# Perancangan dan Implementasi VPN *Server* dengan menggunakan Protokol SSTP (*Secure Socket Tunneling Protocol*) Studi Kasus Kampus Universitas Sam Ratulangi

Kaseger Arthur Farly, Xaverius B. N. Najoan, Arie S. M. Lumenta
Teknik Informatika Universitas Sam Ratulangi
120216110@student.unsrat.ac.id, xnajoan@unsrat.ac.id, al@unsrat.ac.id

***Abstrak* – Jaringan internet merupakan salah satu kebutuhan manusia sekarang ini. Begitu banyak aktifitas manusia menjadi lebih mudah dengan adanya jaringan internet seperti proses mengirim data dari satu tempat ke tempat lain. Proses pengiriman data tersebut hanya membutuhkan beberapa detik untuk sampai ke tempat yang dituju. Tetapi dengan perkembangan jaringan internet tersebut banyak oknum yang mencoba memanfaatkan jaringan internet untuk mencuri data. Seperti Data Perbankan, Data Rekam Medis, Data akademik kampus yang sangat penting seperti di salah satu perguruan tinggi dikota Manado,**

**Oleh karena itu dibutuhkan sebuah teknologi atau sistem yang dapat mengamankan data pada saat proses pengiriman. Dengan menggunakan teknologi Virtual Private Network (VPN) dapat menjamin keaman dalam proses pengiriman data melalui jaringan internet.**

**Kata Kunci** : Internet, VPN, *Server*, *Softether*, Unsrat, SSTP, L2TP, Protokol, Keamanan

## I. PENDAHULUAN

Perkembangan dunia Teknologi Informasi saat ini sudah sangat pesat khususnya Internet, begitu banyak Aktifitas manusia menjadi lebih cepat diselesaikan dengan adanya Teknologi Internet tersebut. Pertukaran informasi dari satu tempat ke tempat lain menjadi mudah dan sangat cepat berkat adanya internet.

Akan tetapi dari segi keamanan walaupun internet memiliki berbagai Jenis *Protocol* keamanan tetapi masih ada orang – orang atau kelompok tertentu yang dapat menembus keamanan yang berakibat pada pencurian data informasi penting.

Contohnya seperti di perusahaan atau kampus begitu banyak informasi penting yang bisa dicuri oleh orang yang tidak bertanggung jawab tentu akan sangat merugikan kampus tersebut oleh karena itu dibutuhkan sebuah cara atau metode yang dapat mengurangi bahkan menghilangkan berbagai tindak pencurian data informasi yang dilakukan melalui Jaringan internet.

*Virtual Private Network* (VPN) merupakan salah satu cara untuk melindungi pertukaran data informasi melalui Jaringan internet, khususnya dengan menggunakan Protokol *Secure Socket Tunneling Protokol* (SSTP) dapat membuat komunikasi antar beberapa Jaringan melalui sebuah *Tunneling* yang melewati Jaringan internet dengan aman.

## II. LANDASAN TEORI

### 2.1 Jaringan Komputer

Jaringan Komputer (*Computer Network*) adalah himpunan *Interkoneksi* sejumlah komputer *Autonomous*. Kata "*Autonomous*" mengandung pengertian bahwa komputer tersebut memiliki kendali atas dirinya sendiri. Bukan merupakan bagian komputer lain, seperti sistem terminal yang biasa digunakan pada komputer *Mainframe*. Komputer juga tidak mengendalikan komputer lain yang dapat mengakibatkan komputer lain *Restart, Shutdown,* Merusak *File*, dan sebagainya.

#### 2.1.1 Jenis – Jenis Jaringan Komputer

Secara umum jaringan komputer terbagi atas 3 jenis yaitu :

- Jaringan LAN (Local Area Networking)
- Jaringan MAN (Metropolitan Area Networking)
- Jaringan WAN (Wide Area Networking)

#### 2.1.2 Topologi Jaringan Komputer

Topologi Jaringan atau Arsitektur Jaringan adalah gambaran perencanaan Hubungan antarkomputer dalam *Local Area Network* yang umumnya menggunakan kabel (sebagai media transmisi), dengan konektor, *Ethernet card*, dan perangkat pendukung lainnya **(Melwin, 2008)**. Ada beberapa jenis Topologi yang terdapat pada hubungan komputer pada jaringan local area, seperti :

- Topologi Star
- Topologi Ring
- Topologi Daisy – Chain
- Topologi Tree
- Topologi Mesh

### 2.2 Protokol – Protokol Jaringan

Protokol merupakan himpunan aturan-aturan yang memungkinkan komputer satu dapat berhubungan dengan komputer yang lain. Aturan-aturan ini meliputi tata cara bagaimana agar komputer bisa saling berkomunikasi, biasanya berupa bentuk (model) komunikasi, waktu (saat berkomunikasi), barisan (Traffic saat berkomunikasi), pemeriksaan error saat transmisi data, dan lain-lain.

Protokol Jaringan adalah berbagai Protokol yang terdapat dari lapisan teratas sampai terbawah yang ada dalam sederetan Protokol. Dipandang dari sudut

komunikasi data, ada beberapa Protokol yang banyak digunakan pada Jaringan komputer, di antaranya:

2.2.1 TCP/IP (*Transmission Control Protocol/Internet Protocol*).

TCP/IP merupakan Protokol standar pada Jaringan internet yang tidak tergantung pada jenis komputer yang digunakan. Dengan menggunakan TCP/IP akan memungkinkan berbagai komputer (seperti PC IBM, Machintosh, Sun, HP, dll) berinteraksi satu dengan lain tanpa mengalami masalah yang berarti.

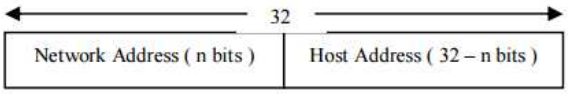
2.2.2 UDP (*User Datagram Protocol*)

*User Datagram Protokol* (UDP) adalah sebuah Protokol yang bekerja pada *Transport Layer*, mulai digunakan dan dikembangkan oleh US *Department of Defence* (DoD) untuk digunakan bersama Protokol IP di *Network Layer*. Protokol UDP memberikan alternatif *Transport* untuk proses yang tidak membutuhkan pengiriman yang handal.

2.3 Arsitektur IPv4 (*Internet Protocol Version* 4)

Model pengalamatan dalam IPv4 menggunakan 32 bit bilangan biner. Namun untuk mempermudah penulisannya maka setiap delapan bit biner diwakili oleh satu segmen bilangan oktet, sehingga setiap alamat akan memiliki empat buah segmen dari 0.0.0.0 sampai dengan 255.255.255.255 misalnya 202.152.254.254 sehingga total alamat sebesar $2^{32}$.

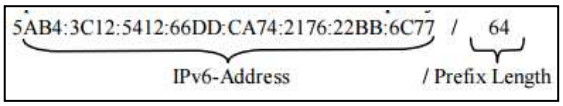
Alamat IPv4 dibagi menjadi dua bagian yaitu alamat jaringan (*network address*) dan alamat komputer (*host address*). *Network address* digunakan untuk menunjukkan di jaringan mana komputer berada, sedangakan "*host address*" menunjukkan komputer tersebut dalam jaringannya tersebut.




Gambar 1. Format IPv4

2.4 Arsitektur IPv6 (*Internet Protocol Version* 6)

Pada dasarnya IPv6 dikembangkan untuk mengantisipasi kelangakaan IP address yang disediakan oleh IPv4. Karena IPv6 ini tidak lagi menggunakan 32 bit biner tetapi 128 bit biner, sehingga alamat yang mampu disediakan yaitu 2128 atau sebesar 3 x 1038 alamat. Selain itu juga dilakukan perubahan dalam penulisannya yaitu 128 bit alamat dipisahkan menjadi masing-masing 16 bit yang tiap bagian dipisahkan dengan ":" dan dituliskan dengan bilangan hexadesimal. Untuk mengetahui letak subnet dari alamat tersebut maka penulisan alamat IPv6 harus mempunyai format :




Gambar 2. Format IPv6

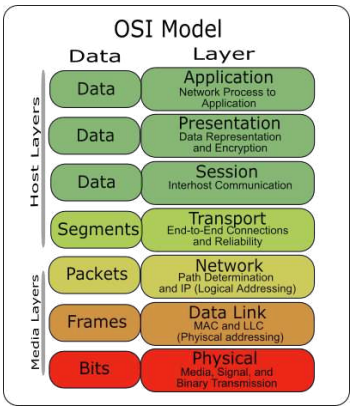
2.5 OSI Layer

OSI (Open Sistem Interconnection) adalah standart arsitektur jaringan yang dikeluarkan oleh International Standards Organizations (ISO), dapat diartikan sebagai sistem yang terbuka untuk berkomunikasi dengan sistem sistem lainnya. Tujuan OSI yaitu :

1. Menghilangkan ketergantungan pada suatu produsen.
2. Mengikuti perkembangan tanpa harus mengorbankan perangkat keras atau perangkat lunak yang sudah ada.

Untuk keperluan itu maka dibuatlah spesifikasi yang bersifat terbuka yang berisi bakuan-bakuan tentang kualitas dan metode kerja suatu sistem jaringan.

Setiap layer mempunyai bakuan bakuan sendiri tetapi bakuan masih memungkinkan untuk berkomunikasi dengan layer yang lain. OSI membagi komponen jaringan dalam 7 layer yaitu :




Gambar 3. OSI Layer

2.6 VPN (*Virtual Private Network*)

VPN adalah singkatan dari *Virtual Private Network*, yaitu sebuah terowongan *Virtual* (*Virtual Tunnel*) dari jaringan ke jaringan lain yang terenkripsi. VPN *server* dan VPN *Client* harus saling ter-autentikasi. VPN mengkoneksikan dua jaringan seperti kantor - kantor cabang atau *Remote User* tunggal ke kantor. (Carla Schroder, 2008:p265).

Teknologi VPN menyediakan 2 fungsi utama untuk penggunanya. Fungsi utama tersebut adalah sebagai berikut:

a. *Confidentiality*

Teknologi VPN memiliki sistem kerja meng*Enkripsi* semua data yang lewat melaluinya. Dengan menerapkan sistem *Enkripsi* ini, tidak ada satupun orang yang dapat mengakses dan membaca isi Jaringan data *Client* dengan mudah. VPN memiliki teknologi yang dapat menjaga keutuhan data yang *Client* kirim agar sampai ketujuannya tanpa cacat, hilang, rusak, ataupun dimanipulasi oleh orang lain.

b. *Origin Authentication*

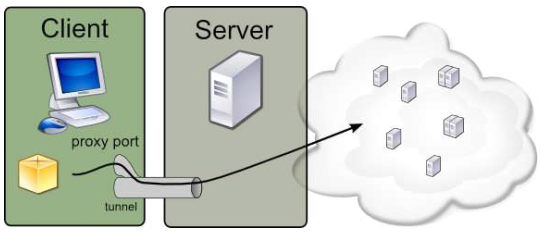
Teknologi VPN memiliki kemampuan untuk melakukan otentikasi terhadap sumber-sumber pengirim data yang akan diterimanya.

2.7 *Tunneling*

*Tunneling* adalah dasar dari VPN untuk membuat suatu Jaringan private melalui Jaringan internet. *Tunneling* juga merupakan enkapsulasi atau pembungkusan suatu Protokol ke dalam paket Protokol.

*Tunneling* menyediakan suatu koneksi *Point-To-Point* logis sepanjang Jaringan IP yang bersifat

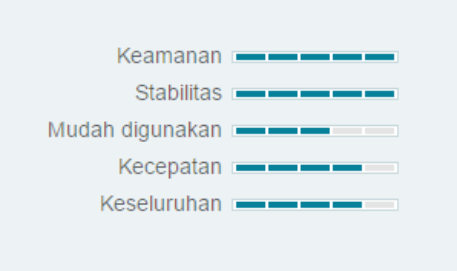
*connectionless*. Proses transfer data dari satu Jaringan ke Jaringan lain memanfaatkan Jaringan internet secara terselubung (*Tunneling*). Ketika paket berjalan menuju ke node tujuan, paket ini melalui suatu jalur yang disebut tunnel.




Gambar 4. Ilustrasi *Tunneling*

2.8 Protokol SSTP

*Secure Socket Tunneling Protokol* adalah tembusan protokol yang tersedia pada platform Microsoft. Protokol ini berbasis pada kombinasi kedua teknologi, SSL dan TCP. Teknologi SSL menjaminkan tingkat keamanan transportasi dan integritas lalu lintas. SSL pada server kami dikonfigurasikan sedemikian rupa sehingga hanya metode enkripsi terkuatlah yang diaktifkan. Sejak sesi SSTP, dalam kenyataannya, sebuah sesi HTTPS, SSTP mungkin bisa digunakan melalui firewalls atau ISP throttling. Di sisi lain, sejak SSTP beroperasi melalui TCP, dalam beberapa kasus akan di kendalikan IKEv2 atau protokol berbasis UDP lainnya. Secara keseluruhan, SSTP adalah pilihan terbaik dan dapat membantu menyelesaikan masalah konektivitas ataupun masalah kecepatan yang anda miliki.

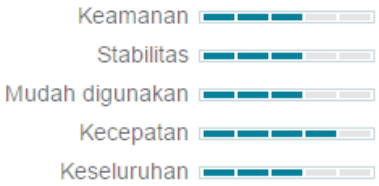



Gambar 5. Performa Protokol SSTP

2.9 Protokol L2TP

L2TP merupakan pengembangan dari PPTP ditambah L2F. *Network Security Protocol* dan *enkripsi* yang digunakan untuk autentikasi sama dengan PPTP. Akan tetapi untuk melakukan komunikasi, L2TP menggunakan UDP port 1701. Biasanya untuk keamaanan yang lebih baik, L2TP dikombinasikan dengan IPSec, menjadi L2TP/IPSec. Contohnya untuk Operating system Windows, secara default OS Windows menggunakan L2TP/IPSec. Akan tetapi, konsekuensinya tentu saja konfigurasi yang harus dilakukan tidak se-simple PPTP. Sisi client pun harus sudah support IPSec ketika menerapkan L2TP/IPSec. Dari segi enkripsi, tentu enkripsi pada L2TP/IPSec memiliki tingkat sekuritas lebih tinggi daripada PPTP yg menggunakan MPPE. Trafik yang melewati tunnel L2TP akan mengalami overhead ± 12%.

L2TP lebih "firewall friendly" dibandingkan jenis VPN yang lainnya seperti PPTP. Hal ini sebuah Keuntungan besar jika menggunakan protocol ini, karena kebanyakan Firewall tidak mensupport GRE. Namun untuk L2TP tidak memiliki encripsi sehingga kita memerlukan service tambahan guna menunjang keamanan yang lebih tinggi. Oleh karena itu kita akan memadukan L2TP dengan IPSec.

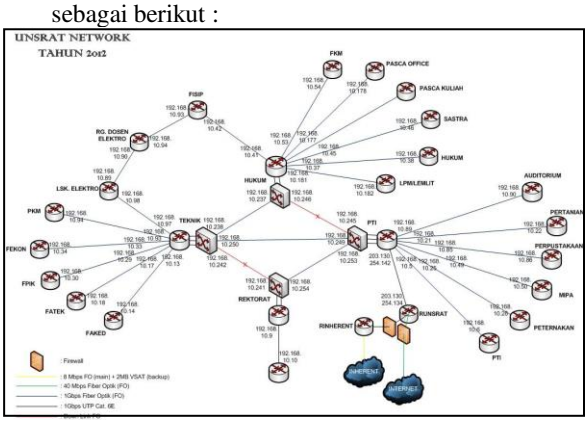



Gambar 6. Performa Protokol L2TP

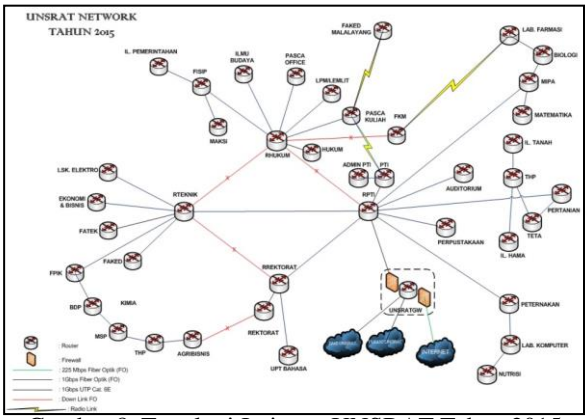
## III. METODOLOGI PENELITIAN

Prosedur penelitian pada pembuatan tugas akhir ini adalah mencari berbagai reference baik dari tempat yang dijadikan studi kasus dan berbagai tempat lain yang dapat mendukung argumen saya untuk membuat tugas akhir ini, kemudian setelah selesai menemukan permasalahan langkah selanjutnya adalah observasi terhadap tempat yang akan di jadikan studi kasus yaitu di gedung Pusat Teknologi Informasi Universitas Sam Ratulangi Manado.

Adapun data hasil observasi secara langsung di gedung Pusat Teknologi Informasi tersebut adalah sebagai berikut :

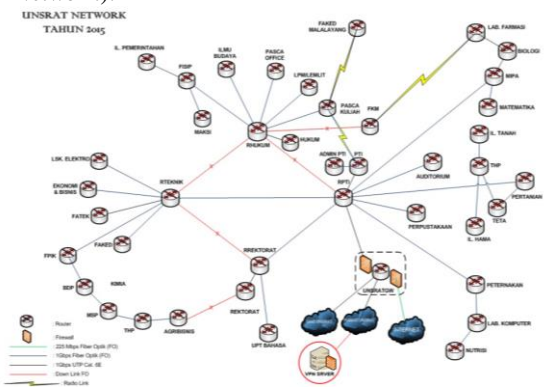



Gambar 7. Topologi Jaringan UNSRAT Tahun 2012




Gambar 8. Topologi Jaringan UNSRAT Tahun 2015 Sampai sekarang

Berdasarkan Topologi Jaringan di atas saya membuat sebuah tambahan Jaringan VPN (*Virtual Private Network*), dimana dengan adanya Jaringan tersebut lebih memudahkan dari segi penggunaan dan keamanan dalam mengakses beberapa situs lokal didalam Jaringan kampus Universitas Sam Ratulangi, dan berikut adalah gambaran Tolopologi Jaringan yang sudah terhubung dengan VPN (*Virtual Private Network*).




Gambar 9. Topologi Jaringan + VPN

Teknologi VPN tersebut terbagi atas dua bagian yaitu Perangkat Keras dan Perangkat lunak yang bekerja sama membentuk jaringan VPN

a. Perangkat Keras VPN

Perangkat keras yang digunakan pada pembuatan teknologi VPN ini adalah beberapa komputer sebagai server untuk memproses dan komputer client yang mengakses VPN tersebut seperti berikut :

- VPN *Server* adalah sebuah perangkat Jaringan yang menjalankan perangkat lunak *Server*. Fungsi fungsi utama pada VPN *Server* yaitu: menerima Request dari koneksi VPN, melakukan negosiasi kebutuhan koneksi dan parameter, melakukan autentikasi dan otorisasi pada VPN *Client*s, menerima data dari *Client* atau meneruskan request data yang dilakukan *Client*, serta berlaku sebagai titik akhir (end point) pada VPN tunnel dan koneksi.
- VPN *Client* adalah sebuah perangkat PC yang melakukan sebuah koneksi VPN pada Jaringan VPN *Server*, dan melakukan login pada sebuah Jaringan jarak jauh setelah diautentikasi pada VPN *Server*, yang kemudian dapat melakukan komunikasi.

b. Perangkat Lunak VPN

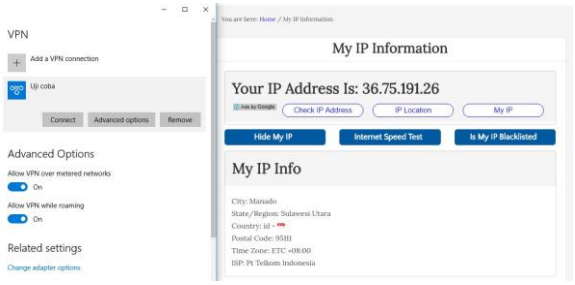
Perangkat Lunak *Virtual Private Network* adalah *Software* yang digunakan untuk dapat membuat Jaringan *Virtual Private Network* adapun jenis dari *Software* penyedia VPN seperti ZenVPN, Hide.meVPN, SurfEasy, Softether dan lain lain, khususnya pada pembuatan Tugas akhir ini *Software* VPN yang di gunakan adalah Software *Softether* karena Software tersebut dapat menangani berbagai jenis Protokol seperti Protokol PPTP ( *Point to Point Tunneling Protokol*), SSTP (*Secure Socket Tunnneling Protokol*), L2TP (*Layer Two Tunneling Protokol*), dan OpenVPN yang bersifat Open Source dan mudah dalam melakukan Konfigurasi serta jaminan keamanan pertukaran data dalam Jaringan *Softether*.

Selain itu dibutuhkan sebuah IP public. IP Public berfungsi sebagai alamat yang di gunakan oleh komputer client untuk mengakses server. IP Public terbagi atas dua jenis yaitu IP *Public Statis* dan IP *Public Dinamis*, dan pada pembuatan *Server* VPN ini saya menggunakan IP *Public Statis* karena dengan menggunakan IP *Public Statis* tidak perlu lagi mendaftarkan pada layanan DNS karena IP *Public Statis* adalah IP yang tidak akan berubah ubah sehingga memudahkan *Client* VPN untuk melakukan koneksi kedalam Jaringan VPN di Universitas Sam Ratulangi.

## IV. HASIL DAN PEMBAHASAN

Berdasarkan hasil dari prosedur penelitian yang dilakukan menghasilkan sebuah produk VPN Server yang dapat diakses menggunakan Jaringan internet, adapun produk tersebut dibuat dengan menggunakan beberapa bentuk Protokol yaitu Protokol SSTP dan Protokol L2TP, VPN Server berada di gedung Pusat Teknologi Informasi yang di berada di Universitas Sam Ratulangi, VPN Server tersebut berjalan di system Operasi Linux Ubuntu Server 16.04, dengan alamat IP Public (103.84.116.62). dan untuk dapat mengakses VPN Server tersebut Client harus mempunyai User dan Password yang sudah terdaftar pada VPN Server dan harus terkoneksi ke Jaringan internet.

Untuk menggunakan VPN ini dapat menggunakan perangkat apa saja dengan syarat terhubung dengan jaringan internet. Dan berikut adalah langkah – langkah yang harus dilakukan untuk dapat mengakses VPN Server menggunakan Personal Computer.




Gambar 10. Membangun Koneksi dengan VPN Server

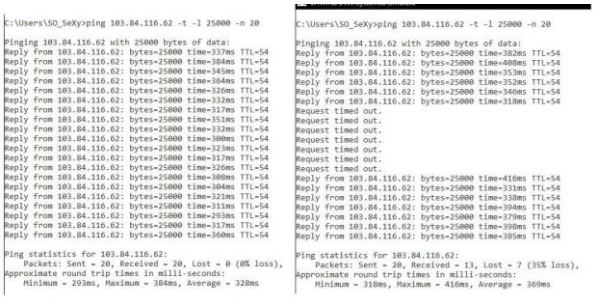
Adapun cara untuk menghubungkan komputer client dengan server VPN adalah dengan menekan tombol connect dan jika tidak ada masalah dengan server VPN dalam beberapa detik kita sudah dapat menikmati VPN tanpa ada perasaan takut jika data pribadi kita akan di culik oleh orang lain.

Selain itu terdapat juga beberapa uji coba yang dilakukan untuk menguji kelayakan dari VPN yang di bangun, pengujian terbagi atas beberapa jenis seperti berikut :

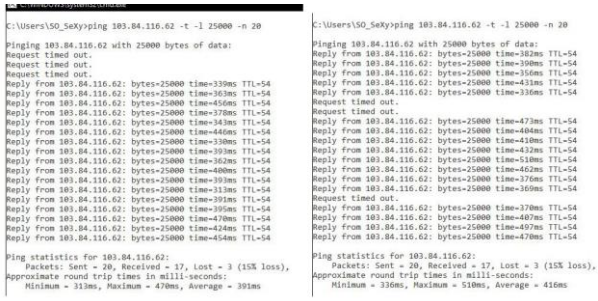
a. Pengujian *Packet Loss*

Pengujian *Packet Loss* ini bertujuan untuk melihat kemampuan dari *Server* VPN dalam mengirimkan dan Menerima Packet Data. Dan dalam pengujian ini saya mencoba melakukan pengiriman data sebesar 25000 byte dengan

20x tes dalam dua percobaan dan Protokol yang berbeda seperti gambar dibawah ini :




Gambar 11. Percobaan Ping ke Protokol L2TP




Gambar 12. Percobaan Ping ke Protokol SSTP

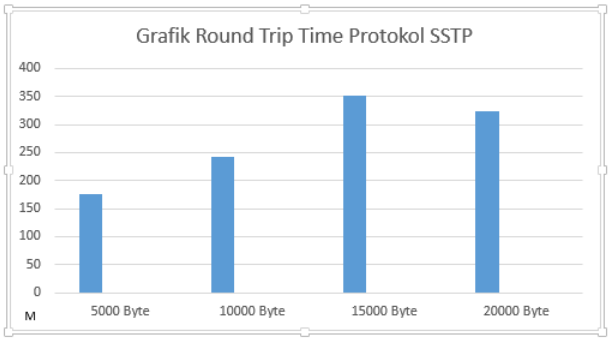
Berdasarkan data hasil percobaan diatas dapat diambil kesimpulan bahwa *Server* VPN dapat berjalan dengan baik dengan kondisi yang berbeda – beda tergantung kecepatan dan jumlah paket data yang dikirimkan dan berikut adalah table perbandingan dengan menggunakan dua Protokol pada percoaan diatas.

Table 1. Percobaan Packet Loss dengan Protokol SSTP dan L2TP

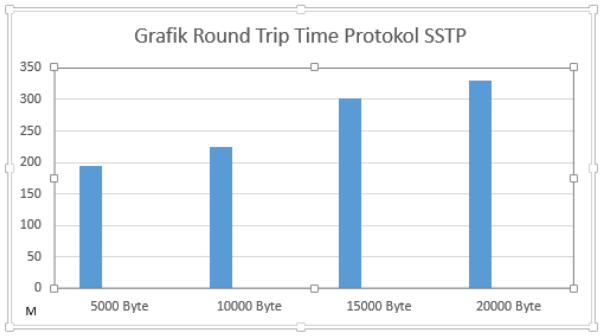
| Protokol | Bytes | Paket dikirim | Paket diterima | Packet Loss |
|---|---|---|---|---|
| SSTP Percobaan 1 | 25000 | 20 | 20 | 0 % |
| SSTP Percobaan 2 | 25000 | 20 | 13 | 35 % |
| L2TP Percobaan 1 | 25000 | 20 | 13 | 35 % |
| L2TP Percobaan 2 | 25000 | 20 | 13 | 35 % |

b. Percobaan Round Trip Time

Pengujian Round Trip Time ini bertujuan untuk menghitung rata rata dan maksimum waktu roundtrip pada VPN Server dengan menggunakan perintah ping dari komputer Client yang telah terhubung dengan Server VPN dan berikut adalah hasil percobaan Round Trip Time tersebut menggunakan beberapa jumlah data yang berbeda.




Gambar 13. Grafik Round Trip Time Protokol L2TP

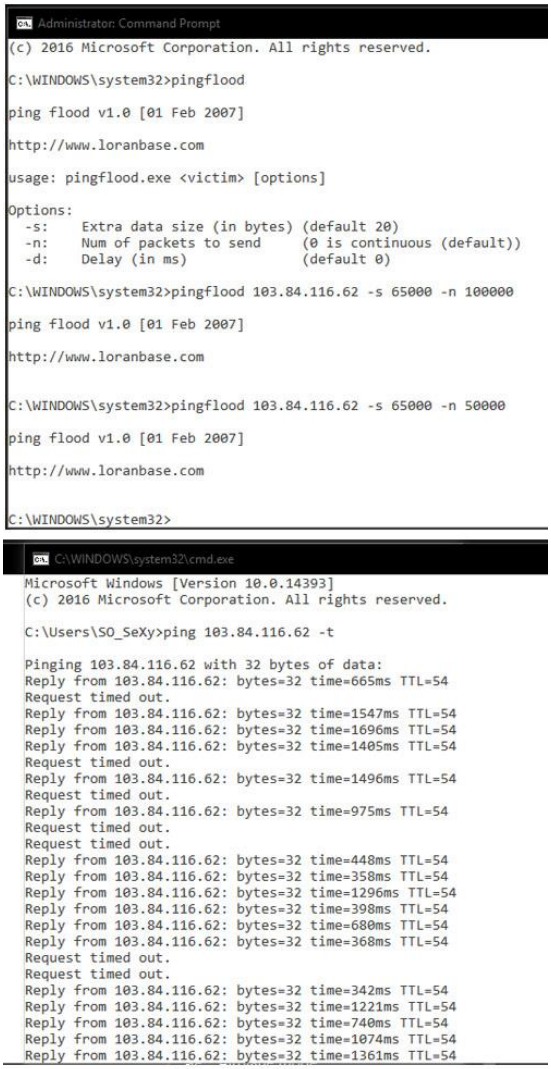



Gambar 14. Grafik Round Trip Time Protokol SSTP

Berdasarkan pengujian terhadap dua Protokol yang berbeda yaitu Protokol L2TP dan SSTP tidak terdapat perbedaan Round Trip Time yang sangat berbeda jauh, karena pada percobaan kedua Protokol tersebut waktu pengiriman data berada di antara 100ms sampai 300ms dan besar paket data yang dikirimkan juga akan mempengaruhi waktu pengiriman data.

c. Pengujian Attacking

Percobaan ini adalah percobaan Attacking dengan menggunakan Software Pingflood, pengujian ini bertujuan untuk menguji kemampuan *Server* saat menangani aktifitas user yang banyak dengan menggunakan *Server* VPN. Percobaan dilakukan menggunakan perintah Pingflood pada CMD diikuti dengan IP dari VPN Tersebut sekaligus parameter tambahan dan berikut adalah perintah yang digunakan untuk melakukan *Attacking* : ***pingflood 103.84.116.62 –s 65000 –n 50000*** dan berikut adalah gambar dari hasil percobaan tersebut.




Gambar 15. Percobaan Attacking dan tes ping

Berdasarkan percobaan diatas ternyata mempengaruhi kinerja *Server* yang mengakibatkan aktivitas *Server* menjadi lambat dan banyak terjadi Request Time Out saat melakukan percobaan tersebut.

## V. PENUTUP

a. Kesimpulan

Dari hasil penelitian yang di lakukan dapat diambil beberapa kesimpulan sebagai berikut :

1. Sistem yang dibuat telah berhasil di implementasikan secara langsung menggunakan Protokol SSTP dan L2TP di UPT Teknologi Informasi dan Komunikasi UNSRAT.
2. Berdasarkan pengujian *Packet Loss* pada kedua protokol bahwa *Packet Loss* tergantug pada jumlah data dan kecepatan koneksi internet. Semakin sedkit data yang dikirimkan dan kecepatan internet cepat maka data akan cepat sampai dengan aman menggunakan kedua protokol tersebut.

Berdasarkan pengujian *Round Trip Time* tidak terdapat perbedaan yang sangat berbeda jauh, karena pada percobaan dengan menggunakan kedua Protokol tersebut waktu pengiriman data berada di antara 100ms sampai 300ms untuk kedua protokol tersebut.

b. Saran

Pada pembuatan sistem ini tentunya masih memiliki banyak kekurangan untuk itu saya ingin memberikan beberapa saran untuk pengembangan sistem ini yaitu :

1. Sistem dapat dikembangkan dengan menggunakan spesifikasi yang lebih besar agar dapat melayani banyak client dalam waktu bersamaan.
2. Kedepan diharapkan sistem yang dibuat agar dapat diterapkan di Universitas Sam Ratulangi guna menunjang Manajemen Informasi Mahasiswa seperti akses sumber daya website internal UNSRAT, tidak lagi menggunakan jaringan publik tapi sudah menggunakan jaringan VPN Kampus.

Dapat mencoba menggunakan protokol VPN lain untuk perbandingan dari segi keamanan agar mendapatkan protokol yang terbaik yang akan di terapkan pada sistem VPN tersebut.

## DAFTAR REFERENSI


[1] Artondo. R.2011. *Analisa Dan Implementasi Ipv 6 Tunnel Broker Untuk Interkoneksi Antara Ipv6 Dan Ipv4*.Semarang: Jurnal teknik Elektro.

[2] Mikrotik. 2010. Interkoneksi Jaringan dengan L2TP+IPSec. Diambil dari: http://www.mikrotik.co.id/artikel_lihat.php?id=152 Diakses pada Bulan Februari 2017.

[3] Monoarfa. M.N.H. 2016. *Analisa dan Implementasi Network Intrusion Prevention System di Jaringan Universitas Sam Ratulangi*. Manado: Journal Teknik Elektro dan Komputer. Vol. 5, No. 4:36.

[4] Muslim. A.M. 2007. *Analisa Teknis Perbandingan Router Linux dengan Router Mikrotik pada Jaringan Wireless*, Semarang: Jurnal Teknologi Informasi DINAMIK. Vol. XII, No. 1:13-14.

[5] N. Karimi. (2013, Novermber 19). "*How To Setup a Multi-Protokol VPN Server Using SoftEther*" [online]. Available : https://www.digitalocean.com/community/tutorials/how-to-setup-a-multi-Protokol-vpn-*Server*-using-softether.

[6] Pribadi. T.P. 2013. *Implementasi High-Availability VPN Client Pada Jaringan Komputer Fakultas Hukum Universitas Udayana*.Bandung: Jurnal Ilmu Komputer. Vol. 6, No.1:21.

[6] Susanto.T.R., Indriyanta. G., dan Santosa. G.R. *Analisis Perbandingan Performa Point To Point Tunneling Protocol Dan Ethernet Over Internet Protocol Dalam Membentuk VPN*.Yogyakarta: Jurnal Informatika. Vol. 9, No.1:12-15.

[7] Sofana, Iwan. 2013. *Membangun Jaringan Komputer*. Bandung : Informatika.

[8] Syafrizal, Melwin. 2008. *Pengantar Jariangan Komputer*. Yogyakarta : Andi.

## SEKILAS TENTANG PENULIS

Saya bernama Arthur Farly Kaseger dan merupakan anak tunggal dari pasangan Bertie E Kaseger dan Jeanne B Manadagi, lahir di Manado pada tanggal 14 Februari 1995. Asal daerah Manado.

Saya mulai menempuh pendidikan di sekolah dasar SD Kristen Eben Haezar 02 (2000 -2006). Kemudian melanjutkan studi tingkat pertama di SMP Kristen Eben Haezar 01 (2006 - 2009) dan selanjutnya saya menempuh pendidikan tingkat atas di SMA Negeri 1 Manado (2009- 2012).

Setelah itu, di tahun 2012 saya melanjutkan pendidikan ke salah satu perguruan tinggi yang berada di Manado yaitu Universitas Sam Ratulangi Manado, dengan mengambil Program Studi S-1 Teknik Informatika di Jurusan Elektro Fakultas Teknik.