Implementasi Virtual Private Network Openstack Terkoneksi Dengan Virtual Private Network Mikrotik Untuk Komunikasi Data Lebih Aman

Cholifah Sulistin Angraeni[1], Hary Nugroho[2], Ega Dian Pramesta[3]
[1,2]Akademi Teknik Telekomunikasi Sandhy Putra Jakarta
cholifah.sulis96@gmail.com[1], harynug@gmail.com[2],26ega.dian@gmail.com [3]

ABSTRAK

OpenStack adalah sistem operasi *cloud computing* yang bersifat *open source*, yang mendukung semua jenis *cloud environments*. sebagian besar Openstack digunakan pada IAAS (*infrastructure as a services).* Sub projek pada Openstack memiliki tugas masing-masing yang saling terintegrasi seperti mengelola sumber daya *network* yang bertugas untuk mengatur jaringan pada Openstack, kemudian akan memastikan setiap komponen dari penyebaran Openstack dapat berkomunikasi satu sama lain. Openstack *networking* memungkinkan *tenant* untuk dapat membuat topologi *virtual networking* dan layanan seperti VPN. Pada penelitian ini penulis menerapkan sistem VPN (*Virtual Private Network*) untuk mempermudah komunikasi melalui jaringan publik, dan terkoneksi dengan jaringan lokal (LAN). VPN dapat terjadi antara dua PC atau lebih dengan menggunakan jaringan yang berbeda. Sistem operasi perangkat lunak yang dapat digunakan untuk menjadikan PC sebagai *router network* yaitu MikroTik yang memiliki keamanan jaringan IPSec *(Internet Protocol Security)*. VPN dapat dibentuk dengan menggunakan teknologi *tunneling* dan enkripsi. Penggunaan enkripsi dalam teknologi VPN, jaringan VPN tidak dapat dibaca oleh pihak-pihak yang tidak berkepentingan karena melewati proses dekripsi terlebih dahulu. Hasil yang di dapat dari penelitian ini yaitu nilai *Bandwidth* yang dihasilkan pada saat melakukan *Upload File* memiliki hasil 0,267 Mbit/sec dan untuk hasil *Download File* bernilai *0,162 Mbit/sec.* Sedangkan untuk hasil *Packet Loss* pada saat melakukan *Upload File* memiliki hasil yang bagus yaitu 0%, dan untuk nilai yang didapat pada saat men*download* yaitu 0%. Menurut standar TIPHON dan ITU-T nilai-nilai *Packet Loss* yang didapat memenuhi standar kategori degredasi, nilai yang sangat bagus adalah 0%, untuk kategori bagus memiliki nilai 3%, pada katagori sedang memiliki nilai 15%, dan untuk kategori jelek memilki nilai 25%.

Kata kunci: Openstack, VPN, MikroTik

ABSTRACT

OpenStack is an open source cloud computing operating system, which supports all types of cloud environments. Most Openstacks are used on IAAS (infrastructure as a services). Sub projects on Openstack have their own integrated tasks such as managing network resources tasked with managing the network on Openstack, then ensuring every component of the OpenStack deployment can communicate with each other. Openstack networking allows tenants to create virtual networking topologies and services such as VPNs. In this final project the authors implement a VPN system (Virtual Private Network) to facilitate communication through public networks, and connected to the local area network (LAN). VPNs can occur between two or more PCs using different networks. Operating system software that can be used to make the PC as a network router that is MikroTik which has IPSec network security (Internet Protocol Security). VPNs can be established using tunneling and encryption technologies. Using encryption in VPN technology, so that VPN networks can not be read by unauthorized parties because they go through the decryption process first. The results obtained from this study that the value of Bandwidth generated at the time of Upload File has a result of 0.267 Mbit / sec and for the results Download File is worth 0.162 Mbit / sec. While for the results of Packet Loss at the time of Upload File has a good result that is 0%, and for the value obtained at the time of download is 0%. According to TIPHON and ITU-T standards the values of Packet Loss obtained meet the standard of degredation categories, a very good value is 0%, for the good category has a value of 3%, the category has a value of 15%, and for the bad category has a value of 25%.

Keywords: Openstack, VPN, MikroTik

I. PENDAHULUAN

A. Latar belakang

Seiring kemajuan teknologi informasi dan komunikasi khususnya internet benar-benar berdampak pada aktivitas di perusahaan, pemerintahan, atau instansi lainnya dalam berinteraksi dengan karyawan, kantor cabang maupun konsumen melalui jaringan komputer. Aktivitas tersebut tentu saja dapat beresiko apabila informasi yang penting dan berharga dapat diakses oleh pihak lain.

Dijaringan komputer keamanan ketika mengirim dan menerima data sangat penting untuk menjamin bahwa data yang dikirim sampai pada pihak yang dituju, dan tidak jatuh pada pihak lain, yang bersifat rahasia. Maka dari itu perlu dilakukan pengamanan data pada jaringan karena banyak orang yang berusaha untuk mengakses atau menyadap data-data tersebut.

Salah satu solusi kerahasiaan data tetap aman adalah melakukan transaksi data melalui jaringan yang dibuat seolah-olah merupakan jaringan *private* oleh karena itu penulis membuat "Implementasi Virtual Private Network Openstack Terkoneksi Dengan Virtual Private Network Mikrotik Untuk Komunikasi Data Lebih Aman" yang merupakan alternatif untuk mengirim data, yang bersifat *private* dan aman, dengan menggunakan VPN kita dapat dengan mudah mengakses dan mengirim data menggunakan komputer dirumah ataupun diluar jaringan kantor kapanpun selama masih terhubung dengan jaringan internet.

B. Tujuan Penelitian

Tujuan penulisan Proyek Akhir ini adalah:

1) Membuat model implementasi *Virtual Private Network* pada OpenStack
2) Mengimplementasikan Virtual Private Network yang terkoneksi dengan Virtual Private Network MikroTik yang aman bagi pengguna jaringan Virtual Private Network
3) Menganalisa dua jaringan VPN dengan teknologi VPNAAS yang ada di sistem cloud dan VPN yang ada pada router, dalam hal ini penulis menggunakan router MikroTik.
4) Membangun koneksi Virtual Private Network dengan konsep IPSec.

C. Rumusan Masalah

1) Bagaimana cara membuat media komunikasi yang dapat mempermudah kinerja, dan menghemat waktu dan biaya.
2) Bagaimana mengetahui parameter-parameter pengukuran VPN yang menghubungkan antar pengguna jarak jauh.
3) Bagaimana meningkatkan keamanan komunikasi pada jaringan VPN.

D. Batasan Masalah

1) Parameter analisa yang akan digunakan adalah Bandwidth, Packet Loss, dan Encryption.
2) Sistem jaringan komunikasi yang dibuat hanya pada Virtual Private Network.
3) Membahas teori tentang jaringan VPN OpenStack yang terkoneksi dengan VPN MikroTik.
4) Dalam membangun Cloud Computing menggunakan platform OpenStack.

II. DASAR TEORI

A. Cloud Computing

Sejarah TCP/IP (Transmission Control Protocol/Internet Protocol) dimulainya dari lahirnya ARPANET (Advanced Research Project Agency Network) yaitu jaringan paket switching digital yang didanai oleh DARPA (Defence Advanced Research Projects Agency) pada tahun 1969. Sementara itu ARPANET terus bertambah besar sehingga protokol yang digunakan pada waktu itu tidak mampu lagi menampung jumlah node yang semakin banyak. Oleh karena itu DARPA menandai pembuatan protokol komunikasi yang lebih umum, yakni TCP/IP, ia diangkat menjadi standar ARPNET pada tahun 1983. Untuk memudahkan konversi, DARPA juga menandai suatu proyek yang mengimplementasikan protokol ini kedalam BSD UNIX, sehingga internet digunakan untuk menunjukan jaringan yang menggunakan jaringan protokol (IP) tapi dengan semakin berkembangnya jaringan, istilah ini sekarang sudah berupa istilah genetik yang dipakai untuk semua kelas jaringan. Internet digunakan untuk menunjukan pada komunitas jaringan komputer worldwide yang saling dihubungkan dengan protokol TCP/IP. Ciri-ciri yang terdapat pada protokol itu sendiri yang merupakan keunggulan dari TCP/IP yaitu:[2]

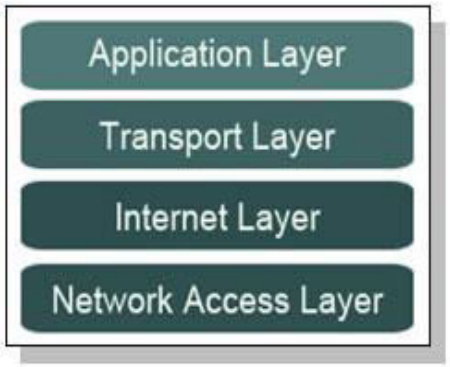
a. Perkembangan protokol TCP/IP menggunakan standar protokol terbuka sehingga tersedia secara luas. Semua orang bisa menggunakan perangkat lunak untuk dapat berkomunikasi menggunakan protokol.[2]
b. Tidak tergantung pada perangkat keras atau sistem jaringan tertentu.[2]
c. TCP/IP memiliki fasilitas routing dan jenis-jenis layanan lainnya yang memungkinkan diterapkan pada internetwork.[2]

- **TCP/IP**

TCP/IP (Transmission Control Protocol/Internet Protocol) adalah standar komunikasi data yang digunakan oleh internet dalam proses tukar-menukar data dari komputer ke komputer lain di dalam jaringan internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (protocol suite). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan kedalam bentuk perangkat lunak (software) disistem operasi. Istilah yang diberikan perangkat lunak ini adalah TCP/IP stack.[11]

- **Lapisan Layer TCP/IP**

Berikut ini adalah lapisan yang terdapat pada TCP/IP meliputi [5]:



Gambar 2.1 Lapisan Layer TCP/IP [5]

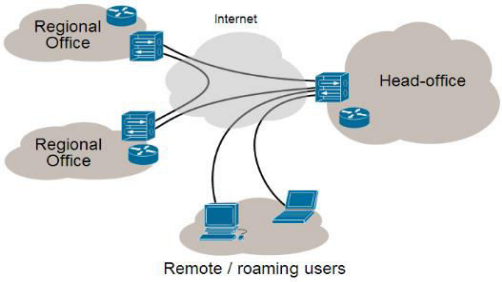
a) Network Access Layer. Fungsi Network Access Layer adalah mengubah IP datagram ke dalam frame yang ditansmisikan oleh jaringan dan memetakan IP Address alamat fisik yang digunakan dalam jaringan.[5]

b) Internet Layer, menyedikan layanan pengiriman paket dasar pada jaringan tempat jaringan TCP/IP dibangun. Seluruh protokol diatas dan dibawah Internet Layer menggunakan Internet Protocol untuk mengirimkan data. Semua data TCP/IP mengalir melalui IP, baik data yang akan masuk maupun yang akan keluar. Internet Layer bertanggung-jawab dalam proses pengiriman paket ke alamat yang tepat.[5]
c) Transport Layer, terdapat dua utama yaitu Transmission Control Protocol (TCP) dan User Datagram Protocol (UPDP) kedua protokol ini mengirimkan paket data diantara Application Layer dan Internet Layer.[5]
d) Application Layer. Pada bagian teratas arsitektur protocol TCP/IP terdapat lapisan Application Layer, seluruh pross di dalam layer ini telah menggunakan Transport Layer untuk mengirimkan paket data dan mencangkup semua proses dalam pengiriman paket data.[5]

B. VPN

VPN (*Virtual Private Network*) merupakan saluran pribadi yang dibuat dalam sebuah koneksi *public* yang difungsikan untuk akses yang aman, baik itu antar satu *site* lainnya, maupun antar *workstation* dengan *site* [1].

VPN dibuat dengan menggunakan jalur *public* seperti internet, dimana kita membuat VPN seperti membangun sebuah *tunnel* (terowongan) dalam area akses internet secara umum, dan *tunnel* (terowongan) tersebut hanya boleh digunakan oleh orang-orang yang sudah kita tentukan, sehingga aktivitas jaringan yang kita lakukan melalui jalur VPN ini aman dari orang yang tidak berhak melihat. Gambar tentang koneksi dengan menggunakan VPN di area publik dapat dilihat di ilustrasikan gambar berikut [1]:



Gambar 2.1 Bentuk Koneksi VPN [1]

Pada gambar diatas dapat dilihat beberapa *server* dan *workstation* yang dipisahkan oleh tempat yang berbeda masih dapat saling terhubung secara aman dalam koneksi internet, dimana seakan-akan *server-server* tersebut dapat bekerja selayaknya di jaringan *local* (LAN).[1]

- **Fungsi VPN**

Teknologi VPN menyediakan beberapa fungsi utama untuk penggunaannya. Fungsi-fungsi utama tersebut antara lain sebagai berikut [7]:

Confidentially (Kerahasiaan)

Dengan digunakannnya jaringan publik yang rawan pencurian data, maka teknologi VPN menggunakan sistem kerja dengan cara mengenkripsi semua data yang lewat melaluinya. Dengan adanya teknologi enkripsi tersebut, maka kerahasiaan data dapat lebih terjaga. Walaupun ada pihak yang dapat menyadap data yang melewati internet bahkan jalur VPN itu sendiri, namun belum tentu dapat membaca data tersebut, karena data tersebut telah teracak.[7]

Data *Intergrity* (Keutuhan data)

Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada VPN terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.[7]

Origin Authentication (Autentikasi sumber)

Teknologi VPN memiliki kemampuan untuk melakukan otentikasiterhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses otentikasinya berhasil.[7]

Non-repudiation

Yaitu mencegah dua pihak dari menyangkal bahwa mereka telah mengirim atau menerima sebuah *file* mengakomodasi perubahan.[7]

Kendali akses

Menentukan siapa yang diberikan akses ke sebuah sistem atau jaringan, sebagaimana informasi apa dan seberapa banyak seseorang dapat menerima.[7]

- **Jenis VPN**

Remote Access VPN

Remote access VPN disebut juga Virtual Private Dial-up Network (VPDN). VPDN adalah jenis user-to-LAN connection. Artinya, user dapat melakukan koneksi ke private network dari manapun, apabila diperlukan. Biasanya VPN dimanfaatkan oleh karyawan yang bekerja di luar kantor[3].

Site-to-Site VPN

Site-to-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 berlangsung secara menerus (24jam) sehari. Untuk mengamankan informasi

yang berasal dari jaringan internal, VPN menggunakan beberapa metode security, seperti Firewall yang menyediakan "penghalang" antara jaringan lokal dengan internet. Pada firewall dapat ditentukan port -port mana saja yang boleh dibuka, paket apa saja yang boleh melalui firewall, dan protokol apa saja yang dibolehkan [3].

a. Enkripsi

Enkripsi merupaka metode yang umum untuk mengamankan data. Informasi akan "acak" sedemikian rupa sehingga sukar dibaca oleh orang lain. Secara umum ada dua buah metode enkripsi yaitu: Symmetric-key dan Public-key encryption[3].

b. IPSec

Internet Protocol Security Protocol (IPSec) menyediakan fitur security yang lebih baik. Seperti algoritma enkripsi yang lebih bagus dan comprehensive authentication. IPSec menggunakan dua buah mode enkripsi, yaitu Tunnel yang melakukan enkripsi pada header dan payload masing masing paket, dan Transport yang hanya melakukan enkripsi pada payload masing-masing paket.[3]

Secara umum ada dua buah asumsi yang digunakan untuk menentukan security pada VPN. Yang pertama yaitu dengan mempercayai bahwa network yang digunakan aman atau dapat dipercaya, disebut sebagai trusted model. Yang kedua adalah sebaliknya, diasumsikan network tidak aman sehingga diperlukan mekanisme security tertentu -disebut secure model.

Authentication merupakan proses untuk memastikan data dikirim kepada penerima yang diinginkan. Sebagai tambahan, authentication juga memastikan integritas penerima dari pesan dan sumbernya. Dalam bentuk yang paling sederhana, authenticationmemerlukan paling sedikit username dan password untuk menerima akses ke sumber spesifik. Dalam bentuk yang kompleks, authentication dapat didasari dari secret-key encryption atau public-key encryption. Autorisasi merupakan proses memberikan atau menolak akses ke sumber yang berlokasi dalam jaringan setelah pengguna telah berhasil diidentifikasi dan diautentikasi.[3]

C. RouterBoard

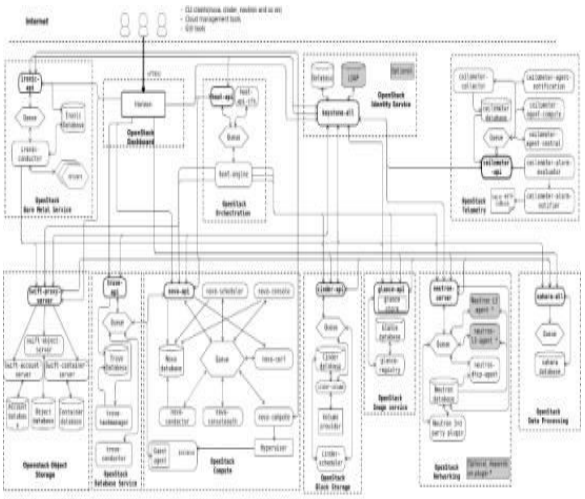
RouterBoard adalah router *embedded* produk dari MikroTik. *RouterBoard* seperti sebuah pc mini yang terintegrasi karena dalam satu *board* tertanam *Processor*, RAM (*Random Access Memory*), ROM (*Read Only Memory*). *RouterBoard* menggunakan os RouterOS yang berfungsi sebagai router jaringan, *Bandwidth Management, Proxy Server, DHCP, DNS Server* dan bisa juga berfungsi sebagai *Hotspot Server*. MikroTik pada standar perangkat keras berbasiskan *Personal Computer* (PC) dikenal dengan kestabilan, kualitas kontrol dan fleksibilitas untuk berbagai jenis paket data dan penanganan proses *route* atau lebih dikenal dengan istilah *Routing*. MikroTik yang dibuat sebagai router berbasiskan PC banyak bermanfaat untuk sebuah ISP yang ingin menjalankan beberapa aplikasi mulai dari hal yang paling ringan hingga tingkat lanjut. Contoh aplikasi yang dapat diterapkan dengan adanya MikroTik selain *routing* adalah aplikasi kapasitas akses (*bandwidth*) manajemen, *firewall*, *wireless access* point (WiFi), *backhaul link, system hotspot*, *Virtual Private Netword* (VPN) *server* dan masih banyak lainnya. Cisco tentunya bukan nama yang asing lagi dalam dunia router. Namun selain cisco ada nama lain yaitu solusi yang lebih murah untuk membangun sebuah router, yaitu MikroTik [10].

D. MikroTik

MikroTik adalah sebuah perusahaan kecil berkantor pusat di Latvia. pembentukannya pertama kali oleh John Trully dan Arnis Riekstins. John dan Arnis mulai me-routing dunia padatahun 1996 (misi MikroTik adalah me-routing seluruh dunia). Mulai dengan sistem Linux dan MS-DOS yang dikombinasikan dengan teknologi Wireless LAN (WLAN) Aeronet berkecepatan 2 Mbps diMoldova, negara tetangga Latvia, barukemudian melayani lima pelanggannya diLatvia. Prinsip dasar mereka bukan membuat Wireless ISP (W-ISP), tetapi membuat program router yang handal dan dapat dijalankan diseluruh dunia. Latvia hanya merupakan tempat eksperimen John dan Arnis, karena saat ini mereka sudah membantu negara-negara lain termasuk Srilanka yang melayani sekitar 400 pengguna. Linux yang pertama kali digunakan adalah Kernel 2.2 yang dikembangkan secara bersama-sama dengan bantuan 5-15 orang staff Research and Development (R&D) MikroTik yang sekarang menguasai dunia routing di negara-negara berkembang. Menurut Arnis, selain staf di lingkungan MikroTik, mereka juga merekrut tenega-tenaga lepas dan pihak ketiga yangdengan intensif mengembangkan MikroTiksecara maraton.[10]

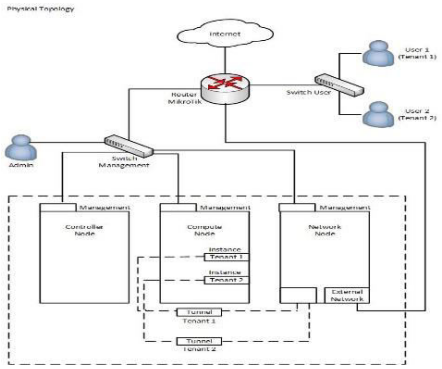
III. PERANCANGAN DAN IMPLEMENTASI

A. Block Perancangan



Gambar 3.1 Block Diagram OpenStack

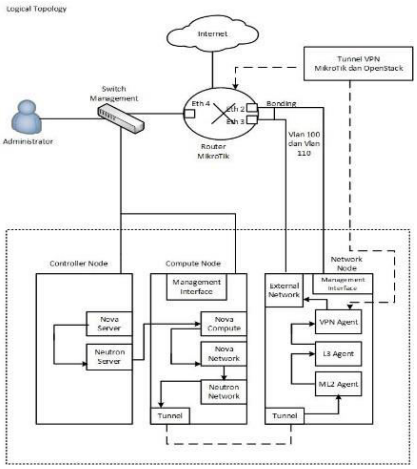
B. Topologi Fisik



Gambar 3.2 Topologi Fisik

Pada gambar Topologi Fisik dijelaskan bahwa *Server Network Node* membagi dua kategori yaitu *Network* untuk *Administrator* yang terhubung dengan *Switch Management* yang me-*manageserver Controller*, *Compute*, *Network*. Untuk membuat jaringan VPN terdapat dua *site* menggunakan Neutron VPN *driver plug-in* di dalam Neutron. Lalu penulis akan membangun dua jaringan *private* didalam dua OpenStack *project* atau *tenant* yang berbeda menggunkan IPSec site to site. *Instance* yang berbeda pada jaringan OpenStack *private* masing-masing harus dapat terhubung satu sama lain menggunakan VPN *tunnel*. Masing-masing OpenStack *tenant* terhubung dengan Router didalam *Gateway External* yang menyediakan akses jaringan *private* yang terhubung dengan sebuah *instance* (VM). Router tersebut berfungsi sebagai VPN *Gateway* lalu dapat diakses oleh *user*.

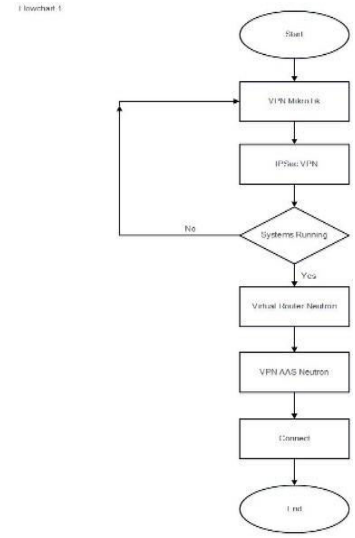
C. Topologi Logika



Gambar 3.2 Topologi Logika

Pada gambar Topology Logika dijelaskan bahwa Administrator akan terhubung dengan Switch Management. Switch Management akan mengatur Controller, Compute, Network Node. Masing-masing layanan memiliki VM (Vitrual Machine) untuk mengatur tugas yang telah diberikan. Untuk Compute Node akan memanage semua VM (Virtual Machine) yang melewati Compute Node, Tunnel di Compute Node akan terhubung melalui ML2 Agent, L3 Agent, dan VPN Agent. VPN Agent ini akan membuat jaringan seolah-olah yang terhubung langsung kedalam Router MikroTik.

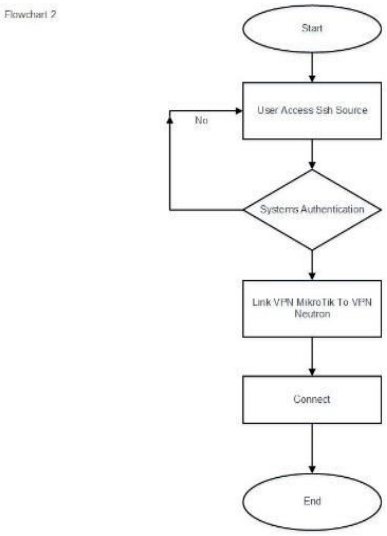
D. Flowchart 1



Gambar 3.3 Diagram Flowchart 1

Pada gambar Diagram Flowchart 1 dijelaskan bahwa VPN MikroTik akan terkoneksi antara perangkat yang memanfaatkan jaringan *public* ketika mengimplementasikan VPN interkoneksi antara *node* akan memiliki jalur khusus. Lalu akan masuk kedalam IPSec, IPSec mengatur protokol jaringan yang akan mengamankan semua aplikasi yang melalui jaringan internet protokol. Kemudian akan terhubung ke VPN Router Neutron yang menghubungkan beberapa *network* yang sama atau yang berbeda. Kemudian masuk ke dalam VPNAAS Neutron akan mengamankan jaringan yang telah dikirim menjadi jaringan *private*.

E. Flowchart 2



Gambar 3.4 Diagram Flowchart 2

Pada gambar Diagram Flowchart 2 dijelaskan bahwa proses masuk yang pertama yaitu *User Acess SSH* (*Secure Shall*) Source berfungsi sebagai

protokol yang menukar data melalui jaringan yang aman antara dua perangkat jaringan, lalu masuk kedalam *System Authentication* berfungsi memverifikasi *user* dan *password* dan memverifikasi setiap orang yang mengakses jaringan secara *remote*, kemudian masuk kesistem *Link* VPN MikroTik To VPN Neutron berfungsi sebagai jaringan VPN MikroTik akan masuk kedalam VPN Neutron akan membuat jaringan *private*.

F. Spesifikasi Perangkat Implementasi

Spesifikasi yang di butuhkan penulis untuk PC server sebelum menjalankan implementasi sebagai berikut:

Tabel 3.1 Spesifikasi Perangkat Server

Perangkat	Jenis
Processor	Xeon E1230 v.5 3.4 GHz 8Mb Cache
Mainboard	Supermicro C7c232
RAM	32 GB DDR4
HDD	4 TB
Power Supply	Cosair vs450
Fan	Deepcool Ganmax 300
Chassis	Dazumba Full Tower
Router	Mikrotik 750 GL

G. Spesifikasi Perangkat untuk Konfigurasi

Spesifikasi laptop yang digunakan penulis untuk mengkonfigurasi dan instalasi, sebagai berikut:

Tabel 3.2 Spesifikasi Perangkat Laptop

Perangkat	Jenis
Processor	Intel(R) Core(TM) i3-4030U CPU@ 1.90 GHz
RAM	4 GB
Operating System	Windows 8 Home 64-bit

IV. PENGUJIAN DAN ANALISA

A. Pengujian Service VPNAAS

- **Tujuan Penelitian**

Tujuan penelitian ini dimaksudkan untuk mengetahui bahwa service VPNAAS yang terdapat di Neutron berjalan dengan baik tanpa kendala dan eror. Pengujian ini sangat sederhana dengan memanfaatkan dua tenant yang berbeda dan didalam tenant-tenant tersebut dibuatkan masing-masing instance serta dibuatkan service VPN, satu sama lain saling terkoneksi.

- **Hasil Pengujian**

Hasil pengujian yang didapat tertera pada gambar 4.10. Hasil pengujian sistem yang dirancang telah berhasil untuk melakukan pengecekan pada sistem tersebut maka penulis akan melakukan PING untuk mengetahui apakah layanan VPNAAS telah terhubung. Dengan melakukan PING pada salah satu tenant dengan IP 10.200.200.1.

Gambar 4.10 Hasil Pengujian PING

Gambar 4.11 Analisa Pengujian PING Kedua Tenant

- **Analisa Pengujian Pertama**

Pada tahap ini dilakukan analisa pengujian pada sistem yang bertujuan untuk melihat apakah VPNAAS terhubung atau tidak. Pengujian VPNAAS harus memiliki 2 instance tenant yang berbeda agar saling terkoneksi satu sama lain. Test PING dan pertukaran data akan berhasil apabila ke 2 instance telah dibuat. Pengujian tidak akan berhasil apabila setting IP pada ke 2 intance tersebut tertukar.

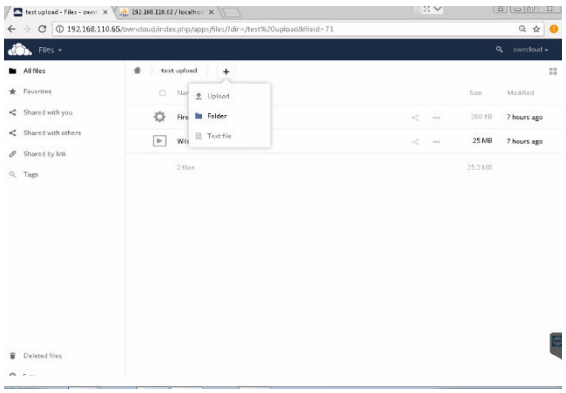
- **Analisa Pengujian Kedua**

Untuk pengujian dan analisa kedua pada sistem dilakukan setelah melakukan PING pada ke 2 Tenant, penulis akan melakukan upload data berupa file yang masuk melalui sistem Owncloud yang telah terhubung melalui IP Address. Lalu akan dianalisa menggunakan software wireshark untuk mengetahui berapa bandwidth dan packet loss yang di dapat ketika upload data.

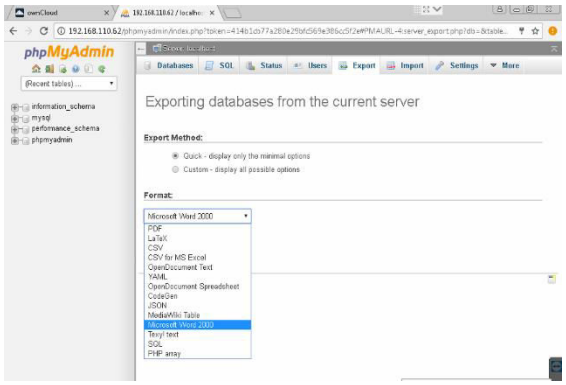
- **Analisa Pengujian Ketiga**

Setelah pengujian kedua selesai, maka penulis akan melalukan analisa dan pengujian ke 3 pada

sistem yaitu mendownload atau me-export data di dalam database yang telah terhubung melalui IP Address VPN. Lalu penulis akan menganalisa menggunakan software wireshark untuk mengetahui berapa bandwidth dan packet loss yang di dapat ketika men-download data.



Gambar 4.12 Analisa Pengujian Upload



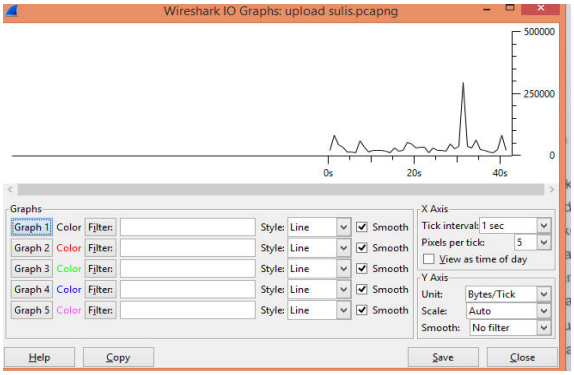
Gambar 4.13 Analisa Pengujian Download

- **Hasil Pengujian menggunakan Wireshark**

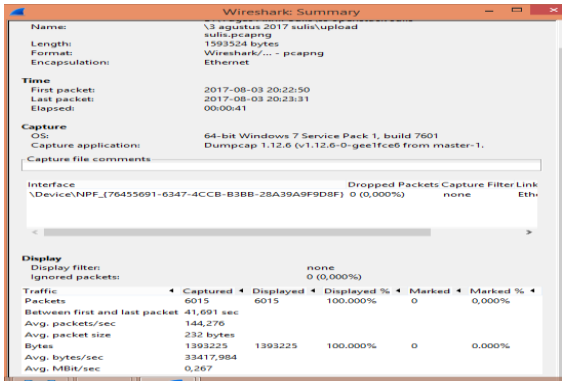
Hasil pengujian menggunakan wireshark penulis melakukan analisa bandwidth dan packet loss, hasil yang telah berhasil dapat dilihat .

Bandwidth (lebar pita) adalah besaran yang menunjukan seberapa banyak data yang dilewatkan dalam koneksi melalui sebuah network. Lebar pita atau kapasitas saluran informasi. Kemampuan maksimum dari suatu alat untuk menyalurkan informasi dalam satuan waktu detik (bit/second).

Berikut adalah nilai bandwidth hasil capture menggunakan software wireshark pada upload file.



Gambar 4.14 Hasil Grafik Bandwidth Upload File



Gambar 4.15 Hasil Pengujian Upload File

Untuk mencari hasil perhitungan Upload File sebagai berikut:

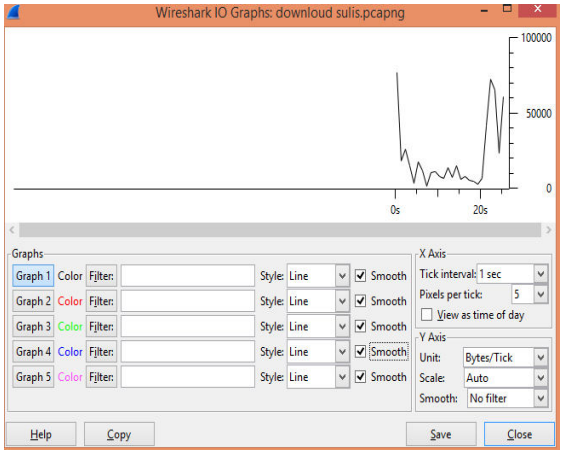
Bandwidth = bytes/ (between first and last packet)(bytes/sec)

=1393225×8=11145800÷1000÷1000

=11,1458/41,691=0,267 Mbit/sec

Dari simulasi yang dilakukan, hasil capture diatas menunjukan bandwidth yang dihasilkan pada saat melakukan Upload file dari Owncloud menggunakan wireshark memiliki nilai 0,267 Mbit/sec.

Sedangkan untuk menghitung bandwidth pada saat mendownload file sebagai berikut:



Gambar 4.16 Hasil Grafik Bandwidth Download File

Untuk mencari hasil perhitungan Download sebagai berikut:

Bandwidth = bytes/(between first and last packet)(bytes/sec)

= 526079×8=4208632÷1000÷1000

= 4,208632/25,952 = 0,162 Mbit/sec

Dari simulasi yang dilakukan, hasil capture diatas menunjukan bandwidth yang dihasilkan pada saat melakukan Download file dari Owncloud menggunakan wireshark memiliki nilai 0,162 Mbit/sec.

Packet Loss merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukan jumlah total paket yang hilang dapat terjadi karena collision (dimana paket dapat bertabrakan dengan satu sama lain ketika dikirim) dan congestion (kelebihan kapasitas dari sebuah path data) pada jaringan. Kategori nilai packet loss yaitu:

Tabel 4.1 Kategori Nilai Packet Loss

Kategori Degredasi	Packet loss (%)	Indeks
Sangat bagus	0	4
Bagus	3	3
Sedang	15	2
Jelek	25	1

Untuk mencari hasil perhitungan packet loss pada saat Upload File yaitu:

packet loss = ((paket data yang dikirim-paket data yang diterima))/(paket data yang dikirim)×100%

= (3014 - 3014)/3014×100%= 0%

Hasil perhitungan packet loss pada saat melakukan Upload masuk kedalam kategori degredasi sangat bagus yaitu 0% menurut standar TIPHON. Semua paket data yang ditransmisi 100% sampai ke pada tujuan.

Untuk mencari hasil perhitungan packet loss pada saat Download yaitu:

packet loss = ((paket data yang dikirim-paket data yang diterima))/(paket data yang dikirim)×100%

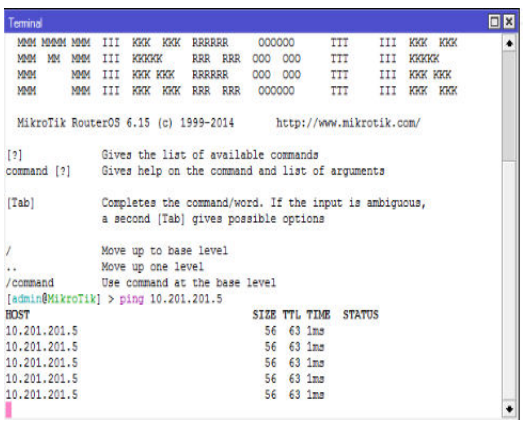
= (6015-6015)/6015×100%= 0%

Hasil perhitungan packet loss pada saat melakukan Download masuk kedalam kategori degredasi sangat bagus yaitu 0% menurut standar TIPHON. Semua paket data yang ditransmisi 100% sampai ke pada tujuan.

B. Hasil Pengujian MikroTik

- **Hasil pengujian VPNAAS Terkoneksi VPN MIKROTIK**

Hasil pengujian yang didapat tertera pada gambar dibawah ini:

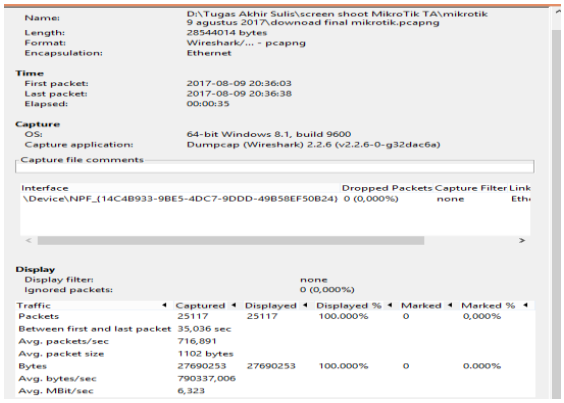


Gambar 4.23 Pengujian VPNAAS Ke MikroTik

Pada gambar diatas jelas bahwa pengujian sistem telah berhasil terhubung. Untuk pengujian VPN MikroTik agar dapat terkoneksi dengan VPNAAS penulis akan melakukan setting IPSec Policies dengan IP Network yang sama dengan IP di dalam VPNAAS pada OpenStack, untuk Peers dan Remote Peers MikroTik harus diberikan IP Gateway yang sama dengan IP Gateway di dalam OpenStack, setelah setting MikroTik selesai hasil pengujian akan dilakukan dengan test PING untuk mengetahui apakah layanan VPNAAS terhubung langsung dengan VPN MikroTik. Dengan melakukan test PING pada VPNAAS dengan IP 10.201.201.5. Setting MikroTik tidak akan terhubung atau terkoneksi apa bila IP yang di setting tertukar.

- **Hasil Pengujian menggunakan Wireshark**

Hasil pengujian menggunakan wireshark penulis melakukan analisa bandwidth dan packet loss, hasil yang telah berhasil dapat dilihat



Gambar 4.24 Hasil Pengujian Download File MikroTik

Untuk menghitung bandwidth dengan rumus sebagai berikut:

Bandwidth = bytes/(between first and last packet)(bytes/sec)

= 27690253×8 =221522024 ÷1000 ÷1000=221,522024/35,036=6,323 Mbit/sec

Hasil pengukuran bandwidth yang didapat pada saat melakukan Download File MikroTik dari Owncloud menggunakan wireshark memiliki nilai 6,323 Mbit/sec.

Untuk menghitung packet loss dengan rumus sebagai berikut:

packet loss = ((paket data yang dikirim-paket data yang diterima))/(paket data yang dikirim)×100%

= (25117 - 25117)/25117×100%= 0%

Hasil perhitungan packet loss pada saat melakukan Download File MikroTik masuk kedalam kategori degredasi sangat bagus yaitu 0% menurut standar TIPHON. Semua paket

data yang ditransmisi 100% sampai ke pada tujuan.

V. KESIMPULAN PENGUJIAN

Kesimpulan yang didapat dari hasil pengujian adalah sebagai berikut:

1) Adanya sistem model jaringan *Virtual Private Network* pada *OpenStack* yang terhubung pada *Virtual Private Network* MikroTik.
2) Dengan adanya sistem *Virtual Private Network* yang terkoneksi dengan MikroTik dapat membuat pengguna lebih aman dalam menggunakan jaringan.
3) Adanya hasil analisa antara dua jaringan VPNAAS pada sistem cloud dan *Virtual Private Network* yang terdapat pada router MikroTik.
4) Adanya sistem *Virtual Private Network* menggunakan keamanan IPSec
5) Bandwidth yang dihasilkan pada saat melakukan *upload file* dari *owncloud*memiliki nilai 0,267 Mbit/secdan hasil pengukuran *bandwidth* yang didapat pada saat melakukan *download file* dari *owncloud* memilik nilai 0,162 Mbit/sec.
6) Untuk hasil perhitungan *packet loss* pada saat melakukan *upload file* pada *owncloud* dan *Download File* pada *Database* dapat di kategorikan dalam degredasi sangat bagus yaitu 0%. Dan untuk perhitungan *packet loss* pada saat melakukan *Download File*melaluiMikroTik masuk kedalam kategori degredasi sangat bagus yaitu 0% menurut standar TIPHON dan ITU-T. Semua paket data yang ditransmisi 100% sampai ke pada tujuan.
7) Standar yang dikeluarkan pada TIPHON dan ITU-T kategori nilai *packet loss* yang sangat bagus adalah 0% dengan *indeks* 4, sedangkan pada kategori jelek 25% memiliki *indeks* 1.

DAFTAR PUSTAKA

[1] Athailah. 2012. Kontrol dan Amankan Koneksi Internet di Jaringan. Jakarta: PT Elex Media Komputindo. (Diakses pada hari Senin, Januari 23, 2017, 15.51)

[2] Drs. Daryanto. 2010. Teknik Jaringan Komputer. Bandung: Alfabeta,cv. (Diakses pada hari Senin, Januari 23, 2017, 15.55)

[3] Firmansyah Fikri, Badrul Mohammad. (2015). "Penerapan Metode Open VPN-Access Server Sebagai Rancangan Jaringan Wide Area Network". Jurnal Techno Nusa Mandiri, 1 (12): 12. http://ejournal.nusamandiri.ac.id/ejurnal/index.php/techno/article/view/125/117 (Diakses pada hari Minggu, Januari 22, 2017, 14:43)

[4] Kurniawan Wiharsono. 2007. Jaringan Komputer. Yogyakarta: C.V Andi Offset. (Diakses pada hari Senin, Januari 23, 2017, 10.36)

[5] Oktivasari, Prihatin. Utomo Andri Budhi. (2016). "Analisa Virtual Private Network Menggunakan OpenVPN Dan Point To point Tunneling Protocol". Jurnal Penelitian Komunikasi dan Opini Publik, 2 (20): 187-189. https://jurnal.kominfo.go.id/index.php/jpkop/article/download/658/489 (Diakses pada hari Minggu, Januari 22, 2017, 17:02)

[6] Purwanto Deny, Dana Raditya Danar. (2015). "Sistem Keamanan Jaringan Model Client Server Menggunakan Enksripsi Data (MD5) Pada Dinas Kesehatan Kota Cirebon". Jurnal Online ICT STMIK IKMI, 1 (13): 4. http://stmik-ikmi-cirebon.net/e-journal/index.php/JICT/article/view/103/98 (Diakses pada hari Jumat, Januari 20, 2017, 22:21)

[7] Tumigolung, Alva S. M.. (2015). "Perancangan Sistem Pencegahan Flooding Data Pada Jaringan Komputer". E-Journal Teknik Elektro dan Komputer, 1 (4): 10. http://ejournal.unsrat.ac.id/index.php/elekdankom/article/view/6520/6045 (Diakses pada hari Selasa, Januari 24, 2017, 14:53)

PENULIS

Cholifah Sulistin Angraeni, lahir di Tangerang 13 Agustus 1996. Memperoleh gelar Diploma III dari Program Studi Teknik Telekomunikasi Akademi Telkom Jakarta. 2016