
ANALISIS PERBANDINGAN PERFORMA SSTP DAN PPTP PADA VPN

¹Deona Carol Gerjana Rijke Saijuna, ²Agustinus Rudatyo Himamunanto, S.Si, M.Kom,
³Jatmika, S.Si, M.Kom

Fakultas Sains dan Komputer, Universitas Kristen Immanuel

Jalan Solo Km. 11 PO Box 4 YKAP Yogyakarta, ph: (0274) 496256-296247 fax: (0274) 496258

e-mail: ¹dcgerjanas@student.ukrimuniversity.ac.id, ²rudatyo@ukrimuniversity.ac.id,

³jatmika@ukrimuniversity.ac.id

Abstract

VPN merupakan sebuah teknologi keamanan jaringan yang dapat dijadikan solusi keamanan informasi. VPN memungkinkan 2 atau lebih site yang berjauhan untuk dapat terhubung secara pribadi melalui jaringan public seperti internet. Untuk menerapkan VPN, diperlukan protokol SSTP (Secure Socket Tunneling Protocol) dan PPTP (Point to Point Tunneling Protocol) yang masing-masing memiliki pengaruh terhadap performa QoS (Quality of Service). Pada penelitian ini, dilakukan analisis perbandingan antara SSTP dan PPTP dengan membandingkan kinerja QoS. Pengujian dilakukan terhadap client yang terhubung ke router board dengan dua scenario jaringan, skenario pertama client mengakses web berbasis download dan skenario kedua client pada jaringan mengakses web streaming video. Tujuan dari penelitian ini adalah untuk mengetahui performa QoS, transfer & download file dari jaringan VPN yang menggunakan protokol SSTP dan PPTP. Hasil pengujian yang didapat dari penelitian ini menunjukkan bahwa PPTP lebih unggul pada parameter QoS dibanding dengan SSTP. Sedangkan hasil yang didapat dari pengujian FTP dan download menunjukkan bahwa SSTP lebih unggul pada kecepatan transfer file dan download jika dibandingkan dengan PPTP.

Kata Kunci : Virtual Private Network (VPN), Secure Socket Tunneling Protocol (SSTP), Point to Point Tunneling Protocol (PPTP)

Abstract

VPN is a network security technology that can be used as an information security solution. VPNs allow 2 or more distant sites to be able to connect privately through public networks such as the internet. To implement VPN, SSTP (Secure Socket Tunneling Protocol) and PPTP (Point to Point Tunneling Protocol) protocols are required, each of which has an influence on QoS (Quality of Service) performance. In this study, a comparative analysis was carried out between SSTP and PPTP by comparing QoS performance. Tests are carried out on clients connected to the router board with two network scenarios, the first scenario the client accesses the web based download and the second scenario the client on the network accesses web streaming video. The purpose of this study was to determine the performance of QoS, transfer & download files from VPN networks using SSTP and PPTP protocols. The test results obtained from this study indicate that PPTP is superior to the QoS parameters compared to SSTP. While the results obtained from FTP and download testing show that SSTP is superior in file and download transfer speeds compared to PPTP.

Keywords : Virtual Private Network (VPN), Secure Socket Tunneling Protocol (SSTP), Point to Point Tunneling Protocol (PPTP), Quality of Service (QoS)

1. PENDAHULUAN

Berdasarkan Laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) dari survei yang melibatkan 5.900 sampel selama periode Maret hingga 14 April 2019, sejumlah 64,8% (171,17) dari total penduduk Indonesia (264 juta jiwa) telah terhubung dengan jaringan internet. Angka tersebut bertumbuh 10,12%. Menurut wilayah geografisnya, Jawa merupakan daerah dengan pengguna internet terbesar, yakni 55%. Selanjutnya Sumatera 21%, Papua 10% dan Kalimantan 9%. Hal ini membuktikan bahwa internet banyak diminati oleh masyarakat luas dan akan semakin bertambah banyak setiap tahunnya (Pratomo, 2019).

Aktivitas – aktivitas yang dilakukan selama penggunaan internet tentulah sangat beresiko apabila informasi yang penting dan berharga dapat diakses oleh pihak yang tidak berkepentingan. Maka dari itu keamanan suatu jaringan sangatlah penting dalam pertukaran data antar *server* dan *client*.

Jika tingkat keamanan jaringan sangat rendah, maka dapat membuat jaringan sangat rentan terhadap serangan-serangan dari luar jaringan tersebut. Sebagai contoh yaitu serangan berupa pemalsuan identitas, pengiriman virus, pencurian data dan hal-hal merugikan lainnya. Oleh karena itu, keamanan menjadi poin penting dalam pembuatan sebuah jaringan (Rasuanda, 2019).

Salah satu cara untuk meminimalkan adanya serangan keamanan dari luar yaitu dengan memanfaatkan *Virtual Private Network (VPN)*. Pada penelitian ini, dilakukan analisis terhadap perbandingan penggunaan protokol SSTP dan PPTP dengan pemodelan jaringan VPN terhadap parameter QoS (*Quality of Service*) untuk dapat diketahui pengaruh penerapan protokol VPN terhadap QoS. Dengan QoS akan mempermudah menentukan perbandingan apa saja yang menjadi pertimbangan performa dari kedua protokol. Perbandingan yang digunakan untuk mengukur yaitu *Throughput*, *Delay*, *Packet Loss* dan *Jitter*. Selain itu, dilakukan juga perbandingan kecepatan transfer dan download file dari masing-masing protokol VPN.

2. LANDASAN TEORI

2.1 Metode Penelitian

Metode penelitian yang penulis terapkan sebagai penunjang pada penelitian ini antara lain :

2.1.1 Analisis

Analisis dilakukan terhadap kebutuhan perangkat penunjang, baik *hardware* (perangkat keras) maupun *software* (perangkat lunak) yang akan digunakan selama proses pembangunan jaringan berdasarkan pada teknologi dan metode yang telah ditetapkan, yaitu VPN SSTP dan PPTP.

2.1.2 Perancangan

Tahap ini merupakan tahap perancangan sistem jaringan dengan topologi yang akan digunakan untuk membangun jaringan VPN dengan metode SSTP dan PPTP. Perancangan dilakukan menggunakan software yang telah ditentukan pada tahap analisis.

2.1.3 Implementasi

Tahap Implementasi merupakan tahap dimana topologi yang telah dibuat diterapkan pada pembangunan sistem dengan cara melakukan setting, konfigurasi serta instalasi terhadap masing-masing perangkat sesuai spesifikasi desain yang telah dibuat sebelumnya.

2.1.4 Pengujian

Tahap pengujian bertujuan untuk melihat pengaruh QoS dari sistem jaringan VPN SSTP dan PPTP yang telah dibuat dalam melakukan komunikasi data. Pengujian pertama dilakukan terhadap konektivitas jaringan yang dipakai apakah dapat terkoneksi dengan client atau tidak. Kemudian

dilanjutkan dengan uji routing, pengujian Throughput, Delay, Packet Loss dan Jitter terhadap masing-masing protocol. Setelah itu, dilakukan pengujian FTP dan download file dari website.

2.1.5 Dokumentasi

Dokumentasi merupakan tahap setelah pengujian yang menyatakan bahwa implementasi dapat diterima dan sesuai dengan apa yang diharapkan.

2.2 Landasan Teori

Landasan teori yang digunakan dalam penelitian ini, yaitu:

2.2.1 Jaringan Komputer

Jaringan komputer adalah himpunan “interkoneksi” antara 2 komputer *autonomous* atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*). Bila sebuah komputer dapat membuat komputer lainnya *restart*, *shut down*, atau melakukan control lainnya, maka komputer-komputer tersebut bukan *autonomous* (tidak melakukan control terhadap komputer lain dengan akses penuh) [10].

2.2.3 Komponen Jaringan Komputer

Komponen jaringan komputer merupakan bagian utama yang perannya diperlukan untuk menginstal *software* guna membantu pembangunan jaringan komputer. Komponen jaringan terbagi menjadi beberapa bagian, yaitu perangkat komputer, kartu jaringan, media transmisi dan perangkat bantu jaringan. [20].

2.2.4 Internet

Internet merupakan jaringan terluas dalam sistem teknologi informasi yang memungkinkan perangkat di seluruh dunia untuk saling terhubung. Jaringan internet dapat diakses publik yang mengirimkan data menggunakan standar Protokol Internet (IP). Informasi yang tersebar di internet dapat diakses melalui jaringan world wide web (www) baik dalam bentuk teks, musik, foto, video, atau apa pun [9].

2.2.5 Virtual Private Network (VPN)

Virtual Private Network merupakan suatu cara untuk membuat sebuah jaringan bersifat private dan aman dengan memanfaatkan jaringan publik seperti internet. Data dalam jaringan tersebut tidak dapat diketahui oleh pengguna lain di jaringan publik karena data tersebut dilewatkan pada tunnel yang dibentuk oleh VPN. Tunnel merupakan suatu mekanisme enkripsi-deskripsi data. Data yang dikirim melalui jalur publik adalah data terenkripsi yang hanya bisa dibuka oleh ujung dari tunnel yang memiliki kunci untuk medeskripsi data tersebut. VPN menggunakan salah satu dari teknologi tunneling yang ada, yaitu: PPTP, SSTP, L2TP dan IPSec [21].

Konsep VPN

VPN membutuhkan sebuah server yang berfungsi sebagai penghubung antar PC yang dapat berupa komputer dengan aplikasi VPN Server atau sebuah Router. Komputer dengan aplikasi VPN client ini kemudian akan menghubungi VPN server yang akan melakukan verifikasi username dan password. Apabila berhasil, VPN server akan memberikan IP Address baru pada computer client dan koneksi/tunnel akan terbentuk. Jika digambarkan, konsep VPN dapat berwujud sebagai berikut :



Gambar 2.1 Konsep Kerja VPN

Tabel 2.1 Penilaian QoS berdasarkan TIPHON

Nilai	Presentase %	Indeks
3,8 - 4	95 - 100	Sangat Memuaskan
3 - 3,79	75 - 94,75	Memuaskan
2 - 2,99	50 - 74,75	Kurang Memuaskan
1 - 1,99	25 - 49,75	Jelek

(Sumber : TIPHON)

Throughput

Throughput yaitu kecepatan (rate) transfer data yang efektif yang diukur dalam bps. Throughput merupakan jumlah total kedatangan paket yang sukses yang diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut [5]. Untuk mengukur throughput, digunakan Persamaan (1).

$$\text{Throughput} = \frac{\text{Bytes}}{\text{Time Span}} \times 8$$

Menurut versi TIPHON, besarnya throughput dapat diklasifikasikan seperti yang ditunjukkan pada Tabel 2.2

Tabel 2.2 Standar Throughput oleh TIPHON

Kategori Throughput	Throughput	Indeks
<i>Bad</i>	0 - 338 kbps	0
<i>Poor</i>	338 - 700 kbps	1
<i>Fair</i>	700 - 1200 kbps	2
<i>Good</i>	1200 kbps - 2,1 Mbps	3
<i>Excelent</i>	> 2,1 Mbps	4

(Sumber : TIPHON)

Delay

Delay adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ketujuan. Delay dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama [19]. Menurut versi TIPHON, besarnya delay dapat diklasifikasikan seperti yang ditunjukkan pada Tabel 2.3

Tabel 2.3 Standar Delay oleh TIPHON

Kategori Latency	Besar Delay
Sangat bagus	< 150 ms
Bagus	150 s/d 300 ms
Sedang	300 s/d 450 ms
Jelek	> 450 ms

(Sumber : TIPHON)

Untuk mengukur delay digunakan Persamaan (2).

$$\text{Delay} = \frac{\text{Time2} - \text{Time1}}{\text{Total Paket yang dikirim} - 1}$$

Packet Loss

Packet Loss merupakan parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang, dapat terjadi karena collision dan congestion pada jaringan dan hal ini berpengaruh pada semua aplikasi karena retransmisi akan mengurangi efesiensi jaringan secara keseluruhan meskipun jumlah bandwidth cukup tersedia untuk aplikasi-aplikasi tersebut. Jika terjadi kongesti yang cukup lama, buffer akan penuh dan data baru tidak akan diterima [5]. Nilai Packet Loss sesuai dengan versi TIPHON ditunjukkan pada Tabel 2.4

Tabel 2. 4 Standar Packet Loss oleh TIPHON

Kategori Packet Loss	Packet Loss	Indeks
<i>Poor</i>	> 25%	1
<i>Medium</i>	12 - 24 %	2
<i>Good</i>	3 - 14 %	3
<i>Perfect</i>	0 - 2 %	4

(Sumber : TIPHON)

Untuk mengukur packet loss, digunakan Persamaan (3).

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

Jitter

Jitter merupakan kumpulan dari semua delay yang terjadi selama proses pengiriman data sampai dengan penerimaan data. Jika jitter mendekati nol maka kecepatan jaringan sangat cepat. Namun sebaliknya, jika tidak mendekati nol maka kecepatannya jelek dan akan terjadi kehilangan data dalam proses pengirimannya (packet loss). Untuk mengukur jitter, digunakan Persamaan (4).

$$\text{Jitter} = \frac{\text{Delay2} - \text{Delay1}}{\text{Total paket yang dikirim} - 1}$$

Menurut versi TIPHON, besarnya jitter dapat diklasifikasikan seperti yang ditunjukkan pada Tabel 2.5

Tabel 2.5 Kategori Jitter Standar TIPHON

Kategori Jitter	Jitter	Indeks
<i>Poor</i>	125 - 225 ms	1
<i>Medium</i>	75 - 125 ms	2
<i>Good</i>	0 - 75 ms	3
<i>Perfect</i>	0 ms	4

(Sumber : TIPHON)

2.2.8 WinSCP

WinSCP adalah sebuah aplikasi *open source* yang berfungsi sebagai SFTP dan FTP *client* untuk sistem operasi Windows. SCP *protocol* juga telah didukung oleh aplikasi WinSCP ini. Fungsi utama dari WinSCP yaitu menyalin file/transfer file antar komputer local dan remote secara aman. Pada umumnya aplikasi ini digunakan untuk mentransfer file dari komputer local (*client*) ke komputer remote (*server*). Manfaat dari WinSCP adalah pengguna tidak perlu repot-repot lagi memakai usb jika akan mentransfer file, cukup memanggil IP komputer remote saja [21].

2.2.9 Wireshark

Wireshark adalah salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network Administrator untuk menganalisa kinerja jaringannya dan mengontrol lalu lintas data di jaringan yang Anda kelola. Wireshark menggunakan interface yang menggunakan Graphical User Interface (GUI).

2.2.10 Standarisasi ETSI TIPHON

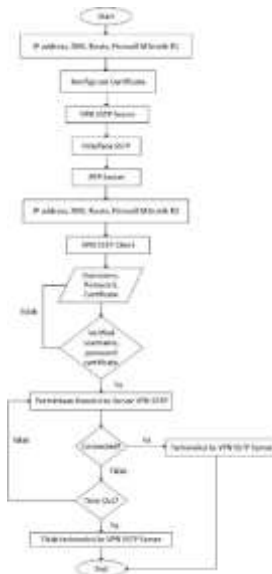
TIPHON (Telecommunications and Internet Protocol. Harmonization Over Network) merupakan standar penilaian parameter QOS yang dikeluarkan oleh badan standarisasi ETSI (European Telecommunications Standards Institute) [15]. ETSI (European Telecommunication Standards Institute) merupakan sebuah organisasi eropa yang didirikan pada tahun 1988 dan bertanggung jawab untuk pembentukan standar telekomunikasi teknik, ETSI menghasilkan European Telecommunication Standards (ETS) untuk anggotanya, yang terdiri dari operator jaringan, produsen PTT, pengguna, dan Lembaga penelitian. [9]

2.3 Perancangan Sistem

Bagian perancangan berisi penjelasan tentang bagaimana sistem jaringan VPN SSTP dan PPTP dirancang. Mulai dari perancangan skema sistem jaringan, desain topologi yang akan digunakan selama proses pembangunan sistem jaringan, hingga analisis kebutuhan.

2.3.1 Skema Sistem Jaringan VPN SSTP

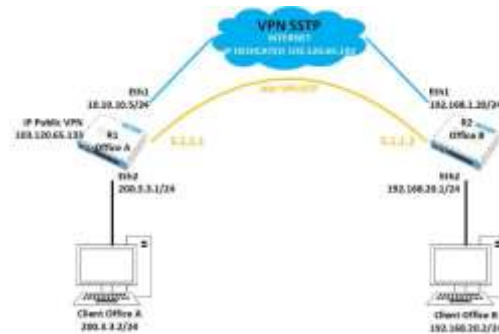
Flowchart sistem jaringan VPN SSTP dapat dilihat pada gambar dibawah ini.



Gambar 2.4 Flowchart VPN SSTP

Desain Sistem Jaringan VPN SSTP

Desain sistem jaringan VPN SSTP dibuat dengan menggunakan software Microsoft Visio 2016 menimbang cara penggunaannya yang mudah, tools-tools yang mudah dipahami, dan lain sebagainya. Topologi dari desain yang dihasilkan meliputi perangkat-perangkat seperti komputer, laptop, router dan jalur routing.



Gambar 2.5 Topologi VPN SSTP

Analisis Kebutuhan Sistem Jaringan VPN SSTP

Kebutuhan sistem jaringan VPN SSTP terbagi menjadi dua, yaitu kebutuhan *hardware* dan *software*. *Hardware* (perangkat keras) yang dibutuhkan untuk membangun sistem jaringan VPN SSTP, yaitu :

- 2 unit laptop, sebagai laptop yang digunakan untuk melakukan konfigurasi R1 Office A (server) dan R2 Office B (client).
- 2 unit Router Board menggunakan Router Board MikroTik RB941-2nd hAP lite, yang diperuntukkan sebagai server SSTP dan client SSTP.
- Kabel UTP, sebagai media transmisi pada jalur LAN.

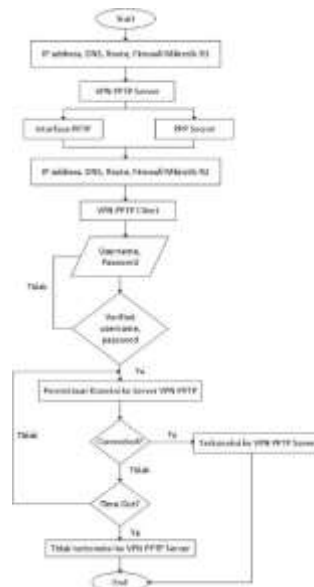
Software (perangkat lunak) yang dibutuhkan untuk membangun sistem jaringan VPN SSTP, yaitu :

- Visio 2016, untuk mendesain topologi dan flowchart sistem jaringan.
- Notepad++ v7.5.9 (64-bit), untuk merancang script.
- Winbox 3.18, untuk melakukan seluruh konfigurasi sistem jaringan VPN SSTP.
- Command Prompt, untuk melakukan tes koneksi antar perangkat yang telah dikonfigurasi.

- Wireshark, untuk melakukan pengujian terhadap sistem jaringan berdasarkan parameter yang telah ditentukan.
- WinSCP, untuk melakukan pengujian FTP antara client dan server.

2.3.2 Skema Sistem Jaringan VPN PPTP

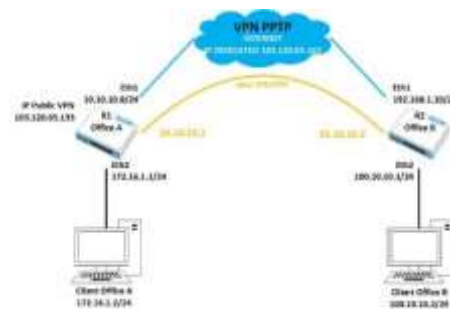
Flowchart sistem jaringan VPN PPTP dapat dilihat pada gambar berikut ini.



Gambar 2.6 Flowchart VPN PPTP

Desain Sistem Jaringan VPN PPTP

Desain sistem jaringan VPN PPTP dibuat dengan menggunakan software Microsoft Visio 2016 menimbang cara penggunaannya yang mudah, tools-tools yang mudah dipahami, dan lain sebagainya. Topologi dari desain yang dihasilkan meliputi perangkat-perangkat seperti komputer, laptop, router dan jalur routing.



Gambar 2.7 Topologi VPN PPTP

Analisis Kebutuhan Sistem Jaringan VPN PPTP

Kebutuhan sistem jaringan VPN PPTP terbagi menjadi dua, yaitu kebutuhan *hardware* dan *software*. *Hardware* (perangkat keras) yang dibutuhkan untuk membangun sistem jaringan VPN PPTP, yaitu :

- 2 unit laptop, sebagai laptop yang digunakan untuk melakukan konfigurasi R1 Office A (server) dan R2 Office B (client).
- 2 unit Router Board menggunakan Router Board MikroTik RB941-2nd hAP lite, yang diperuntukkan sebagai server PPTP dan client PPTP.
- Kabel UTP, sebagai media transmisi pada jalur LAN

Software (perangkat lunak) yang dibutuhkan untuk membangun sistem jaringan VPN SSTP, yaitu :

- Visio 2016, untuk mendesain topologi dan flowchart sistem jaringan.
- Notepad++ v7.5.9 (64-bit), untuk merancang script.
- Winbox 3.18, untuk melakukan seluruh konfigurasi sistem jaringan VPN PPTP.
- Command Prom p, untuk melakukan tes koneksi antar perangkat yang telah dikonfigurasi.
- Wireshark, untuk melakukan pengujian terhadap sistem jaringan berdasarkan parameter yang telah ditentukan.
- WinSCP, untuk melakukan pengujian FTP antara client dan server.

3. HASIL DAN PEMBAHASAN

3.1 Implementasi

Pada bagian ini menjelaskan mengenai implementasi dari perancangan sistem jaringan yang telah dibuat sebelumnya. Konfigurasi dilakukan secara bertahap mulai dari konfigurasi pada Router Office A untuk *server* VPN SSTP, kemudian dilanjutkan dengan konfigurasi pada Router Office B untuk *client* VPN SSTP, begitu juga dengan konfigurasi pada *Router Board* yang digunakan untuk sistem jaringan VPN PPTP.

3.1.1 VPN SSTP

Tahap implementasi VPN SSTP meliputi pembangunan SSTP server dan client. Baik server dan client harus memiliki certificate yang bertujuan untuk autentifikasi. Pada kedua sisi, dilakukan manajerial jaringan agar router server dan router client dapat berkomunikasi melalui tunnel VPN.

- Implementasi sistem jaringan VPN SSTP dilakukan dengan tahapan sebagai berikut :
- Konfigurasi ip address, DNS, Gateway dan NAT pada R1 Office A (server VPN SSTP).
- Mengatur NTP (Network Time Protocol) pada router server untuk menyesuaikan (sinkronasi) waktu antara server dan client.
- Pembuatan interface untuk client VPN SSTP.
- Penambahan IP public VPN.
- Pembuatan certificate (CA certificate, server certificate dan client certificate).
- Sign semua certificate yang telah dibuat sebelumnya.
- Pembuatan interface untuk server VPN SSTP.
- Pembuatan secret VPN SSTP.
- Konfigurasi ip address, DNS, Gateway dan NAT pada R1 Office A (server VPN SSTP).

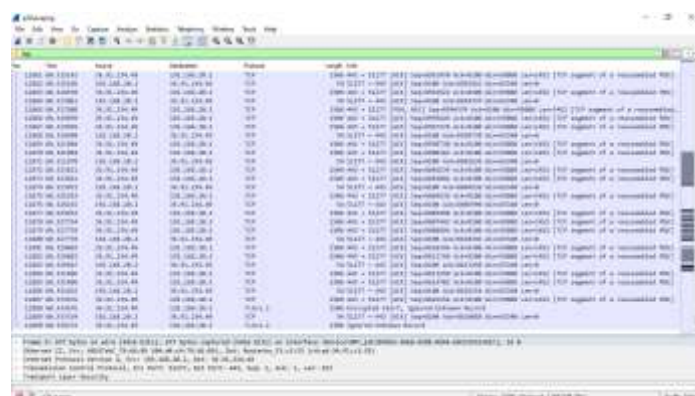
3.1.2 VPN PPTP

Tahap implementasi VPN PPTP meliputi pembangunan PPTP server dan client. Baik server dan client harus memiliki certificate yang bertujuan untuk autentifikasi. Pada kedua sisi, dilakukan manajerial jaringan agar memungkinkan komunikasi router server dan router client melalui tunnel VPN. Implementasi sistem jaringan VPN PPTP dilakukan secara simulasi dengan tahapan sebagai berikut :

- Konfigurasi ip address, DNS, Gateway dan NAT pada R1 Office A (server VPN PPTP).
- Mengatur NTP (Network Time Protocol) pada router server untuk menyesuaikan (sinkronasi) waktu antara server dan client.
- Pembuatan interface untuk client VPN PPTP.
- Penambahan IP public VPN.
- Pembuatan interface untuk server VPN PPTP.
- Pembuatan secret VPN PPTP.
- Konfigurasi ip address, DNS, Gateway dan NAT pada R2 Office B (client VPN PPTP).
- Mengatur NTP (Network Time Protocol) pada router client untuk menyesuaikan (sinkronasi) waktu antara server dan client.
- Connect-to IP public server VPN PPTP.

3.2 Pengujian Parameter QoS

Pengujian QoS VPN SSTP dilakukan pada PC client yang meliputi pengujian terhadap throughput, delay, packet loss dan jitter selama proses streaming menggunakan tools Wireshark. Pengujian dilakukan sebanyak 30 kali dengan lama waktu masing-masing 60 detik (1 menit) per 1 kali pengujian. Langkah-langkahnya yaitu, buka aplikasi Wireshark, lalu klik tombol start (tombol dengan sirip hiu berwarna biru). Setelah 60 detik, klik tombol stop (tombol dengan icon kotak merah). Kemudian, ketik “tcp” pada addressbar hingga berubah warna menjadi hijau (tanda bahwa perintah yang diketikkan adalah benar), lalu tekan tombol “Enter” hingga muncul data tcp seperti pada gambar dibawah ini.



Gambar 3.1 Data Pengujian dari Wireshark

Langkah selanjutnya yaitu klik menu “Statistics” > “Capture File Properties” atau bisa juga dengan cara Ctrl+Alt+Shift+C hingga muncul *capture* seperti pada gambar dibawah ini.



Gambar 3.2 Capture File Properties Data Pengujian

Setelah itu, lakukan perhitungan besaran *throughput* menggunakan persamaan 1, *delay* menggunakan persamaan 2, *packet loss* menggunakan persamaan 3 dan *jitter* menggunakan persamaan 4 yang telah dijabarkan pada BAB II untuk pengujian 1 – 30. Kemudian, hitung rata-ratanya untuk dibandingkan hasil antara VPN SSTP dan VPN PPTP.

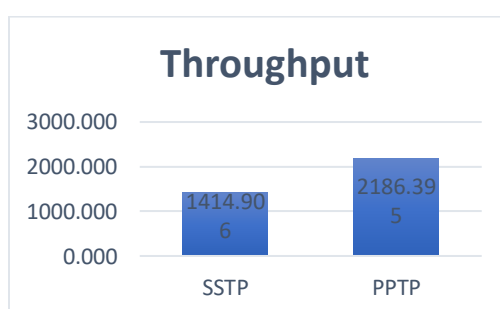
Hasil perhitungan rata-rata dari pengujian parameter QoS dapat dilihat pada tabel berikut ini.

Tabel 3.1 Perbandingan QoS VPN SSTP dan PPTP

PENGUJIAN	PROTOCOL							
	SSTP				PPTP			
	THROUGHPUT	DELAY	PACKET LOSS	JITTER	THROUGHPUT	DELAY	PACKET LOSS	JITTER
P1	2657.843	4.525	0.82%	4.525	897.999	7.004	0.000%	11.646
P2	1130.805	7.303	0.38%	7.303	5578.765	0.884	0.000%	1.748
P3	1350.957	59.163	0.36%	110.374	1500.028	4.414	0.008%	8.725
P4	1688.758	4.705	0.37%	8.896	3566.572	1.703	0.000%	3.349
P5	804.838	9.303	1.41%	18.160	2180.352	2.700	0.000%	5.170

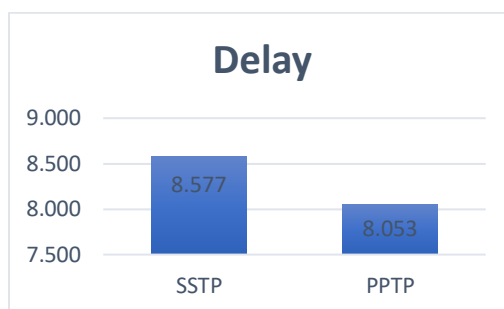
P6	2548.119	2.564	0.60%	4.640	5853.075	0.924	0.000%	1.812
P7	1580.666	4.948	0.75%	9.281	564.839	11.278	0.000%	22.288
P8	1448.950	4.529	1.75%	8.487	3613.326	1.591	0.000%	3.126
P9	1238.766	6.270	0.70%	12.139	3956.998	1.229	0.000%	2.429
P10	1168.531	6.548	0.50%	12.783	4039.188	1.396	0.003%	2.728
P11	523.600	14.042	0.68%	27.686	4459.404	1.571	0.000%	3.093
P12	2622.873	2.750	0.94%	5.111	463.711	13.025	0.492%	21.000
P13	1125.399	6.248	0.66%	12.205	5536.833	0.956	0.034%	1.856
P14	852.291	9.223	0.25%	18.049	545.418	11.884	1.322%	19.867
P15	1005.750	8.063	0.19%	15.849	147.230	36.442	0.376%	57.580
P16	1106.329	6.515	0.87%	12.574	2972.528	1.314	0.000%	2.594
P17	1798.095	4.380	0.58%	8.493	1219.696	6.232	0.012%	12.255
P18	1499.096	4.967	0.97%	9.619	2447.966	2.931	0.000%	5.756
P19	1928.854	4.045	0.70%	7.868	3299.484	2.312	0.016%	4.296
P20	1136.824	6.792	0.50%	13.190	431.608	12.011	0.031%	23.373
P21	1543.663	5.132	0.66%	9.524	68.094	60.615	0.004%	118.026
P22	258.751	24.312	0.82%	47.950	411.753	15.172	0.000%	29.843
P23	2547.960	2.811	0.74%	5.058	812.210	8.162	0.000%	14.094
P24	677.226	11.013	0.74%	21.287	691.112	9.162	0.053%	17.518
P25	832.798	9.728	0.10%	18.656	1675.045	4.482	0.000%	8.836
P26	1092.670	6.882	0.68%	13.228	1628.589	4.915	0.000%	9.607
P27	1770.080	4.521	0.17%	8.749	1432.794	4.513	0.000%	8.878
P28	1498.696	4.997	0.94%	9.623	1472.834	4.368	0.000%	8.392
P29	1870.385	4.287	0.57%	8.183	3106.340	2.056	0.000%	4.012
P30	1137.608	6.756	0.29%	12.746	1018.066	6.344	1.874%	12.326
Total	42447.181	257.323	19.69%	482.237	65591.856	241.591	0.141%	446.221
Rata-Rata	1414.906	8.577	0.66%	16.075	2186.395	8.053	0.141%	14.874

Grafik perbandingan rata-rata parameter QoS VPN SSTP dan PPTP dapat dilihat pada gambar-gambar berikut ini.



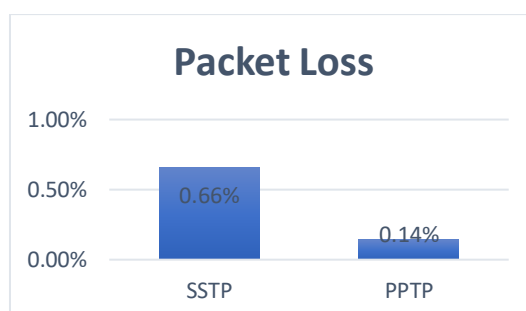
Gambar 3.3 Grafik Perbandingan Throughput VPN SSTP & PPTP

Kondisi throughput dari masing-masing protokol menunjukkan perbedaan yang cukup signifikan, yakni SSTP 1414.906 kbps atau masuk dalam indeks 3 (Good), sedangkan PPTP 2186.395 kbps atau masuk dalam indeks 4 (Excellent). Hal ini menunjukkan bahwa throughput PPTP lebih baik dibandingkan dengan throughput SSTP karena throughput PPTP lebih besar.



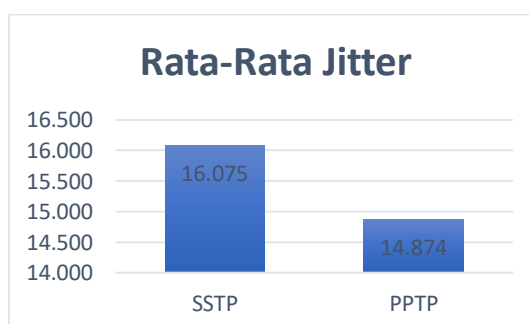
Gambar 3.4 Grafik Perbandingan Delay VPN SSTP & PPTP

Berdasarkan grafik perbedaan rata-rata delay yang ditunjukkan pada Gambar 4.36, nilai rata-rata delay dari SSTP berjumlah 8.577 ms, sedangkan nilai rata-rata delay dari PPTP berjumlah 8.053ms. Keduanya masuk dalam kategori latency “Sangat Bagus”. Maka, dapat diketahui bahwa delay dari PPTP lebih baik dibanding SSTP karena nilai delay PPTP lebih kecil.



Gambar 3.5 Grafik Perbandingan Packet Loss VPN SSTP & PPTP

Berdasarkan grafik perbedaan rata-rata packet loss yang ditunjukkan pada Gambar 4.38, keduanya masuk dalam indeks 4, yaitu perfect. Nilai packet loss dari SSTP adalah sebanyak 0.66%, sedangkan nilai packet loss dari PPTP sebanyak 0.14%. Hal ini berarti packet loss PPTP lebih baik dibanding SSTP karena nilai packet loss PPTP lebih kecil.



Gambar 3.6 Grafik Perbandingan Jitter VPN STTP & PPTP

Kondisi jitter dari masing-masing protokol menunjukkan perbedaan yang tidak terlalu signifikan, keduanya masuk kedalam indeks 3, yaitu Good dengan nilai SSTP 16.075ms, sedangkan PPTP 14.874ms. Hal ini berarti PPTP lebih baik dibandingkan dengan SSTP.

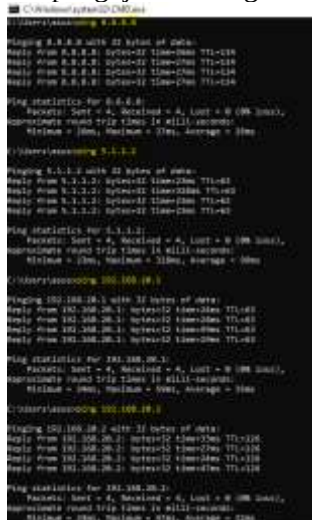
Berdasarkan analisis perbandingan yang telah dijabarkan sebelumnya, dapat diambil rangkuman analisis perbandingan QoS yang ditunjukkan pada tabel berikut ini:

Tabel 3.2 Hasil Perbandingan Performa QoS

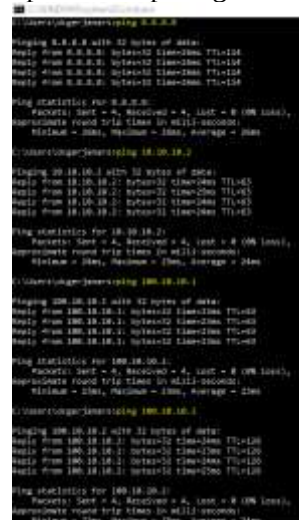
Parameter	Protokol	
	SSTP	PPTP
Throughput	-	Lebih Baik
Delay	-	Lebih Baik
Packet loss	-	Lebih Baik
Jitter	-	Lebih Baik

3.3 Pengujian Routing

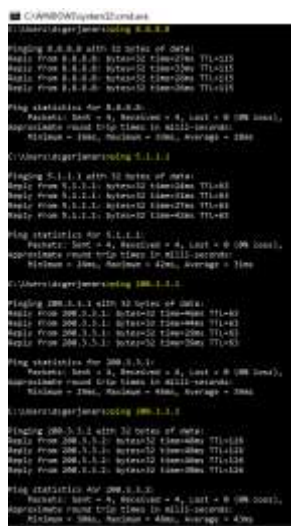
Hasil pengujian routing antar client VPN SSTP dan PPTP dapat dilihat pada gambar berikut ini.



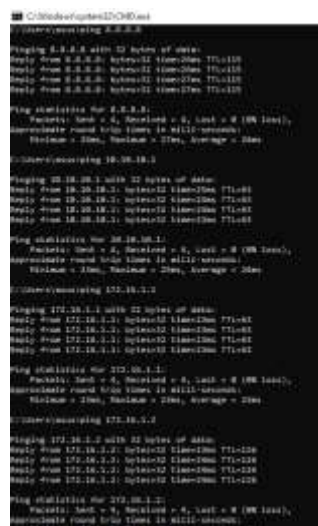
Gambar 3.7 Uji Routing client Office A ke Office B VPN SSTP



Gambar 3.9 Uji Routing client Office A ke Office B VPN PPTP



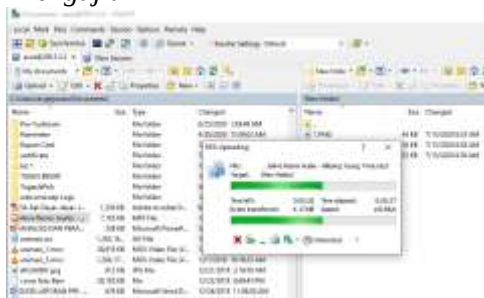
Gambar 3.8 Uji Routing client Office B ke Office A VPN SSTP



Gambar 3.10 Uji Routing client Office B ke Office A VPN PPTP

Dari keempat gambar diatas, dapat kita lihat bahwa routing antar *client* baik dari VPN SSTP maupun VPN PPTP berhasil, karena semua *ping* mendapat *reply*.

3.4 Pengujian FTP



Gambar 3. 11 Pengujian FTP VPN SSTP



Gambar 3. 12 Pengujian FTP VPN PPTP

Hasil pengujian menunjukkan bahwa VPN SSTP lebih unggul dibanding VPN PPTP pada pengujian FTP. VPN SSTP dengan kecepatan 142 KB/s, sedangkan VPN PPTP dengan kecepatan 131 KB/s.

3.5 Pengujian Download



Gambar 3.13 Pengujian Download VPN SSTP



Gambar 3.14 Pengujian Download VPN SSTP

Hasil pengujian menunjukkan bahwa VPN SSTP lebih unggul pada pengujian download dibanding dengan VPN PPTP. Nilai kecepatan download dari VPN SSTP yaitu sebesar 248 KB/dtk, sedangkan VPN PPTP sebesar 169 KB/dtk.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan selama perancangan sampai analisis perbandingan dari VPN SSTP dan PPTP, maka dapat ditarik kesimpulan sebagai berikut :

1. PPTP lebih unggul dibandingkan dengan SSTP pada performa QoS VPN.
2. SSTP lebih unggul dibandingkan dengan PPTP pada pengujian transfer file & download.
3. Berdasarkan penerapannya, konfigurasi VPN SSTP memiliki tingkat kerumitan yang lebih tinggi dibandingkan dengan VPN PPTP.

4.2 Saran

Peneliti berharap penelitian ini dapat dijadikan suatu referensi untuk lebih mengembangkan performansi jaringan VPN. Sebab, masih banyak yang perlu dianalisa dari jaringan VPN, terkhususnya metode PPTP, L2TP, SSTP dan IPSec, baik dari sisi transmisi data, tingkat keamanan serta hal lain sebagainya yang dapat mempengaruhi performansi jaringan VPN.

DAFTAR PUSTAKA

- [1] Afrianto and E. B. Setiawan. 2011. Kajian Virtual Private Network (VPN) Sebagai Sistem Pengamanan Data Pada Jaringan Komputer, Maj. Ilm. UNIKOM, Vol. 12, No.1
- [2] Aria, Y. 2018. Aplikasi Komunikasi Socket Client-Server Layanan Kamar Hotel Berbasis Android Pada Jaringan Lokal Menggunakan TCP/IP. Diploma thesis, STMIK AKAKOM, Yogyakarta.
- [3] Budiadji. 2009. Simulasi Untuk Membandingkan Kinerja PPTP dan L2TP untuk Berbagai Kelas Trafik, Depok. Depok: Universitas Indonesia.
- [4] Cnnindonesia.com. 2019. Mengenal Sejarah Internet, (Online), (<https://www.cnnindonesia.com/teknologi/20190312125646-185-376484/mengenal-sejarah-internet>, diakses tanggal 15 Oktober 2019).
- [5] Iskandar. 2015. Analisa Quality of Service (QoS) Jaringan Internet Kampus (Studi Kasus: UIN Suska Riau), UIN Suska Riau.
- [6] J. B. R. Lawas, A. C. Vivero and A. Sharma. 2016. Network Performance Evaluation of VPN Protocols (SSTP and IKEv2), Department of Computing National Technology Institute, Vols. -, no. -, pp. -, -.
- [7] K. A. Yoga. 2018. Konfigurasi VPN PPTP Pada MIKROTIK. (http://www.mikrotik.co.id/artikel_lihat.php?id=43, diakses tanggal 21 Juni 2020).
- [8] Mariana, N. 2009. Pemanfaatan Perangkat Lunak PC2 Untuk Sistem Otomatisasi Ujian Praktek (Studi Kasus Pada Mata Kuliah Bahasa Pemrograman Di Universitas Stikubank Semarang). Jurnal Dinamika Informatika, Vol.1, No.1. hh. 22.
- [9] Nancy, Y. 2019. Pengertian fungsi perbedaan internet intranet dan ekstranet : (<https://tirto.id/pengertian-fungsi-perbedaan-internet-intranet-dan-ekstranet-ely8>, diakses 08 Mei 2020).
- [10] Pratomo, Gito Yudha. 2019. APJII: Jumlah Pengguna Internet di Indonesia Tembus 171 Juta Jiwa. Dikutip 14 Juni 2020 : (<https://tekno.kompas.com/read/2019/05/16/03260037/apjii-jumlah-pengguna-internet-di-indonesia-tembus-171-juta-jiwa>, diakses tanggal 24 April 2020).
- [11] P.P. Romadhon. 2014. Analisis Kinerja Jaringan Wireless LAN Menggunakan Metode Qos Dan RMA Pada PT. Pertamina Ep Ubep Ramba (Persero). Skripsi. Palembang: Ilmu Komputer Universitas Bina Darma.
- [12] Putri T.U, dkk. 2013. Analisis Infrastruktur Jaringan Wireless Local Area Network (WLAN) Pada PSTA Lapan Bandung. Universitas Bina Darma, Palembang
- [13] Rasuanda, Moezes. 2019. Perbandingan Performa VPN Menggunakan PPTP dan SSTP Over SSL Dengan Metode Quality of Service. Undergraduate thesis, Universitas Internasional Batam.
- [14] R. Pahlevi. 2017. Analisis Dan Pengembangan Jaringan Internet Di SMK Negeri 3 Oku Kota Baturaja Menggunakan Metode Top Down. Skripsi, Palembang: Ilmu Komputer Universitas Bina Darma.
- [15] Suhervan. 2010. Analisis Penerapan QOS (Quality Of Service) pada jaringan fram Relay Menggunakan Cisco Router. Jakarta: Universitas Esa Unggul.
- [16] Syafrizal, M. 2005. Pengantar Jaringan Komputer. STMIK AMIKOM. Yogyakarta: Penerbit Andi.
- [17] Tommy. 2015. Perbandingan Metode PPTP, L2TP, SSL dan SSTP Pada Mikrotik sebagai Upaya Optimalisasi Layanan Jaringan Pada Fakultas Teknik Universitas Tanjungpura. Pontianak: Universitas Tanjungpura.
- [18] Wagito. 2005. Jaringan Komputer Teori dan implementasi Berbasis Linux. Yogyakarta: Penerbit GAVA MEDIA.
- [19] Yasin K. 2018. Ap aitu FTP dan Bagaimana Cara Menggunakan FTP?, (Online), (<https://www.niagahoster.co.id/blog/apa-itu-ftp/>, diakses tanggal 10 juli 2020).
- [20] Zainuddin, Z. 2006. Pola Pemanfaatan Internet oleh Mahasiswa Program Magister Ilmu Hukum Program Pascasarjana Universitas Sumatera Utara. Jurnal Studi Perpustakaan dan Informasi, vol.2, No.1. hh. 38
- [21] Zamalia, dkk. 2018. Analisis Perbandingan Performa Qos, Pptp, L2tp, Sstp Dan Ipsec Pada Jaringan Vpn Menggunakan Mikrotik. Universitas Halu Oleo. Kendari.