memanfaatkan jenis komunikasi virtual ini memanfaatkan teknologi VPS untuk mendapatkan IP Public statis yang akan digunakan antara perorangan dengan media internet. Dalam tulisan ini akan diulas aspek-aspek implementasi pengendalian sumber daya jaringan rumah dengan akses jarak jauh dengan memanfaatkan Virtual Private Server (VPS), Virtual private network L2TP (VPN) dan router yang ada di komputasi awan, Cloud Hosted Router (CHR) untuk memanfaatkan IP Public static. Sehingga mempermudah mengontrol dan mengatur jaringan sebagai solusi jaringan rumah pintar (smart home) untuk komunikasi jarak jauh yang aman meskipun hanya memiliki IP Public dinamic.
Kata Kunci: Virtual Private Server, CHR, jalur pribadi, VPN

ABSTRACT

Internet-based information and data communication technology has developed rapidly. Access and usefull from between companies, between regions and to housing for private use. With the development of virtual cloud systems, there is need for remote access and secure data access. To access existing networks at home, IP public is required. IP Public is given by ISP (Internet Service Provider) to private customers usually uses IP public dynamic so it is not easy to access with fixed connection. Considering the above, it is necessary to have private network that is used to secure or private data through the internet network with a IP public Fix/ static, through the use of VPS (virtual private server) technology to build a private home (Virtual Private Network). In this study, the authors utilize this type of virtual communication utilizing VPS technology to obtain IP Public static which will be used between individuals on internet media. In this paper will review the implementation aspects of controlling home network resources with remote access by utilizing a Virtual Private Server (VPS), Virtual private network L2TP (VPN) and routers in cloud computing, Cloud Hosted Router (CHR) to take advantage of IP Public static. Making it easier to control and manage the network as a smart home network solution for secure remote communication even though it only has dynamic Public IP.
Keywords: Virtual Private Server, CHR, Private Network, VPN

JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -

PENDAHULUAN

Penggunaan jaringan internet untuk komunikasi data sudah menjadi kebutuhan yang tidak bisa dipisahkan. Yang menjadi isu adalah keamanan data dan keterbatasan IP public yang di miliki oleh pelanggan (pengguna perumahan). ISP (Internet service Provider) untuk pelanggan yang kecil (retail) biasanya IP public yang diberikan bersifat dinamis bukan berupa IP public yang tetap tetapi akan berubah disetiap periode waktu.

Untuk memenuhi factor keamanan data di jalur umum atau internet dibutuhkan solusi enkripsi data. VPN merupakan salah satu teknik untuk membuat terowongan jalur pribadi dan data dienkripsi. L2TP merupakan salah satu teknik protocol VPN, dimana sistemnya bekerja pada OSI 2 (Data Link Layer) sebagai penerima paket data dan pada OSI 5 (Session Layer) sebegai pengamanan paket data yang masuk tersebut. L2TP biasanya digunakan dalam membuat Virtual Private Dial Network (VPDN) yang dapat bekerja membawa semua jenis protokol komunikasi di dalamnya. L2TP memungkinkan penggunanya untuk tetap dapat terkoneksi dengan jaringan lokal milik mereka dengan policy keamanan yang sama dan dari manapun mereka berada, melalui koneksi VPN ataupun VPDN. Koneksi ini sering dianggap sebagai sarana memperpanjang jaringan lokal milik penggunanya, namun memiliki media publik.

Virtual private network (VPN) ini juga berkembang pada saat perusahaan besar memperluas jaringan bisnisnya, namun mereka tetap dapat menghubungkan jaringan lokal (private) antar kantor cabang dengan perusahaan mitra kerjanya yang berada di tempat yang jauh. Perusahaan juga ingin memberikan fasilitas kepada pegawainya (yang memiliki hak akses) yang ingin terhubung ke jaringan lokal milik perusahaan di manapun mereka berada. Perusahaan tersebut perlu suatu jaringan lokal yang jangkauannya luas, tidak bisa diakses oleh sembarang orang, tetapi hanya orang yang memiliki hak akses saja yang dapat terhubung ke jaringan lokal tersebut.

Salah satu perkembangan tekhnologi cloud berbasi IaaS (Infrastructure as a Service) adalah Virtual private server (VPS), teknologi ini merupakan sebuah tipe server yang menggunakan teknologi virtualisasi untuk membagi hardware server fisik menjadi beberapa server virtual yang di hosting di infrastruktur fisik yang sama. Dengan memberikan satu IP public tetap. Di jaman dahulu, sistem administrator secara tradisional hanya memiliki satu server fisik dan hanya digunakan untuk satu tujuan saja. Sementara virtualisasi menawarkan kemudahan untuk meng-host beberapa server pada satu server fisik. Setiap server dapat memiliki tujuan mereka sendiri dan sistem operasi yang berbeda satu sama lain.

Hal ini dapat membantu mengimprovisasi tingkat fleksibilitas yang tersedia pada administrator sistem dalam hal pemilihan konfigurasi software yang dapat mereka jalankan. Selain itu, ini juga dapat memberikan keuntungan yang signifikan dalam hal skalabilitas dari daya pemrosesan (processing power), RAM, dan disk space dengan biaya yang lebih rendah daripada menggunakan hardware fisik tradisional.

Berawal dari masalah diatas penulis memiliki gagasan untuk membuat sebuah perancangan infrastruktur untuk aksesbilitas jaringan intranet yang berada pada private network, dan juga meninjau efektifitasnya dari segi performa yang ada, dengan memanfaatkan teknologi yang ada seperti Virtual Private Server dan Virtual Private Network. Dimana ketika infrastruktur aksesbilitas ini berjalan, maka untuk melakukan koneksi kedalam jaringan intranet tidak perlu lagi hanya dalam 1 ruang lingkup area, namun dari berbagai tempatpun sudah bisa untuk melakukan koneksi tersebut. Tujuan penelitian ini untuk mengetahui bagaimana efektifitas penggunaan VPN yang berjalan pada VPS untuk mendapatkan IP public yang tetap.

JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -

Identifikasi Masalah

Permasalahan yang menjadi perhatian peneliti dalam hal ini berhubungan dengan hal-hal sebagai berikut:

1.Untuk berlangganan koneksi internet ISP pribadi hanya memberikan layanan IP Public Dinamic.
2.Adanya kebutuhan untuk mengakses jaringan lokal/Jaringan rumah dari luar dengan aman.
3. Efektifitas performa transfer dan isu keamanan pada VPN menggunakan VPS.

Rumusan Masalah

Setelah masalah teridentifikasi, selanjutnya penulis merumuskan penelitian yang akan dilakukan, yaitu:

1.Bagaimana membuat infrastuktur jaringan mengatur Routing IP Public untuk mengakses jaringan lokal menggunakan VPN dan VPS.
2. Bagaimana otentifikasi akses client ke VPN dengan menggunakan L2TP/IPSec.
3. Bagaimana performa VPN dengan VPS dengan memanfaatkan Clouding Hosted Routing

Batasan Masalah

Implementasi pengamanan akses jarak jauh dengan memanfaatkan VPS dibatasi hanya pada 3 model yaitu:

1. Akses jaringan rumah dengan simulasi sumber daya FTP server menggunakan jaringan internet Indihome.
2. VPS yang digunakan menggunakan cloud milik provider, untuk mendapatkan IP Public statik untuk Routing dengan MikroTik RouterOS
3. Protokol VPN yang digunakan hanya L2TP/IPSec
4. Pengujian QoS hanya dilakukan di VPN cloud untuk akses FTP

Tujuan Penelitian

Penelitian ini diharapkan menghasilkan rancangan dan membangun infrastruktur jaringan untuk kemudahan akses/koneksi kedalam jaringan lokal (intranet) yang dapat diakses dari luar, dengan pemanfaatan IP publik yang dimiliki VPS sehingga jaringan di rumah bisa diakses penuh dari manapun, dan mendapatkan hasil analisis QoS (Quality of Service) VPN Cloud sehingga bisa di rekomendasikan untuk penerapan kedepannya

TINJAUAN PUSTAKA

Penelitian terkait dengan implementasi telah dilakukan oleh lima pustaka yaitu pustaka pertama berupa tugas akhir yang berjudul“Implementasi VPN Metode IP Security pada PT. Global Terminal Marunda Jakarta”, pustaka kedua berupa tugas akhir yang berjudul “Implementasi Jaringan VPN Dengan Menggunakan Protokol Ethernet Over IP (EoIP) Pada PT. Remala Abadi”, pustaka ketiga berupa tugs akhir yang berjudul “Optimalisasi Manajemen Bandwidth Jaringan Komputer Menggunakan Metode Queue Tree Dan PCQ (Peer Connection Queue)”, pustaka keempat berupa jurnal yang berjudul “Membangun Jaringan Virtual Private Network (VPN) Dengan Metode Tunneling menggunakan MikroTik Untuk Komunikasi Lokal Di Stmik PPKIA Pradnya Paramita Malang “, pustaka kelima berupa jurnal yang berjudul “L2TP/IPsec Interworking”, pustaka keenam berupa jurnal yang berjudul “Virtual Private Server (VPS) Sebagai Alternatif Pengganti Dedicated Server.

JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -

Virtual Private Network (VPN)

Ahmad Habibi Dan Samsul Arifin (2015:116) menjelaskan bahwa VPN (Virtual private network) merupakan suatu cara untuk membuat jaringan bersifat "private" dan aman dengan menggunakan jaringan publik, misalnya internet.VPN (Virtual Private Network) adalah variasi jaringan komputer yang tingaktanya lebih advanced dibandingkan jaringan komputer biasa.

VPN telah dikembangkan menjadi beberapa jenis. Para ahli berbeda pendapat tentang pembagian jenis VPN tersebut. Ada yang membagi VPN berdasarkan cakupan area, yaitu intranet, extranet dan internet. Ada yang membagi VPN berdasarkan jenis protokol yang digunakan, yaitu jenis proteksi data, dan sebagainya. Secara umum VPN dapat dikelompokkan menjadi:

1) Remote Access VPN

Remote access VPN disebut juga Virtual Private Dial-up Network (VPDN). VPDN adalah jenis use-to-LAN connection. Artinya, user dapat melakukan koneksi ke Private Network dari manapun, apabila diperlukan biasanya VPDN dimanfaatkan oleh karyawan komputer laptop yang sudah dilengkapi perangkat tertentu untuk melakukan koneksi dengan jaringan LAN di kantor. Sebelum koneksi terjadi akan dilakukan proses dial-up ke Network Access (NAS). Biasanya NAS disediakan oleh provider yang memberikan komputer dan aplikasi untuk mendial-up NAS. Secara umum VPDN hampir mirip dengan dial-up internet connection. Namun, secara teknis tentu saja VPN lebih canggih dan lebih secure dibandingkan dial-up internet. Koneksi biasanya hanya dilakukan sewaktu-waktu.

2) Site-site VPN

Site-site VPN diimplementasikan dengan memanfaatkan perangkat dedicated yang dihubungkan via internet. Site-to-site VPN digunakan untuk menghubungkan berbagai area yang sudah fixed atau tetap, misal kantor cabang dengan kantor pusat. Koneksi antara lokasi-lokasi tersebut secara terus-menerus (24 jam) sehari.

Jika ditinjau dari segi kendali atau administrative control. Secara umum site-to-site VPN dapat dibagi menjadi:

a) Intranet

Manakala VPN hanya digunakan untuk menghubungkan beberapa lokasi yang masih satu instansi atau satu perusahaan, seperti kantor pusat dihubungkan dengan kantor cabang. Dengan kata lain, administrative control berada sepenuhnya bahwa satu kendali.

b) Extranet

Manakala VPN digunakan untuk menghubungkan beberapa instansi atau perushaan yang berbeda namun di antara mereka memiliki hubungan "dekat". Seperti perusahaan tekstil dengan perusahaan angkutan barang yang digunakan oelh perushaan teksstil tersebut. Dengan kata lain, administrative control berada di bawah kendali beberapa instansi terkait ditulis.

Virtual Private Server (VPS)

Virtual Private Server (VPS) juga dikenal dengan Virtual Dedicated Server (VDS) atau Virtual Server atau Virtual Environment, yaitu suatu teknologi yang memungkinkan sebuah komputer (server) dengan kapasitas resource hardware yang sangat besar dapat dibagi-bagi menjadi beberapa virtual komputer yang mandiri. Virtual komputer tersebut secara fisik tidak terhubung langsung dengan hardware yang digunakan, namun masing-masing antar virtual komputer saling terpisah satu sama lain seperti halnya sebuah

JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -

komputer sungguhan yang memiliki private resource hardware.
Pengguna virtual komputer dapat menginstal sistem operasi (OS) nya sendiri serta dapat mengkustomisasi virtual komputernya tanpa mengganggu virtual komputer yang lain. Pembagian resource ini menggunakan teknologi virtualisasi yang biasa dikenal dengan Virtual Machine (VMWare) pada OS Windows atau Virtual Environment (Virtuozzo) pada OS Linux. Teknologi virtualisasi yang sering dipakai diantaranya, Open Vz, XEN, KVM, Microsoft Hyper-V

Cloud Hosted Router (CHR)

Pada dasarnya fitur ini bukanlah fitur yang terdapat pada menu RouterOS, melainkan sebuah file image yang digunakan di aplikasi VM (Virtual Machine). MikroTik ingin memberikan solusi bagi pengguna RouterOS yang berbasis Virtual Machine. Walaupun bisa dibilang masih sebuah "Test Version", namun memiliki performa yang bagus. Ketika melakukan instalasi pada VM, tentu akan mendapatkan RouterOS dengan Level 0 atau Trial Version selama 24 Jam. Dan untuk bisa menggunakannya lebih lama (Full Functionality) diharuskan membeli lisensi baru dan menambahkannya di RouterOS tersebut. Ada juga yang istilahnya mencari 'jalan pintas' dengan melakukan crack supaya bisa digunakan lebih lama lagi.
Dengan hadirnya Cloud Hosted Router (CHR), kita tidak perlu lagi melakukan hal diatas. Jika meng-install pada VM maka tidak akan melihat lagi ketentuan trial version. MikroTik telah menyertakan sebuah lisensi pada CHR dengan kategori Licence Free. Namun, untuk kecepatan trafik masih dibatasi pada 1Mbit per interface dan CHR ini memiliki base platform PCx86_64, sehingga apabila meng-installnya pada aplikasi VM dimana Host Operating System menggunakan 32 bit maka tidak bisa

FTP Server

File Transfer Protocol atau disingkat FTP adalah suatu protokol yang berfungsi untuk pertukaran file dalam suatu jaringan komputer yang mendukung protokol TCP/IP. Dua hal pokok pada FTP yaitu FTP Server dan FTP Client.
File Transfer Protocol juga merupakan sebuah protokol internet yang berjlaan di dalam level aplikasi yang merupakan standar untuk proses transfer file antar mesin komputer dalam sebuah framework.

Fungsi utama dari FTP adalah melakukan pertukaran file dalam jaringan. Namun, Fungsi FTP Server adalah menjalankan perangkat lunak yang digunakan untuk pertukaran file atau istilah asing file exchange, yang selalu siap memberikan layanan FTP apabila mendapat request atau permintaan dari FTP client. FTP client adalah komputer yang meminta koneksi ke FTP Server untuk tujuan tukar menukar file (upload dan download file).
Fungsi FTP adalah melakukan transfer file antara komputer yang terhubung melalui jaringan, termasuk internet. Dalam bahasa teknis, FTP dikenal sebagai protokol jaringan yang memungkinkan transfer file antara komputer yang tersambung pada TCP/IP yang berbasis jaringan. Hal ini mencakup serangkaian peraturan dan prosedur untuk transfer data digital yang aman. Fungsi FTP lainnya adalah otentikasi dan kesalahan penanganan teknik untuk membangun koneksi antara komputer host dan klien untuk pertukaran data

JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -

METODE PENELITIAN

Dalam pembuatan virtual private network pada virtual private server ini ada beberapa hal atau kegiatan yang dilakukan, perancangan design rancangan jaringan yaitu Membuat rencana topologi awal dari jaringan yang akan diterapkan implementasi sistem VPN berbasis VPS ini, pemilihan bahan dan komponen jaringan, instalasi komponen jaringan, pengujian alat dan penyusunan laporan.

Topologi Jaringan

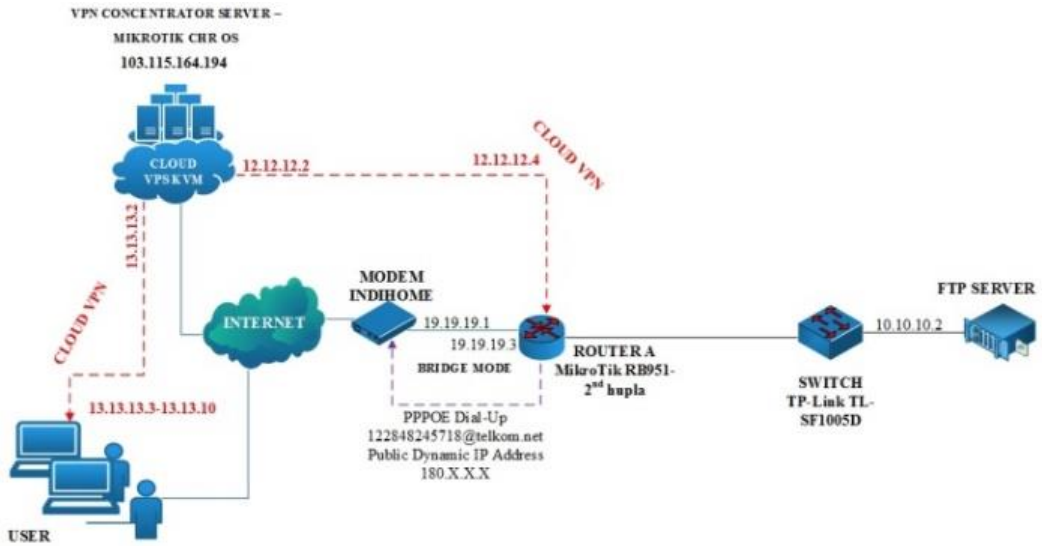
Sebelum melakukan tunneling untuk VPN, tentunya harus menghubungkan router yang ada di VPS, dengan router lainnya yang ada dirumah. Serta menghubungkan router dengan server FTP. Administrator jaringan harus membuat topologi jaringan dengan menggunakan router-router tersebut. Metodologi yang digunakan dalam pengembangan jaringan LAN dengan jaringan ini lebih bersifat teknis, di mana setiap tahapan dilakukan secara berurutan agar pengembangan routing dengan beberapa Router MikroTik dapat dilakukan secara terstruktur. Adapun metodologi yang digunakan antara lain seperti berikut ini:

A. Perangkat Keras

1. VPS KVM (Unmanaged), berperan sebagai tempat Router dengan MikroTik CHR RouterOS.
2. MikroTik RB 951 2nD (hAP-lite), digunakan untuk router lokal yang mempunyai akses langsung ke FTP Server
3. Indihome Modem, berperan sebagai penyedia layanan internet.
4. FTP Server, berperan sebagai server file transfer.

B.Perangkat lunak

Perangkat lunak yang digunakan meliputi sistem operasi dan software yang digunakan untuk router dan file transfer yaitu : FTP Server Windows 7, MikroTik CHR RouterOS, Winbox yang digunakan untuk manajemen router, Wireshark untuk mengukur QoS Jaringan.



Gambar 1. Topologi Jaringan VPS-VPN

JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -

Penjelasan topologi :

1. VPS KVM dalam simulasi perancangan penelitian ini adalah layanan sewa dari provider natanetwork.com, dirubah menjadi VPN Server dengan protokol L2TP/IPSec menggunakan MikroTik CHR RouterOS.
2. Modem Indihome dirubah menjadi bridge mode , kemudian dibuat IP LAN dan terhubung dengan router lokal MikroTik RB951-2nd hupla.
3. Router Lokal MikroTik RB951-2nd hupla melakukan proses dial-up ¬PPPOE untuk mendapatkan IP Publik Dinamik dari Indihome.
4. MikroTik RB951-2nd hupla terhubung dengan VPN Server MikroTik CHR menggunakan layanan L2TP Client
5. Router Lokal MikroTik RB951-2ndn hupla terhubung dengan FTP Server pada jaringan LAN.
6. Pada VPN Server MikroTik CHR, dibuat sebuah routing statik menuju FTP Server agar user dapat mengakses jaringan LAN pada Router Lokal MikroTik RB951-2ndn hupla
7. User dari tempat manapun dapat melakukan dial-up kedalam VPN Server untuk mengakses FTP Server pada jaringan lokal atau sumber daya yang lain yang ada di jaringan lokal rumah.

Perangkat	*Interface*	IP *Address*	*Gateway*	DNS	DDNS
MikroTik CHR RouterOS	Ether 1	103.115.164.194/24	103.115.164.0	8.8.8.8 / 8.8.4.4	-
	L2TP-*routerserver*	12.12.12.2	12.12.12.4		-
	User	13.13.13.2	-	-	-
Indihome Modem GPON	Fiber	*Bridge Mode*	*Bridge Mode*	-	-
	Eth1	19.19.19.1/24	19.19.19.0	-	-
MikroTik RB 951 2nD (hAP-lite)	WAN	19.19.19.3/24	19.19.19.0	-	-
	PPOE *Client* (Indihome Public)	*Dynamic IP*	*Dynamic IP*	-	-
	LAN	10.10.10.1/24	10.10.10.1		-
	L2TP-*routerclient*	12.12.12.4	12.12.12.2		
FTP *Server*	LAN	10.10.10.2	10.10.10.1	8.8.8.8 / 8.8.4.4	-

Tabel 1. Interface dan IP Address Jaringan Penelitian VPN Clouding

Quality Of Service (QoS)

Quality of Service (QoS) adalah kemampuan sebuah jaringan untuk menyediakan layanan yang lebih baik lagi bagi layanan trafik yang melewatinya. QOS merupakan sebuah sistem arsitektur end to end dan bukan merupakan sebuah feature yang dimiliki oleh jaringan. Quality of Service suatu Network merujuk ke tingkat kecepatan dan keandalan penyampaian berbagai jenis beban data di dalam suatu komunikasi. Quality of Service digunakan untuk mengukur tingkat kualitas koneksi jaringan TCP/IP internet atau intranet (Ferguson, P, 1998).Dari definisi diatas dapat disimpulkan QOS (Quality of Service) adalah kemampuan suatu jaringan untuk menyediakan layanan yang baik. Oleh karenanya buruk atau baiknya kualitas dan kemampuan suatu jaringan dapat kita ukur melalui unjuk kerja jaringan tersebut. Beberapa parameter yang dijadikan referensi umum untuk dapat mengukur dan melihat unjuk kerja dari suatu jaringan antara lain, Throughput, Delay, Jitter dan Packet loss. Dengan referensi nilai sebagai berikut (TIPHON, 1999):

JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -

Kategori Throughput	*Throughput (bps)*	*Indeks*
Sangat Bagus	76% - 100%	4
Bagus	51% - 75%	3
Sedang	26% - 50%	2
Jelek	< 25%	1

Tabel 2. Standard Nilai Throughput
Sumber : Jurnal CoreIT, Vol.1, No.2, Desember 2015:68

Kategori Latensi	*Besar Delay (ms)*	*Indeks*
Sangat Bagus	<150ms	4
Bagus	150ms s/d 300ms	3
Sedang	300ms s/d 450ms	2
Jelek	>450ms	1

Tabel 3. Standard Nilai Delay
Sumber : Jurnal CoreIT, Vol.1, No.2, Desember 2015:69

Kategori Degredasi	*Packet loss (%)*	*Jitter (ms)*	*Indeks*
Sangat Bagus	0	0ms	4
Bagus	3	0 s/d 75ms	3
Sedang	15	75ms s/d 125ms	2
Jelek	25	125ms s/d 255ms	1

Tabel 4. Standard Nilai Packet loss and Jitter
Sumber : Jurnal CoreIT, Vol.1, No.2, Desember 2015:69

Implementasi Jaringan

Setelah perancangan jaringan sesuai topologi diatas, dilakukan implementasi serta pengujian QoS terhadap sistem VPN yang dibangun.

Cloud VPN

Instalasi MikroTik Cloud Hosted Router (CHR)

Tahap satu, Setelah regristasi di provider VPS KVM selanjutnya adalah dengan meng-install MikroTik Cloud Hosted Router (CHR) pada virtual mesin yang ada di cloud VPS KVM yang telah dimiliki.

Jendela c-panel (Control Panel) akan disediakan provider VPS untuk melakukan intevensi OS di VPS KVM yang secara default adalah dengan OS Ubuntu server.

VPS KVM ini akan memberikan informasi IP public yang didapat. Yang nantinya akan digunakan oleh OSrouter MikroTik sebagai inti akses jaringan.

IP Public statis yang diperoleh dari provider yang menyediakan layanan VPS tersebut adalah 103.115.164.194 (sesuai gambar 1. dan tabel 1.) beserta user dan password dari provider.

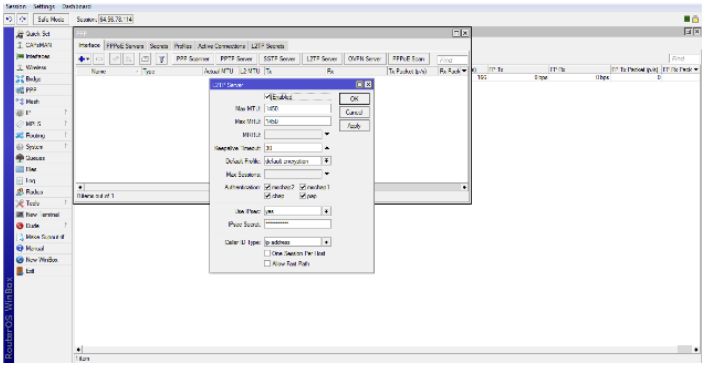
Cloud Hosted Network (CHR)

JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -

Konfigurasi CHR menggunakan port SSH dengan software PuTTy mengarah ke IP Publik dan User name, password diatas, untuk merubah setting di VPS KVM dari OS default linux ke MikroTik CHR RouterOS.
Dengan memanfaat koneksi dengan google drive, untuk mengambil sumber installer RouterOS tersebut.
Berikut Script command yang dijalankan setelah masuk ke VPS server dengan PuTTy.

```
wget https://goo.gl/XhzESA -O chr.img.zip  && \
gunzip -c chr.img.zip > chr.img  && \
mount -o loop,offset=33554944 chr.img /mnt && \
ADDRESS=`ip addr show eth0 | grep global | cut -d' ' -f 6 | head -n 1` && \
GATEWAY=`ip route list | grep default | cut -d' ' -f 3` && \
echo "/ip address add address=$ADDRESS interface=[/interface ethernet find
where name=ether1]
/ip route add gateway=$GATEWAY
 " > /mnt/rw/autorun.scr && \
umount /mnt && \
echo u > /proc/sysrq-trigger && \
dd if=chr.img bs=1024 of=/dev/vda
```

Setelah MikroTik RouterOS CHR terinstall di VPS selanjutnya adalah instalasi Virtual private network (VPN) Concentrator. VPN yang akan implementasi adalah VPN yang menggunakan service Layer Two Tunneling Protocol (L2TP) dengan protokol enkripsi data IP Security (IPSec). Dan pengaktifan protokol IPsec pada menu Use IPsec ubah pengaturan menjadi “yes”, kemudian pada kolom IPsec Secret penulis memberikan kata kunci “password2024” sebagai identitas akses kedalam L2TP Server yang penulis buat.



Gambar 2.
Tampilan Service L2TP Server Setelah Di Konfigurasi

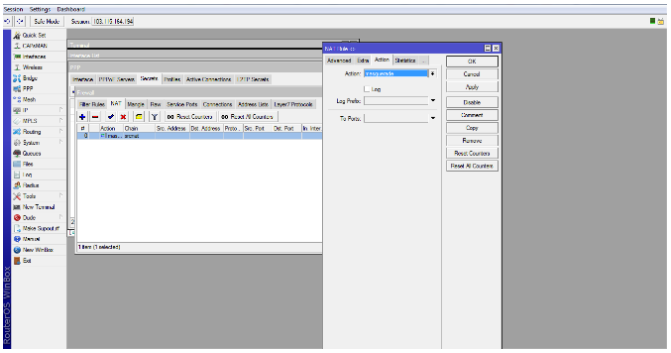
Kemudian kembali lagi pada interface PPP, selanjutnya penulis membuat dua buah user, user pertama penulis gunakan untuk menghubungkan antara MikroTik CHR degan router lokal, sedangkan user kedua penulis gunakan untuk client yang akan mengakses VPN nantinya. Masuk pada tab secrets kemudian buat profile baru, pada tab name penulis isi “routerlocal”, tab name ini yang nantinya berfungsi sebagai username saat akan melakukan dial-up kedalam VPN.

JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -

Kemudian pada tab password penulis isi dengan “1234567890”, pada tab profile biarkan berisi “default”, pada tab local Address penulis isi dengan IP Address “12.12.12.2”. Local Address ini yang nantinya berfungsi sebagai IP VPN lokal yang berada pada MikroTik CHR, lalu pada remote Address penulis isi dengan IP Address “12.12.12.4”. Remote Address ini yang nantinya berfungsi sebagai IP VPN client yang didapatkan oleh router lokal.

Untuk profile kedua, profile ini akan digunakan untuk user yang akan mengakses VPN. membuat IP pool terlebih dahulu, IP pool ini yang nantinya akan di dapatkan ketika user sukses mengakses VPN. 8 range IP Address dari 13.13.13.3 – 13.13.13.10, yang artinya hanya 8 user yang dapat mengakses VPN nanti. local Address ini yang nantinya berfungsi sebagai IP VPN lokal yang berada pada MikroTik CHR. Pada tab Remote Address penulis menggunakan profile IP pool. Pada tahap terakhir konfigurasi VPN server adalah membuat Network Address translation (nat) dengan sebuah action “masquerade”. Nat ini digunakan agar IP Address Private bisa terhubung kedaam jaringan internet.

Gambar 3.

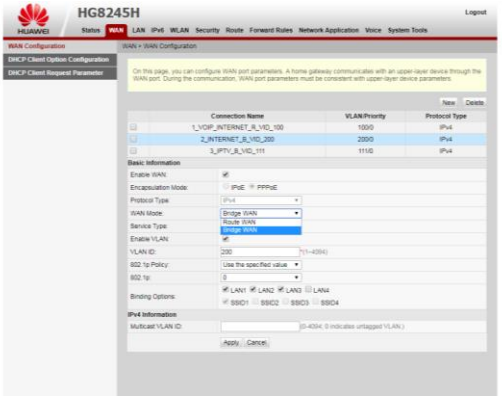


Konfigurasi NAT VPN server

Konfigurasi IP Public Pada MikroTik

Pada tahap kedua implementasi ini adalah mendapatkan IP public milik penyedia layanan internet langsung dari MikroTik. MikroTik harus mendapatkan IP public tersebut secara langsung.

Solusinya adalah dengan melakukan dial Point-to-Point Pro



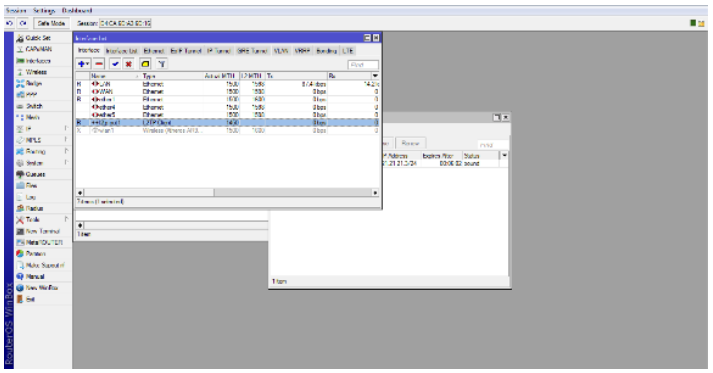
Gambar 4. Konfigurasi Mode Bridge Router Indihome

JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -

Protocol Over Ethernet (PPPOE) bukan dari router milik penyedia layanan internet, melainkan langsung dari MikroTik. Konfigurasi yang dilakukan adalah membuat router milik penyedia layanan internet menjadi bridge, melakukan dial PPPOE pada mikrotik. Setelah dial berhasil maka IP Public akan didapatkan langsung pada MikroTik

Mengkoneksikan Router Lokal ke VPN Server MikroTik CHR

Pada tahap ketiga implementasi adalah mengkoneksikan perangkat lokal meuju MikroTik CHR, perangkat lokal yang penulis maksud adalah Router MikroTik RB 951-2nd hupla. Router ini akan berfungsi sebagai VPN client yang nantinya akan terhubung dengan VPN server Mikrotik CHR, disamping itu router lokal ini yang memiliki akses langsung meunju FTP Server. Selanjutnya membuat koneksi dari router lokal menuju MikroTik CHR menggunakan VPN client. Sama seperti membuat VPN server , masuk kedalam sub menu PPP kemudian pilih button new, lalu pilih service VPN L2TP Client. Lalu pada interface L2TP Client , pada menu General di tab name penulis beri nama VPN Client, kemudian masuk kedalam menu Dial Out. Pada tab Connect To masukkan IP Address milik VPN Server di MikroTik CHR, pada tab user masukkan username yang sudah dibuat pada MikroTIk CHR.



Gambar 5. VPN Client Service Running

Koneksi Client ke VPN Server MikroTik CHR

Pada tahap keempat adalah mengkoneksikan client atau user kedalam VPN, client atau user yang digunakan untuk penelitian ini menggunakan windows 7. Masukkan IP Address milik VPN Server MikroTik CHR yaitu “103.115.164.194”, masukkan username dan password untuk login kedalam VPN, untuk username yang penulis gunakan adalah “client” dan untuk password. Lalu pilih profile VPN Cloud Setelah interface properties terbuka lalu pilih tab security, pada tab type of VPN ubah menjadi Layer Two Tunneling Protocol with IPSec (L2TP/IPSec). Masukkan used preshared key for authentification dan penulis memasukkan kata kunci IPsec yang penulis buat pada L2TP Server di MikroTik CHR sebelumnya. dial-up pada profile VPN yang telah di buat, masukkan username dan password kemudian terjadi koneksi (connected). Jika berhasil IP address VPN client akan terbentuk

Membuat Routing Menuju FTP Server

Pada tahap kelima implementasi adalah membuat static routing menuju ke FTP Server. Buka menu route list, penulis menambahkan route baru. Pada interface new route , dalam tab general pada bagian Dest.Address penulis isi dengan IP FTP Server yaitu”10.10.10.2”, gateway penulis isi dengan IP VPN client milik router lokal yaitu “12.12.12.4”, karna saat

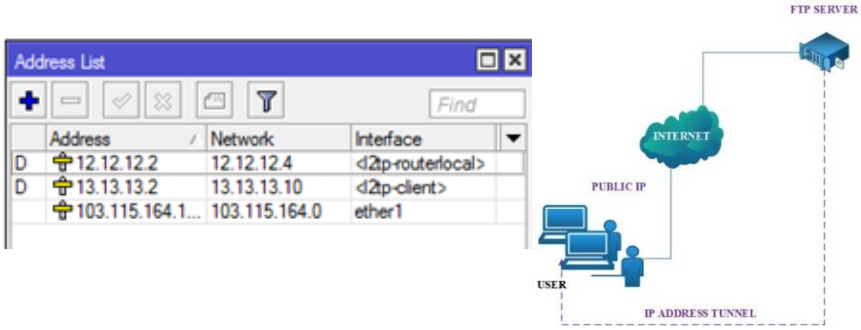
JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -

menuju FTP Server terlebih dahulu melewati router lokal yang menjadi sebuah gerbang. Instalasi FTP Server. Disini penulis menggunakan XAMPP dan FileZilla sebagai FTP Server nantinya. Seperti biasa setelah XAMPP ter-install, kemudian start pada service FileZilla yang ada pada control Panel XAMPP. Setelah service FileZilla berjalan,kemudian setting FTP Server pada menu admin, untuk server Address penulis tetap menggunakan IP Address localhost yaitu "127.0.0.1" dan untuk portnya penulis tetap menggunakan port stadard milik FileZilla yaitu "14147".

HASIL DAN PEMBAHASAN

Otentifikasi Client

Pada saat *client* terkoneksi kedalam VPN, yang terjadi adalah *client* tidak hanya memiliki 1 buah *IP Address,* tapi terbentuk interface baru juga mendapatkan sebuah IP *Address tunneling VPN* yang berfungsi untuk menjangkau jaringan lokal (FTP Server)



Gambar 6. Otentifikasi *Client* Pada VPN

Analisis Paket

Dengan menggunakan aplikasi *Network* analyzer wireshark, dapat men-capture segala aktivitas lalu lintas yang terjadi pada sebuah jaringan komputer saat memulai *browsing* ke sebuah alamat *Uniform Resource Locator* (URL) di internet hingga mendapatkan halaman yang diinginkan.

Metode pengambilan data sampelnya yaitu :

Perhitungan *Request Time* dan *Respawn Time* pada paket *download* dan *upload.*

Perhitungan jumlah paket keseluruhan, jumlah waktu keseluruhan dan jumlah paket keseluruhan dalam bytes.

Pengujian *Download* dan *Upload* dilakukan menggunakan *VPN Cloud*

Sampel data dibatasi hanya dari 5 buah file.

Perhitungan *Delay*, *Packet loss*, *Jitter*, *Throughput*.

Percobaan Download Dan Upload Dengan VPN Clouding

Proses percobaan dilakukan lima kali. Dengan ukuran file yang berbeda.

Nama File	Type File	Size
File A	PDF	747 KB
File B	ZIP	1019 KB
File C	JPEG	1826 KB
File D	XLS	3208 KB
File E	MP3	5125 KB

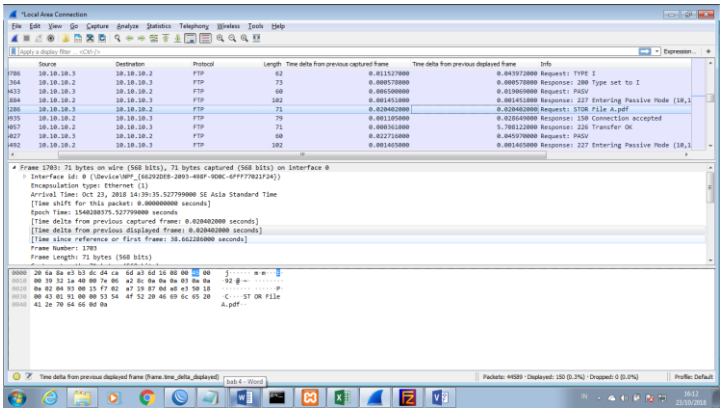
Tabel 5. Besar file yang diupload dan download

Percobaan *upload* dan file melalui *VPN Cloud* terlihat transfer data dari *client* "10.10.10.3" ke *server* "10.10.10.2", dengan pesan "STOR" yang merupakan pesan request dari *client* ke *server* yang berarti meminta *server* untuk menerima dan menyimpan data dari *client* (*upload* File A). *Server* akan membalas dengan response pesan kode 150

JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -

(status file oke, koneksi data akan dilakukan). dan pesan kode 226 Transfer OK berarti (transfer file sukses). File tersebut dikirimkan dari port 1171 menuju port 21.

Percobaan *download* file melalui *VPN Cloud* t terlihat transfer data dari *server* "10.10.10.2" ke *client* "10.10.10.3", dengan pesan "RETR" yang merupakan pesan request dari *client* ke *server* yang berarti meminta *server* untuk mengirim copy data yang berada pada direktori *FTP Server* (*download* File A). *Server* akan membalas dengan response pesan kode 150 (status file oke, koneksi data akan dilakukan). dan pesan kode 226 Transfer OK berarti (transfer file sukses). File tersebut dikirimkan dari port 21 menuju port 1171.

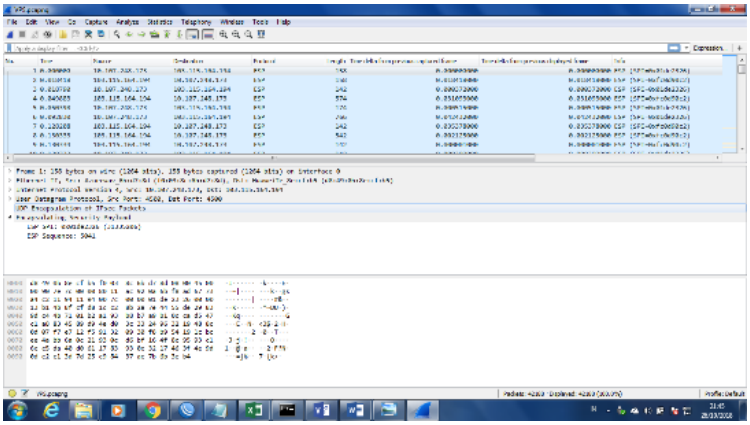


Gambar 7. *Capture Process Upload File* Menggunakan VPN *Cloud*

Keamanan Pada User

Keamanan yang didapat ketika *user* menggunakan IPSec , seluruh informasi paket yang keluar dan masuk di enkripsi, yang artinya paket-paket data tersebut tidak bisa di *sniff* oleh orang lain. Dapat dilihat pada gambar 4.70 saat *user* menggunakan VPN *cloud.* terlihat pada aplikasi wireshark, protokol yang terbaca adalah protokol ESP (*Encapsulating Security Payload*) . Disitu membuktikan bahwa penerapan IPSec pada VPN berjenis L2TP ini sangatlah baik

JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -



Gambar 8. Enkripsi Pada *User* Yang Menggunakan VPN *Cloud*

Hasil Pengujian Upload dan Download dengan VPN Cloud

Dari *capture* data yang telah dilakukan pada wireshark maka didapatkan beberapa hasil dari point-point berikut ini :

Request Time* dan *Respawn Time

Nama File	Transfer File			
	Request Time		Respawn Time	
	VPN Upload	VPN Download	VPN Upload	VPN Download
File A	63,69	230,21	69,93	242,82
File B	70,48	242,41	79,69	253,18
File C	80,51	254,53	98,10	272,55
File D	98,94	272,90	130,66	304,77
File E	131,41	305,44	183,40	357,43
Rata-Rata	89,01	261,10	112,36	286,15

TABEL 6. *Timming Moment Request* Dan *Respawn Time* Pada Pada Percobaan *Download* Menggunakan VPN *Cloud*

Packet loss

$$Packet\ loss = \frac{\text{(Paket data dikirim - Paket data diterima) x 100 \%}}{\text{Paket data yang dikirim}}$$

Nama File	Packet Loss (%)	
	VPN Cloud Upload	VPN Cloud Download
File A	8,92	5,19
File B	11,56	4,25
File C	17,93	6,61
File D	24,28	10,46
File E	28,35	14,55
Rata-Rata	18,208	8,212

Tabel 7. Hasil *Packet loss Upload* Dan *Download* Dengan VPN *Cloud*

Delay

$$Delay = \frac{\text{Packet Length}}{\text{Link Bandwith}}$$

Rata-Rata Delay Keseluruhan Paket				
Source	Jumlah Delay Keseluruhan	Jumlah Paket Keseluruhan	Rata-Rata Delay Keseluruhan	Satuan
VPN Cloud	48,40	11.925	4,06	msec

JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -

Tabel 8. Hasil Rata-Rata upload dan download *Delay* Keseluruhan Paket

Throughput

$$Throughput = \frac{\text{Paket data diterima}}{\text{Lama Pengamatan}}$$

Throughput				
Source	Jumlah Paket Keseluruhan Dalam bytes/s	Jumlah Delay Keseluruhan	Throughput Yang Didapat	Satuan
VPN Cloud	11.925.000	48,40	246384.29	bps

Tabel 9. Hasil Rata-Rata upload dan download Throughput Keseluruhan Paket

Jitter

$$Jitter = \frac{\text{Total variasi } delay}{\text{Total paket yang diterima}}$$

Jitter			
Source	Upload	Download	Satuan
VPN Cloud	0,96	0,90	msec

Tabel 10. Hasil *Jitter Upload* Dan *Download* Dengan Menggunakan VPN *Cloud*

Berdasarkan hasil yang diperoleh dari percobaan yang telah dilakukan. Untuk nilai rata-rata *Packet loss* sendiri untuk percobaan pada *VPN Cloud*, untuk *upload* sendiri memiliki persentase 18.21%, dan untuk *download* memiliki persentase 8.21%. Pada tabel *Packet loss* nilai *upload* milik *VPN Cloud* adalah sedang, dan untuk nilai *download* milik *VPN Cloud* adalah bagus (TIPHON,1999).
Untuk nilai rata-rata *Delay* pada percobaan yang menggunakan *VPN Cloud* adalah 4.06 msec. Pada tabel *Delay* masing masing nilai baik (TIPHON, 1999)
Lalu untuk nilai rata-rata *Throughput* pada percobaan yang menggunakan *VPN Cloud* adalah 246.384,29 bps. Pada tabel *througput* keduanya memiliki nilai dengan kategori Sangat bagus, jadi untuk kualiatas jaringan dalam pengiriman data dapat dikatakan sudah baik.

Sedangkan untuk nilai rata-rata *Jitter* pada percobaan *VPN Cloud*, untuk *upload* sendiri memiliki nilai 0.96 msec, dan untuk *donwload* memiliki nilai 0.90 msec. Pada tabel *Jitter* nilai-nilai yang didapatkan ini semuanya masuk pada kategori sangat bagus (TIPHON, 1999).
Dari data diatas, efektifitas *VPN Cloud* layak untuk digunakan dan diterapkan, hanya saja pada beberapa point seperti kecepatan internet yang digunakan harus diperhatikan kembali karna untuk meminimalisir dampak pada QoS yang terjadi nantinya

PENUTUP

Simpulan

Berdasarkan dari analisis design implementasi dan pengujian pengamanan akses jarak jauh ini disimpulkan Sebagai berikut:

1. Pembuatan infrastruktur jaringan agar dapat mengakses jarigan lokal atau jaringan rumah dengan menggunakan VPN melalui VPS dapat dilakukan dengan membuat sebuah cloud router pada VPS, dimana nantinya cloud router CHR yang berfungsi sebagai VPN server.
2. Kekurangan berlangganan internet di rumah yang hanya memperoleh IP Public dinamik, bisa diselesaikan dengan memakai IP public statik yang diperoleh di VPS,

JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -

sehingga akses jarak jauh bisa dilakukan kapanpun dan dimanapun dengan menggunakan satu IP publik yang statis.

3. Otentifikasi akses client kedalam VPN dengan menggunakan L2TP/IPSec dengan memasukkan username dan password yang terdaftar pada VPN server berjalan dengan pengamanan IPSec. client sukses terhubung kedalam jaringan VPN maka client akan mendapat sebuah IP Address lokal milik VPN server, dan data akses akan aman karena data yang ditansmisikan dienkripsi.
4. performa pada VPN Cloud dari pemeter (TIPHON,1999) timming moment, packet loss, delay, throughtput dan jitter. ujicoba pada masing-masing VPN menuju FTP server. Dari hasil ujicoba tersebut dapat diketahui bahwa VPN Cloud ini sudah cukup baik dalam segi performa Paket loss download 8.21% bagus, Delay 4.06 msec bagus, throughput 246 Kbps sangat vagus dan Jitter 0.90 msec bagus sekali. VPN Cloud ini dapat menjadi solusi ketika tidak memiliki sebuah IP Public Static

SARAN

Design pengamanan akses jarak jauh ini. Ada beberapa saran yang dapat dikemukakan dari hasil penelitian ini antara lain:

1. Perlu dibandingkan unjuk kerja metode akses dengan VPN ini atara metode direct VPN dan Cloud, sehingga bisa mengetahui performa dari teknologi yang diterapkan dalam pengamanan akses jarak jauh dengan aman.
2. Akses Jarak jauh bisa diterapkan untuk mengontrol semua peralatan (device) berbasis IP yang berada dirumah. Sehingga dimanapun lokasi bisa melakukan akses Kontrol penuh (Full Access Control). Dalam waktu 24 jams sehingga perlu pelajari perangkat yang handal.
3. Karena keterbatasan IP Publik statis, maka yang hanya memiliki IP Publik dinamik bisa menggunakan Teknologi DDNS bisa menjadi salah satu solusi utk mengunakan jaringan pribadi VPN.
4. Pengujian keamanan sistem terhadap serangan membanjiri paket data (flooding) dalam jaringan VPN perlu diantisipasi

REFERENSI

Ahmad Imanudin. 2018. *Virtualisasi server bebasis PROMOX*. Excellent Publising

Davide Gatti. 2014. *VPS Toolkit Ubuntu Server LTS*. DeewHY London

Athailah. 2013. *Mikrotik Untuk Pemula*. Mediakita TransMedia

Anne Hemni, Mark Lucas. 2006. *Firewall Policies and VPN Configuration*, Syngress Publising, Inc. Rockland

Ferguson, P., & Huston, G.1998. *Quality Of Service*, John Wiley & sons Inc

Ikandar, Iwan dan Alvinur Hidayat. *Analisa Quality of Service (QoS) Jaringan Internet Kampus (Studi Kasus : UIN Suska Riau).* Riau : Jurnal CoreIT. Vol 1. No 2 : 67 – 76, 2015

Kustanto & Daniel T Saputro. 2015. Belajar Jaringan Komputer Berbasis Mikrotik OS. Gava Media : Yogyakarta

JURNAL TRIDI
Teknologi Informatika & Komputer
Vol. 2 No. 1 Bulan 2024
Universitas Bani Saleh FTID
P-ISSN: - , E-ISSN: -

Miguel Barreiros and Peter. 2010. *QoS Enabled Network: Tools and Foundations*, John Wiley & sons Inc

Tiphon. 1999. *Telecommunication Internet Protocol Harmonization Over Network (TIPHON) General aspecs of Quality Of Service*

Wicaksana, M. R. (2022). *Perancangan Virtual Private Network Layer 2Tunneling Protocol (L2TP) Berbasis Mikrotik*. Journal of Network and Computer , 24-36.