DESIGN PENGAMANAN AKSES JARAK JAUH JARINGAN RUMAH DENGAN TEKNOLOGI VPN (VIRTUAL PRIVATE NETWORK) BERBASIS DI CLOUD VPS (VIRTUAL PRIVATE SERVER)

Domo Pranowo Kuswandono
Program Studi Teknik Informatika, STMIK Bani Saleh, dpranowo@gmail.com

ABSTRAK

Teknologi informasi dan komunikasi berbasis internet telah berkembang dengan pesat, akses dan pemanfaatannya berkembang dari perusahaan atau korporasi, ke perkotaan dan sampai ke perumahan untuk penggunaan pribadi yang dikenal dengan *smart home*. Dengan berkembangnya sistem komputasi awan (*virtual cloud system*) untuk memenuhi kebutuhan akses data yang aman dan juga akses jarak jauh. Untuk mengakses jaringan yang ada dirumah dibutuhkan IP public, dimana Penggunaan pribadi masih terbatas menggunakan IP Public dinamis sehingga tidak mudah untuk melakukan koneksi dengan mudah. Mempertimbangkan hal diatas perlu adanya jalur khusus yang digunakan untuk mengamankan data yang penting atau bersifat pribadi melalui jaringan internet dengan IP public stastis, di dalam penulisan ini penulis akan memanfaatkan teknologi VPS (virtual Private server) untuk membangun jalur pribadi rumah (*Virtual Private Network*), komunikasi virtual ini memanfaatkan teknologi VPS untuk mendapatkan IP Public statis yang akan digunakan antara perorangan atau perumahan 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 (VPN) dan router yang ada di komputasi awan, Cloud Hosted Router (CHR) untuk memanfaatkan IP Public static. Sehingga mempermudah sekaligus mengamankan jaringan atau komunikasi data dari jarak jauh, menjadikan solusi jaringan rumah pintar (smart home) yang hanya memiliki IP Public dinamik

Kata Kunci: Virtual Private Server, CHR, jalur pribadi, VPN

PENDAHULUAN

Peranan dari teknologi informasi akan semakin penting untuk perusahaan bahkan personal, Berdasar survey yang dilakukan APJII tempat yang paling banyak untuk akses internet adalah dari rumah 62.35%, dan dari kantor 16.08% (Hasil survey APJII 2016). Oleh karena itu dibutuhkan sistem jaringan komputer untuk menyediakan pelayanan aliran informasi atau pengendalian akses sumber daya jaringan dari jarak jauh yang letaknya berjauhan. Untuk personal kebutuhan mengakses sumber daya data atau komputer yang ada dirumah bisa diakses dari tempat manapun dengan aman menjadi idaman. Sejauh ini banyak yang sudah mengimplentasikan sistem jaringan lokal seperti instansi/perusahaan, bandara, universitas untuk komunikasi dari jarak jauh (*remote access*). Namun ada beberapa yang menggunakan sistem jaringan komputer melalui internet tidak aman yaitu masalah penyadapan informasi karena data yang dikirim tidak terenkripsi dan melalui jalur umum (internet). Teknologi *Virtual Private Network (VPN)* menjadi salah satu solusi. VPN mampu membuat jalur sendiri diatas jalur umum dan data yang dikirim dienkripsi sehingga tidak bisa dibaca oleh orang yang tidak berhak. VPN cocok digunakan untuk jaringan komputer diperumahan, masalah yang dihadapi adalah keterbatasan kepemilikan IP Public statis karena membutuhkan biaya sewa yang cukup mahal untuk pribadi. Karena untuk memudahkan akses VPN diperlukan IP Public statis. Namun perkembangan tekhnolgi vitrualisasi yang makin berkembang salah satu contohnya adalah tentang *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. Dan yang tidak kalah penting adalah VPS menyediakan IP public yang statis yang bisa dimanfaatkan secara bersama-sama melalui teknologi Cloud Hosted Routing (CHR) utk membuat menjadi jaringan

private. 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, makalah ini akan disampaikan tentang bagaimana mengimplementasikan sebuah perancangan infrastruktur untuk mengakses jaringan *intranet* yang berada pada *private network*, dan juga meninjau pengaruh performa yang ada, dengan memanfaatkan teknologi yang ada seperti *Virtual Private Server* dan *Virtual Private Network*. Makalah ini juga akan menjelaskan cara implementasi penggunaan VPN dengan protokol L2TP, L2TP ini memungkinkan penggunanya untuk tetap dapat terkoneksi dengan jaringan lokal milik mereka dengan *policy* keamanan yang sama dan dari manapun mereka berada, melalui koneksi VPN. Serta menjelaskan penggunaan Cloud Hosted Router (CHR) untuk memanfaatkan IP public static sebagai penghubung antar jaringan yang ada dirumah-rumah. Harapannya sember daya jaringan yang ada dirumah bisa di kendalikan secara jarak jauh dan aman.

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 Publik Dinamik.
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 Cloud*ing 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.

Metodologi 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

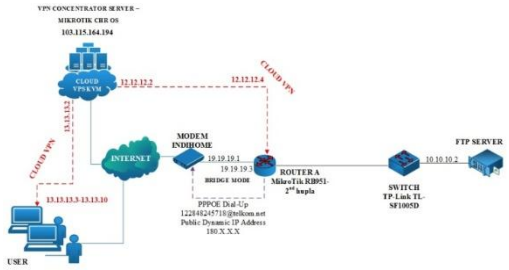
pengembangan jaringan LAN dengan jaringan ini lebih bersifat teknis, di mana setiap tahapan dilakukan secara berurutan agar pengembangan *routing* dengan beberapa Router MikroTik dapat dilakukan secara terstruktur. Adapun metodologi yang digunakan antara lain seperti berikut ini:

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*.

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

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.

Tabel 1. *Interface* dan IP *Address* Jaringan Penelitian VPN *Clouding*

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-*server*	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-*client*	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	-

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):

Tabel 2. Standard Nilai Throughput

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

Sumber : Jurnal CoreIT, Vol.1, No.2, Desember 2015:68

Tabel 3. Standard Nilai *Delay*

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

Sumber : Jurnal CoreIT, Vol.1, No.2, Desember 2015:69

Tabel 4. Standard Nilai *Packet loss and Jitter*

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

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)

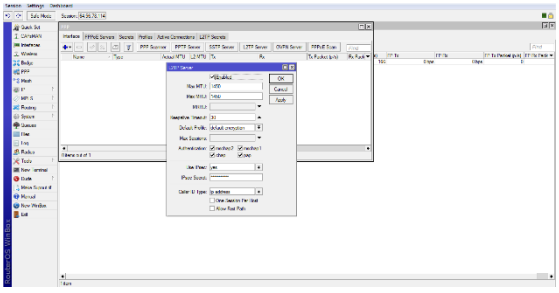
Konfigurasi CHR menggunakan port SSH dengan software PuTTy mengarah ke IP Publik dan User name, password diatas, untuk merubah setting di VPS KVM dari OS default linux ke MikroTik CHR RouterOS.

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
```

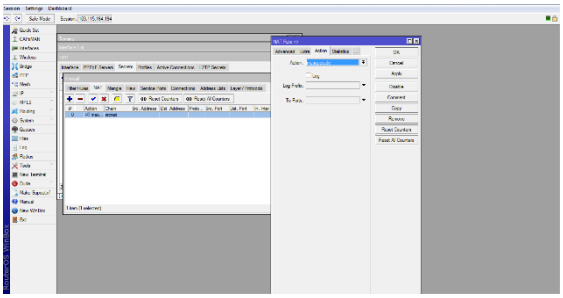
Setelah MikroTik RouterOS CHR terinstall di VPS selanjutnya adalah instalasi Virtual private network (VPN) Concentrator. VPN yang akan implementasi adalah VPN yang menggunakan *service Layer Two Tunneling Protocol* (L2TP) dengan protokol enkripsi data IP *Security* (IPSec). Dan pengaktifan protokol IPsec pada menu *Use IPsec* ubah pengaturan menjadi "*yes",* kemudian pada kolom *IPsec Secret* penulis memberikan kata kunci "password2018" 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. 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

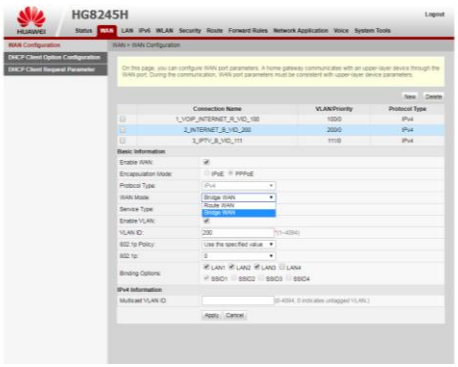
Konfigurasi IP Public Pada MikroTik

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 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

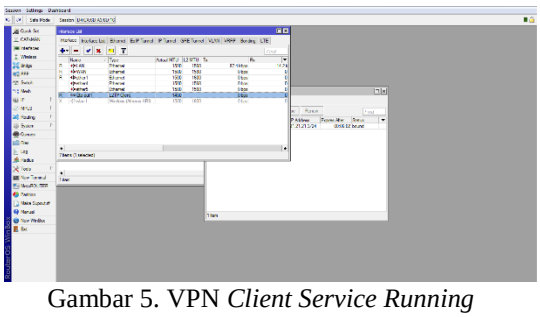
Mengkoneksikan Router Lokal ke VPN Server MikroTik CHR

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.*



Gambar 4. Konfigurasi *Mode Bridge* Router Indihome

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 *user*name 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

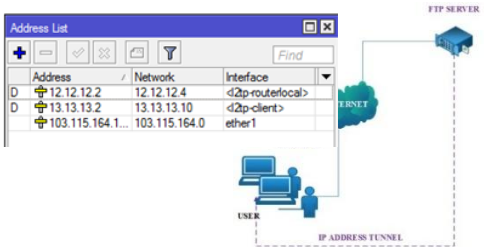
Membuat Routing Menuju FTP Server

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 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".

Uji Coba 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 :

1. Perhitungan *Request Time* dan *Respawn Time* pada paket *download* dan *upload.*
2. Perhitungan jumlah paket keseluruhan, jumlah waktu keseluruhan dan jumlah paket keseluruhan dalam bytes.
3. Pengujian *Download* dan *Upload* dilakukan menggunakan *VPN Cloud*
4. Sampel data dibatasi hanya dari 5 buah file.
5. Perhitungan *Delay*, *Packet loss*, *Jitter*, *Throughput*.

Percobaan Download Dan Upload Dengan VPN Clouding

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

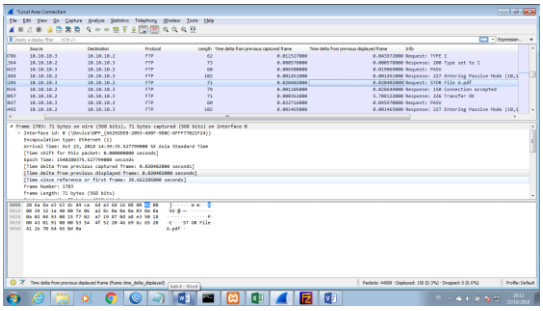
Tabel 5. Besar file yang diupload dan download

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

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 (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.

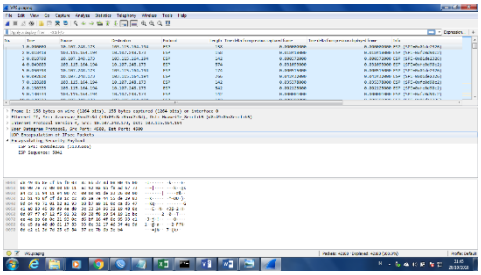
Percobaan *download* file melalui *VPN Cloud* t terlihat transfer data dari *server* "10.10.10.2" ke *client* "10.10.10.3", dengan pesan "RETR" yang merupakan pesan request dari *client* ke *server* yang berarti meminta *server* untuk mengirim copy data yang berada pada direktori *FTP Server* (*download* 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



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 *Respon Time

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

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

Packet loss

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

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

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

Delay

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

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

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

Throughput

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

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

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

Jitter

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

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

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

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

SIMPULAN DAN SARAN

Simpulan

Kesimpulan dari design implementasi pengamanan akses jarak jauh ini antara lain:

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* tersebut yang berfungsi sebagai VPN *server*. *cloud router* bisa di dapatkan dengan menerapkan MikroTik *Cloud Hosted Router* (CHR) pada VPS.
2. Kekurangan berlangganan internet di rumah yang hanya memperoleh IP Public dinamik, bisa diselesaikan dengan memakai IP public statik yang diperoleh di VPS, 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, 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

DAFTAR PUSTAKA

Ahmad Imanudin, Virtualisasi server bebasis PROMOX, Excellent Publising, 2018

Athailah, Mikrotik Untuk Pemula, Mediakita TransMedia, 2013

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

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

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. Belajar Jaringan Komputer Berbasis Mikrotik OS. Gava Media : Yogyakarta, 2015

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

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