ANALISA QOS PADA JARINGAN SITE TO SITE VPN MENGGUNAKAN PROTOCOL SSTP

Raisul Azhar
STMIK Bumigora Mataram
[1]raisul_azhar@yahoo.co.id/raisul264@gmail.com

Abstrak

VPN (*Virtual Private Network*) merupakan teknologi yang memungkinkan terbentuknya sebuah jaringan data *private* pada jaringan publik dengan menerapkan autentikasi dan enkripsi sehingga akses terhadap jaringan tersebut hanya dapat dilakukan oleh pihak-pihak tertentu. Pada VPN terdapat banyak protokol untuk mendukung keamanan data. Salah satu protokol yang dipergunakan untuk kebutuhan tersebut adalah SSTP (*Secure Socket Tunneling Protocol*). Penerapan teknologi VPN pada jaringan menyebabkan dua atau lebih tempat yang berjauhan lokasi dapat terintergrasi atau bertukar infomasi dengan lebih aman dikarenakan mempergunakan jalur private yang terbentuk. Penelitian ini mengadopsi sebagian metodologi NDLC *(Network Development Live Cycle*) yaitu terdiri dari analysis, design dan simulation prototype. Fokus penelitian adalah mengamati pengaruh kualitas layanan/ QoS pada jaringan VPN terutama terhadap parameter delay, packet loss dan throughput ketika tiga buah type file yang dikirimkan melewati jaringan VPN dengan type dan ukuran yang berbeda. Berdasarkan tiga parameter tersebut hasil penelitian menunjukkan bahwa jaringan yang menerapkan *site-to-site* VPN protocol terutama menggunakan SSTP memiliki kualitas layanan dan keamanan yang lebih baik dibandingankan dengan jaringan Non VPN.

Kata Kunci : *VPN, SSTP, QOS, Mikrotik, Jaringan Komputer*

I. PENDAHULUAN

Dengan semakin berkembangnya teknologi mengakibatkan kebutuhan akan jaringan komunikasi semakin meningkat. Pertukaran data yang pada awalnya hanya melalui *hard copy* berupa tulisan tangan, dokumen, laporan bulanan dan sebagainya, saat ini telah berkembang menjadi komunikasi menggunakan jaringan internet karena tuntutan waktu dan efisien. Komunikasi data melalui jaringan internet mengakibatkan masalah kecepatan transfer dan keamanan. Hal yang harus diperhatikan dalam melakukan kegiatan di dunia internet adalah dengan semakin banyak orang yang berusaha menyadap data-data yang lalu-lalang dan kejahatan lainny di internet. VPN merupakan teknologi yang memungkinkan terbentuknya sebuah jaringan data *private* pada jaringan publik dengan menerapkan autentikasi dan enkripsi sehingga akses terhadap jaringan tersebut hanya dapat dilakukan oleh pihak-pihak tertentu. Pada VPN terdapat banyak protokol untuk mendukung keamanan data. Salah satu protokol yang dapat digunakan untuk pengembangan VPN adalah SSTP (*Secure Socket Tunneling Protocol)*

Virtual Private Network merupakan suatu cara untuk mensimulasikan jaringan pribadi ke jaringan publik, seperti internet. Disebut "*virtual*" karena bergantung pada penggunaan *virtual* yaitu koneksi, koneksi sementara yang tidak memiliki kehadiran fisik secara nyata, tetapi terdiri dari paket diarahkan melalui variasi mesin di internet secara ad-hoc [7]. Adapun fungsi utama yang dimiliki *Virtual Private Network*(VPN) yaitu:

Confidentially

Teknologi VPN mempunyai sistem kerja mengenkripsi semua data yang lewat melaluinya.Dengan adanya teknologi *enkripsi*, maka kerahasiaan klien menjadi lebih terjaga walaupun ada pihak yang dapat menyadap data klien yang lalu-lalang, tapi belum tentu bisa dibaca dengan mudah karena memang sudah diacak. Dengan menerapkan sistem enkripsi, tidak ada yang dapat mengakses dan

membaca isi jaringan data klien dengan mudah.

Data Integrity

Ketika melewati jaringan Internet, data yang ada pada sisi *client* sebenarnya sudah berjalan sangat jauh melintasi berbagai negara.ditengah perjalanannya, apapun bisa terjadi terhadap paket data yang dikirim.hilang, rusak, bahkan data yang dikirim dapat dimanipulasi oleh orang-orang yang tidak bertanggung jawab. VPN memiliki teknologi yang dapat menjaga keutuhan data yang klien kirim agar sampai ke tujuannya tanpa cacat, hilang, rusak, ataupun dimanipulasi oleh orang lain.

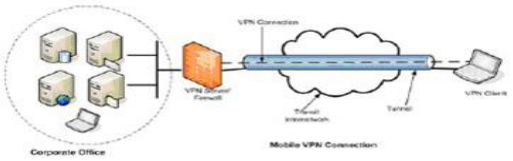
Authentication

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber pengirim data yang akan diterimanya. VPN juga akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi *source* datanya. Alamat *source* data ini akan disetujui jika proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima oleh klien berasal dari sumber yang semestinya. Tidak ada data yang dipalsukan atau dikirimkan oleh pihak-pihak lain keculai pengguna yang asli [].

Dalam implementasinya, VPN terbagi menjadi *remote access* VPN dan *site-to-site* VPN. *Site-to-site* VPN yang digunakan untuk meng*hub*ungkan antara 2 tempat yang letaknya berjauhan, seperti halnya kantor pusat dengan kantor cabang. VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya: mitra kerja, *supplier* atau pelanggan) disebut *ekstranet*. Sedangkan VPN yang digunakan untuk meng*hub*ungkan kantor pusat dengan kantor cabang disebut dengan intranet *site-to-site* VPN [4]. Penelitian ini dilakukan untuk mengetahui kualitas layanan (QoS) pada jaringan yang menerapkan site to site VPN. Penelitian ini dilakukan guna memperoleh apakah terdapat pengaruh yang significant apabila suatu file dengan type yang berbeda dilewatkan pada jarfingan yang menerapkan VPN terutama pada saat menerapkan protocol SSTP. Penekanan hasil penelitian diutaman pada unjuk kerja performa jaringan berdasarkan parameter QoS *(Quality of Serfice)* antara jaringan yang tidak menerapkan VPN dengan jaringan yang menerapkan VPN terutama pada pemanfaatan protocol SSTP pada jaringan kantor pusat dan kantor cabang. VPN atau jaringan dengan dua tempat yang saling berjauhan dengan menetapkan paramter-paramter tersebut untuk mengetahui apakah aspek keamanan telah dapat terpenuhi.

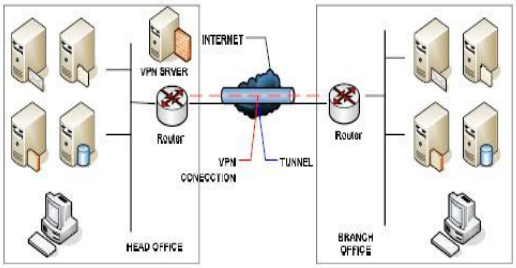
1.1. Penerapan VPN

Pada penerapan VPN dibagi menjadi dua jenis yaitu *remote access* VPN dan *site-to-site* VPN.. *Remote access* VPN. Jenis inplementasi yang pertama adalah *remoteaccess* yang biasa juga disebut *virtual private dial-up network* (VPDN), menghubungkan antara pengguna yang *mobile* dan *local areanetwork* (LAN).Jenis VPN yang seperti digunakan oleh pegawai perusaan yang ingin terhubung ke jaringan khusus perusaannya dari berbagai lokasi yang jauh (*remote*) dari perusahaannya.[5]



Gambar 1. *Remote Access* VPN

Jenis impelementasi VPN yang kedua adalah *site-to-site* VPN. Implementasi jenis ini menghubungkan antara dua tempat yang letaknya berjauhan, seperti halnya kantor pusat dengan kantor cabang atau suatu perusahaan dengan perusahaan mitra kerjanya.



Gambar 2 *Site-to-site* VPN

1.2. Protokol VPN

Protokol protokol jaringan VPN yang paling banyak digunakan atau biasa diguanakan oleh

user atau pengguna yang menggunakan jaringan VPN adalah:[5]

PPTP

Point-to-Point TunnelingProtocol (PPTP) adalah suatu protokol jaringan yang memungkinkan pengiriman data secara aman dari *remote client* kepada server perusahaan swasta dengan membuat suatu *Virtual Private Network* (VPN) melalui jaringan data berbasis TCP/IP

L2TP

Layer Two Tunneling Protocol (L2TP) adalah suatu standar IETF (RFC 2661) pada layer 2 yang merupakan kombinasi dari keunggulan-keunggulan fitur dari protokol L2F (dikembangkan oleh *Cisco)* dan PPTP (dikembangkan oleh Microsoft), yang didukung oleh vendor-vendor :*Ascend, Cisco*, IBM, *Microsoft* dan 3Com.Untuk mendapatkan tingkat keamanan yang lebih baik.Terdapat dua model tannel yang dikenal, yaitu *compulsory* dan *voluntary*.Pebedaan utama keduanya terletak pada *endpoint tunnel*.Pada *compulsorytunnel*, ujung *tunnel* berada pada ISP sedangkan pada *voluntary* ujung *tunnel* berada pada *client* berada pada *client remote*.L2TP murni hanya membentuk jaringan *tunnel*, oleh karena itu L2TP sering dikombinasikan dengan *IPsec* sebagai metode *enkripsi*.

IPsec

IPSec merupakan protokol VPN yang dikembangkan oleh *Internet Engineering Task Force* (IETF) yang bertujuan untuk menyediakan *framework* keamanan pada layer ketiga (*Third Layer*) yaitu pada *Network Layer* sehingga dapat mengamankan data dari layer yang diatasnya [6]. Inilah alasan mengapa IPSec di kembangkan pada layer 3 dari pada layer 2. Ada beberapa sistem keamanan *internet* yang digunakan seperti *Secure Socket Layer* (SSL),*Transport Layer Security* (TLS) *dan Secure Shell* (SSH)yang beroperasi di atas model TCP/IP.[5] Oleh karenanya *IPSec* melindungi semua aplikasi yang melewati jaringan *Internet Protocol*.Aplikasi-aplikasi tidak perlu di desain khusus untuk menggunakan *IPSec* tidak seperti TLS/SSL yang mengharuskan didesain khusus pada aplikasi agar dapat melindungi keamanan dari aplikasi yang dibuat.*IPSec* terdiri dari 3 kombinasi protokol kunci, yaitu:[6]

1. *AuthenticationHeader* (AH) protokol, yang berfungsi untuk memberi header tambahan pada IP Datagram, *header* ini akan mengotentikasi IP Datagram yang dikirim ke penerima.
2. *EncapsulatingSecurityPayload* (ESP) tujuan utama dari ESP yaitu meyediakan kerahasiaan pada proses autentikasi pengirim serta melakukan verifikasi integrasi data selama proses transit.
3. *Internet Key Exchange* (IKE) protokol, merupakan protokol yang menyediakan kunci *otentikasi* sebelum IPSec diimplementasikan.

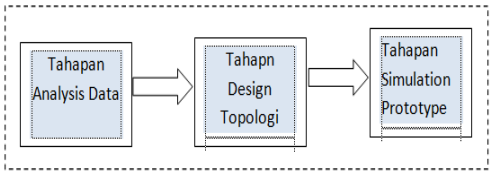
SSTP

SSTP *(Secure Socket Tunneling Protocol)* adalah sebuah tunneling yang dibuat untuk menjalankan mekanisme untuk mengangkut ppp frame di dalam SSL/TLS Channel. Dengan menggunakan SSL, akan memungkinkan packet yang akan dikirimkan tersebut, memiliki keamanan yang akan memungkinkan kedua perangkat jaringan melakukan negosiasi, enkripsi, dan juga pengecekan traffic.

Protocol SSTP merupakan bentuk baru dari VPN *tunnel* yang memiliki fitur mengizinkan trafik dapat melewati *firewall* yang memblok trafik PPTP dan trafik L2TP/IPsec.SSTP menyediakan mekanisme untuk mengenkapsulasi trafik PPP*over* SSL*channel* dari protokol HTTPS.Penggunaan PPP memungkinkan dukungan untuk metode autentikasi yang kuat dan handal seperti EAP-TLS [3]

II. METODOLOGI

Dalam penelitian ini, peneliti menggunakan beberapa tahapan penelitian yang mengacu pada metode penelitian dibidang jaringan komputer terutama untuk pengembangan system jaringan yaitu metode *Network Development Life Cycle* (NDLC). Metode NDLC yakni tediri dari 6 tahapan yaitu *analysis, design, simulation prototyping, implementation, monitoring* dan *Management*. Dari 6 tahapan yang terdapat pada metode tersebut peneliti hanya menggunakan 3 tahapan antara lain *Analysis, Design* dan *Simulation Prototype*.



Gambar 3. Tiga Tahapan Metodologi NDLC

Rincian tahapan yang dipergunakan pada penelitian ini adalah sebagai berikut:

Tahapan Analysis

Pada tahap ini Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, dan analisa topologi jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap adalah:

a. Membaca dan menganalisis manual, jurnal, buku atau blueprint dokumentasi topologi jaringan VPN yang pernah didesain sebelumnya. Diilakukan pula dengan review serta evaluasi terhadap informasi dari manual-manual atau blueprint dokumentasi yang khusus menerapkan protocol SSTP pada sebuah jaringan pada sebuah kasus terterntu. Sudah menjadi keharusan dalam setiap pengembangan pengembangan jaringan komputer, dokumentasi menjadi pendukung akhir dari pengembangan tersebut, begitu juga pada project network, dokumentasi menjadi syarat mutlak setelah sistem selesai dibangun.
b. Menelaah setiap data yang didapat dari data-data sebelumnya, maka diperlukan analisa terkait konfigurasi, pengaturan serta aturan yang pernah dilakukan dalam kaitannya dengan penerapan VPN dalam jaringan komputer.
c. Tahap analisis ini dilakukan dengan Menetapkan parameter parameter pengukuran QOS (Quality Of Service). Penetapan kualitas QoS merupakan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari suatu servis [1]. Komponen-komponen dari QoS adalah *delay, packet loss, throughput* dan *jitter*. Penjelasan dari setiap aspek yang dikemukakan adalah :

1. Delay (Latency)

Delay (Latency) merupakan waktu yang dibutuhkan data untuk menempuh jarak dari asal ketujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, *congesti* atau juga waktu proses yang lama [8]. Pada Tabel 1 diperlihatkan kategori dari *delay* dan besar *delay.*

Tabel 1. Katagori Parameter delay

Ukuran delay	Besaran(ms)	Indeks
Sangat Bagus	<150ms	4
Bagus	150 – 300ms	3
Sedang	300-450ms	2
Buruk	>450ms	1

Latency: Delay=
*(*Packet Length / Link Bandwit) [8]

2. *Packet Loss*

Packet Loss merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang dapat terjadi karena *collision* dan*congestion* pada jaringan. Indeks dan

Tabel 2. Katagori Paramter Packet Loss

Packet Loss	Packet Loss (%)	Indeks
Sangat Bagus	0	4
Bagus	3	3
Sedang	15	2
Buruk	25	1

3. *Throughput*

Throughput yaitu kecepatan (rate) transfer data efektif, yang diukur dalam *bps (bitpersecond)*. *Throughput* adalah jumlah total kedatangan paket yang

sukses yang diamati pada tujuan selama interval waktuter tentu dibagi oleh durasi interval waktu tersebut. Kategori *Throughput* diperlihatkan di Tabel dibawah ini.

Tabel 3 Kategori Paramter *Throughput*

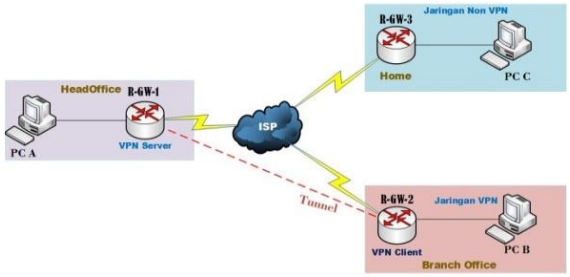
Throughput	***Throughput (bps)***	***Indeks***
SangatBagus	100	4
Bagus	75	3
Sedang	50	2
Jelek	<25	1

Persamaan perhitungan *Throughput [8]*

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

Tahapan Design

Tahap Design ini akan membuat gambar design topology jaringan interkoneksi yang akan digunakan untuk melakukan pengujian, diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan penelitian. Design bisa berupa design struktur topology, design akses data, design tata layout perkabelan yang akan memberikan gambaran jelas tentang jaringan site to site komputer yang akan dianlisis sebagai subyek penelitian. Berikut ini merupakan design topologi jaringan yang digambar dengan aplikasi viso yang akan dipergunakan sebagai subyek penelitian dan diterapkan dalam simulator, yang dapat terlihat seperti gambar dibawah ini:

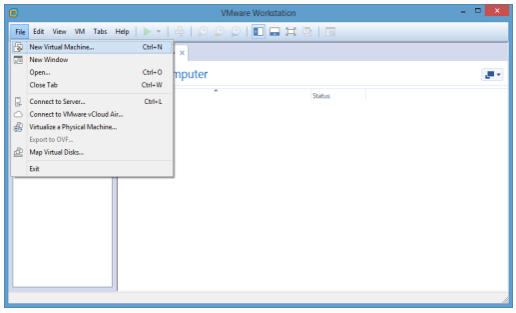


Gambar 4. Topologi Jaringan Pengujian VPN

Pada design topologi tersebut menunjukkan 3 jaringan *private* yang berbeda lokasi, yaitu *HeadOffice* sebagai VPN *Server*, *BranchOffice* sebagai VPN *Client* dan *Home* sebagai jaringan *Client* yang tidak menerapkan jaringan VPN. Jaringan *internal BranchOffice* berkomunikasi dengan jaringan *internal Server/HeadOffice* menggukan *tunnel* VPN, sedangkan jaringan *internal Home* berkomunikasi dengan jaringan *internal HeadOffice* hanya menggunakan jaringan *public*. Dimana masing-masing jaringan private memiliki *router gateway* yang terhubung langsung ke internet.

Tahapan Simulation Prototype

Beberapa tahapan konfigurasi, design topologi dan pengujian jaringan komputer akan terbuat dalam bentuk simulasi dengan bantuan Tools khusus di bidang jaringan komputer seperti aplikasi Boson, Packet Tracer, NetSim, dan lain sebagainya, Hal tersebut dimaksudkan untuk melihat kinerja awal dari jaringan komputer yang akan dibangun. Keterbatasan perangkat lunak (sumber: T. Pratama, 2015) pada simulasi prototype seperti ini mempunyai kekurangan yang hanya menggunakan satu produk device jaringan. Penelitian ini mensimulasikan topologi dengan menggunakan perangkat lunak viso sebagai tahapan design atapun dapat juga dilakukan dengan aplikasi Grafik Network Simulator (GNS3) yang dintegarsikan dengan virtual mesin seperti penggunaan aplikasi Vmware wokstation. Penelitian melakukann simulasi dengan hanya mempergunakan Vmware wokstation yang didalamnya telah terinstalasi perangkat jaringan yang dibutuhkan seperti router mikrotik, swich maupun sistem operasi windows sebagai client seperti gambar dibawah ini.



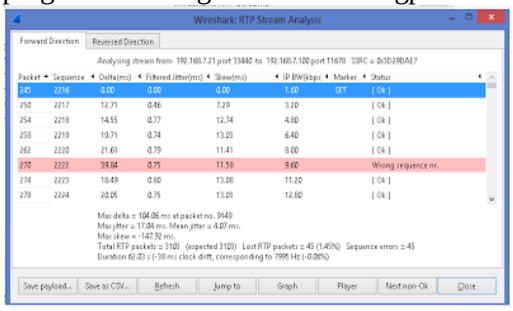
Gambar 5. Aplikasi VMware Workstation

Diperlukan pula simulasi menggunakan aplikasi team viewer serta network analyzer, seperti aplikasi wireshark sebagai tools yang digunakan

untuk memonitor aktifitas komunikasi data yang terjadi antar jaringan. [2]. Komunikasi data yang terjadi antara kantor pusat dan kantor cabang baik sebelum menerapkan protocol SSTP atau tidak menggunakan protocol SSTP. Penggunaan tools wireshark diperlukan untuk mengamati nilai parameter-paramter QoS pada jaringan VPN. Nilai hasil parameter pengukuran diperoleh dari fiture yang terdapat pada tools wireshark, dan selanjutnya dianalis berdasarkan hasil pengukuran yang diperoleh.

III. HASIL DAN PEMBAHASAN

Hasil pengujian pengiriman data dilakukan dengan aplikasi TeamViwer dari jaringan *internal Server* ke jaringan *internal Client.* Proses pengiriman akan terbagi menjadi tiga kali pengujian dari masing-masing jenis serta ukuran file. Data yang dikirim merupakan data dengan ukuran, jenis dan *format file* yang berbeda. kemudian akan dilakukan analisa terhadap nilai parameter QoS berupa *delay, packet loss,* dan *throughput.* Hasil pengukuran dilakukan dengan menggunakan *tool* wireshark, dimana tools ini dipergunakan sebagai network analyzer paket data yang melewati suatu jaringan. Berikut adalah tampilan contoh data ketika tools wireshark dipergunakan mengukur nilai througput.



Gambar 6 Hasil Throuhput Pada Wireshark

3.1. Analisis Paramter QoS

Setelah melakukan pengamatan dari kedua jaringan tersebut maka peneliti mendapatkan data yang digunakan untuk melakukan analisa terhadap performa dari jaringan yang menerapkan VPN dengan jaringan yang tidak menerapkan VPN. Berikut adalah hasil analisa perbandingan nilai rata-rata *delay, packet loss* dan *throughput.*

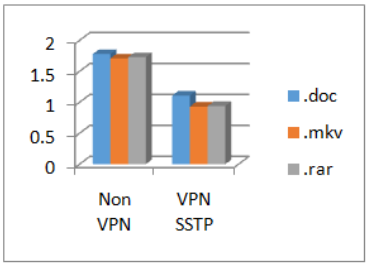
a. Delay

Dalam komparasi nilai rata-rata *delay* yang dilakukan, nilai *delay* terkecilah yang merupakan nilai terbaik. Semakin kecil nilai *delay* maka semakin baik kondisi kualitas sebuah jaringan. Berikut adalah hasil perbandingan keseluruhan nilai rata-rata *delay* antara jaringan non- VPN dengan jaringan *site-to-site* VPN SSTP:

Tabel 4. Perbandingan Rata-rata *Delay*

Jenis/Ukuran File (MB)		**Rata-rata *Delay (ms)***	
		Jaringan Non- VPN	**Jaringan VPN SSTP**
.doc	4.86	1.78	1.11
.mkv	12.2	1.71	0.93
.rar	22.3	1.73	0.94

Dari tabel 4 diperoleh rata-rata *delay* yang dihasilkan pada seluruh pengujian terhadap jaringan Non VPN dalam pengiriman *file .doc* nilai rata-rata *delay* sebesar 1.178 ms, pada pengiriman *file .mkv* nilai rata-rata *delay* adalah 1.71ms sedangkan pada pengiriman *file .rar* nilai rata-rata *delay* yang diperoleh adalah 1.73ms. Kemudian pada keseluruhan pengujian terhadap jaringan *site-to-site* VPN dalam pengiriman *file .doc* nilai rata-rata *delay* sebesar 1.11 ms, pada pengiriman *file .mkv* nilai rata-rata *delay* adalah 0.93 ms sedangkan pada pengiriman *file .rar* nilai rata-rata *delay* yang diperoleh adalah 0.94 ms. Dari hasil analisa rata-rata nilai *delay* yang diperoleh, maka jaringan yang menerapkan VPN SSTP memiliki kinerja lebih baik dari pada jaringan yang tidak menerapkan VPN. Berikut adalah gambar grafik perbandingan rata-rata *delay* antara kedua jaringan:



Gamab 7 Perbandingan pengukuran *Delay*

Packet Loss

Dalam komparasi nilai rata-rata *packet loss* yang dilakukan, nilai *packet loss* terkecilah yang merupakan nilai terbaik. Semakin kecil nilai *packet loss* maka semakin baik kondisi kualitas sebuah jaringan. Berikut adalah hasil perbandingan nilai rata-rata *packet loss* antara jaringan non-VPN dengan jaringan *site-to-site* VPN SSTP:

Tabel 5 Perbandingan rata-rata*Packet Loss*

Jenis/Ukuran File (MB)		**Rata-rata *Packet Loss* *(%)***	
		Jaringan Non- VPN	**Jaringan VPN SSTP**
.doc	4.86	0 %	0 %
.mkv	12.2	0 %	0 %
.rar	22.3	0 %	0 %

Dari tabel 5 dapat diketahui bahwa jaringan yang menerapkan VPN dan tanpa VPN memiliki *packet loss* 0%. Hal ini membuktikan kedua jaringan tersebut pada saat melakukan percobaan pengiriman *file* tidak ada paket yang hilang. Berikut adalah gambar grafik perbandingan nilai *packet loss* antara jaringan non- VPN dengan jaringan *site-to-site* VPN SSTP:

Throughput

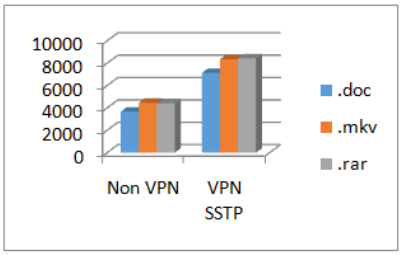
Dalam komparasi nilai rata-rata *throughput* yang dilakukan, nilai *throughput* terbesar yang merupakan nilai terbaik. Semakin bersar nilai *throughput* maka semakin baik kondisi kualitas sebuah jaringan. Berikut adalah hasil perbandingan nilai rata-rata *throughput* antara jaringan *Public* dengan jaringan VPN SSTP:

Tabel 6 Perbandingan rata-rata*Throughput*

Jenis/Ukuran File (MB)		**Rata-rata *Throughput* *(Kbps)***	
		Jaringan Non- VPN	**Jaringan VPN SSTP**
.doc	4.86	3663.5	7122.7
.mkv	12.2	4452.0	8347.4
.rar	22.3	4406.9	8431.1

Dari tabel 6 diperoleh rata-rata *throughput* yang dihasilkan pada seluruh pengujian terhadap jaringan non- VPN dalam pengiriman *file .doc* nilai rata-rata *throughput* sebesar 3663.5 Kbps, pada pengiriman *file .mkv* nilai rata-rata *throughput* adalah 4452.0 Kbps, sedangkan pada pengiriman *file .rar* nilai rata-rata *throughput* yang diperoleh adalah 4406.9 Kbps. Kemudian pada keseluruhan pengujian terhadap jaringan *site-to-site* VPN dalam pengiriman *file .doc* nilai rata-rata *throughput* sebesar 7122.7 ms, pada pengiriman *file .mkv* nilai rata-rata *throughput* adalah 8347.4 Kbps, sedangkan pada pengiriman *file .rar* nilai rata-rata *throughput* yang diperoleh adalah 8431.1 Kbps.

Dari hasil analisa rata-rata nilai *throughput* yang diperoleh, maka jaringan yang menerapkan VPN SSTP memiliki performa lebih baik dari pada jaringan yang tidak menerapkan VPN. Berikut adalah gambar grafik perbandingan rata-rata *throughput* antara jaringan non- VPN dengan jaringan *site-to-site* VPN SSTP:



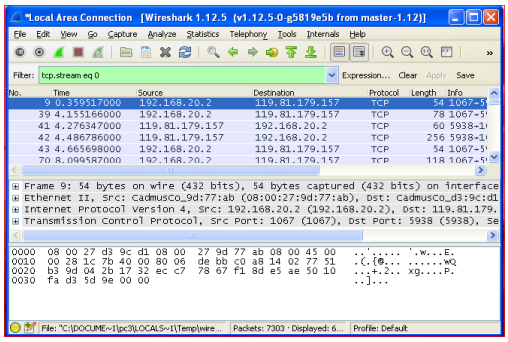
Gambar 8 Perbandingan *Throughput*

1.1. Analisis Jaringan

Evaluasi jaringan ini dilakukan untuk mengetahui apakah aspek kemanan sudah terpenuhi atau tidak. Keamanan merupakan salah satu keunggulan dari model rancangan VPN ini. Pengujian keamanan akan meliputi aspek kerahasiaan *(privacy)*, integritas data *(integrity)*, dan ketersedian layanan *(availability)*. Evalusi jaringan meliputi jaringan Non- VPN dan Jaringan VPN.

Jaringan Non- VPN

Pada pengujian ini dilakukan percobaan *capturing* pada jaringan non- VPN dengan menggunakan aplikasi wireshark dengan skenario sebagai berikut. Komputer *server* akan mengirim sebuah *file* yang di kirim ke komputer *client* kemudian dilakukan proses *capturing* dengan menggunakan aplikasi Wireshark. Berikut adalah hasil *capture* yang di dapatkan:

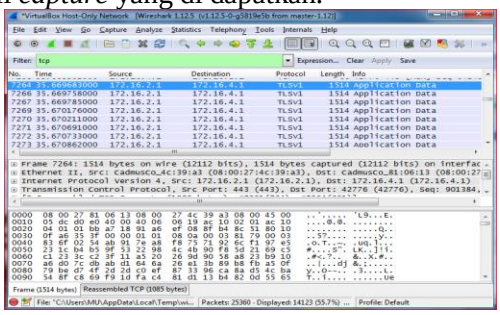


Gambar 9 Hasil *Capture* Non VPN

Hasil penangkapan menunjukkan bahwa paket data terkirim melalui jaringan internet *(public)*. Paket data yang terkirim melalui jaringan publik tidak menjamin keamanan data, karena paket data tidak ada yang membungkus sehingga data bisa saja di sadap dan dimanipulasi oleh pihak-pihak yang tidak bertanggung jawab. Sebagaimana diketahui pengguna jaringan publik berlalu lalang sehingga kerahasiaan data tidak terjaga dan keutuhan data tidak terjamanin ke aslian dan sumbernya.

Jaringan *Site-to-site* VPN SSTP

Pada eksperimen ini dilakukan percobaan *capturing* pada jaringan VPN dengan menggunakan aplikasi wiresharkdengan skenario sebagai berikut. Komputer server akan mengirim sebuah *file* yang di kirim ke komputer client kemudian dilakukan proses *capturing* dengan menggunakan aplikasi Wireshark. Berikut adalah hasil *capture* yang di dapatkan:



Gambar 10 Hasil *Capture* VPN dengan SSTP

Hasil penangkapan menunjukkan bahwa paket data yang dikirm telah dienkapsulasi melalui *tunnel* VPN dan hal ini membuktikan bahwa enkripsi telah berjalan dengan baik dan aman untuk digunakan di jalur internet publik. Dengan ini terbukti bahwa penggunaan VPN berbasis SSTP akan menjamin keamanan data, terutama dalam hal kerahasiaan karena menggunakan SSL sebagai pengamanannya. Dengan menggunakan saluran SSL/TLS diharapkan paket data tidak akan mengalami perubahan yang disebabkan oleh pihak-pihak yang tidak berwenang. Dengan begitu aspek integritas data dapat terjamin keasliannya. Didalam pengaplikasian *site-to-site* VPN, media yang digunakan adalah internet yang sudah tersedia dan dapat diakses dengan mudah sehingga layanan VPN ini akan selalu tersedia selama VPN *Server* dan VPN *Client* terhubung ke internet.

IV. KESIMPULAN DAN SARAN

Kesimpulan yang dapat diambil dari hasil penelitian yang dilakukan dalam bentuk simulasi dengan mengamati parameter-parameter QoS yang ditentukan diperoleh kesimpulan bahwa:

1. Jaringan yang menerapkan *site-to-site* VPN memiliki kualitas layanan lebih baik dari pada jaringan yang tanpa VPN. Ketika melakukan beberapa pengujian dan pengamatan terhadap pengiriman *file*, nilai rata-rata *delay* jaringan *site-to-site* VPN dengan SSTP lebih kecil dibandingkan dengan nilai rata-rata *delay* dari jaringan yang tidak menerapkan VPN.
2. Kulitas Paket yang dikirim tidak mengalami *broken* (rusak) ataupun hilang (*lost*) pada saat pengiriman ataupun penerimaan data, hal ini terlihat dari hasil pengujian sebesar 0% dari nilai packet loss, begitu pula dengan hasil thougput yang lebih besar dibandingkan dengan jaringan yang tanpa menerapkan VPN.
3. Penggunaan protocol SSTP Pada jaringan site to site VPN dengan protocol SSTP memiliki kinerja yang lebih baik berdasarkan paramter delay, packet loss dan throuhput. Disamping itu dari sisi keamanan file atau data yang dikrimkan penggunaan protocol SSTP dapat melindungi data dari aktifitas ilegal hal ini disebabkan file akan terinkripsi menajdi bentuk yang berbeda dengan file aslinya.

Berdasarkan pengujian parameter-parameter QoS pada jaringan site-to-site VPN yang telah

dilakukan, ada beberapa saran yang dapat diberikan adalah diperlukan penelitian lanjutan untuk mengamati parameter Qos pada jaringan VPN atau kinerja layanan pada kondisi yang lebih nyta dalam arti penelitian menggunakan perangkat sesungguhnya seperti penggunaan perangkat personal komputer, kabel, switch maupun router atau penelitian dalam kasus sesungguhnya disebuah kantor pusat dan kantor cabang di sebuah instansi ataupun perusahaan.

.

REFERENSI

[1]. Ferguson, P. & Huston, G. "*Quality of Service"*. John Wiley & Sons Inc, 1998

[2]. Herianto, D. (n.d.). Embedded System Network Analyzer pada Jaringan LAN, 2010.

[3]. Iswara, G. S., Periyadi, and Ismail, S. J. I. *Implementasi Protokol SSTP dalam Membangun Server VPN Menggunakan Konfigurasi Routing dan Remote Access untuk Access Client pada Windows Server 2008*.

[4]. Iswan. L. M., "*implementasi virtual private network(VPN) remote acces dengan linux openswan*." Laporan Penelitian . Fakultas sains dan teknologi universitas islam negeri syarif hidayatullah jakarta, 2010.

[5]. Rosidin, *B. "Konfigurasi VPN Dengan Mengkombinasikan PPTP/IPSEC Pada Router Mikrotik", 8-9. 2014*

[6]. Syafrizal, Melwin,. "*Pengantar Jaringan Komputer"*. Penerbit C.V.Andi Offset. *Yogyakarta 2005*

[7]. Sahari, "Perancangan Dan Implementasi Virtual Private Network (VPN) Pada Jaringan Nirkabel (Study Kasus :UPY-YPTK Paang)" *POLI REKAYASA* , 47, 2008.

[8]. T.Pratama,"Perbandingan Metode PCQ, SFQ, Reddan FIFO pada Mikrotik sebagai Upaya Optimalisasi Layanan Jaringan pada Fakultas Teknik Universitas Tanjungpura, "*Jurnal Sistem dan Teknologi Informasi* Vol3,No.1 Universitas Tanjungpura 2015.