SKRIPSI

ANALISIS PERFORMA PROTOKOL *SECURE SOCKET TUNNELING PROTOCOL* DAN *LAYER TWO TUNNELING PROTOCOL / INTERNET PROTOCOL SECURITY* PADA *VIRTUAL PRIVATE NETWORK*

Disusun dan diajukan oleh :

MARJONO UMAR

D421 15 023

DEPARTEMEN TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS HASANUDDIN

MAKASSAR

2021

LEMBAR PENGESAHAN SKRIPSI

ANALISIS PERFORMA PROTOKOL *SECURE SOCKET TUNNELING PROTOCOL* DAN *LAYER TWO TUNNELING PROTOCOL / INTERNET PROTOCOL SECURITY* PADA *VIRTUAL PRIVATE NETWORK*

Disusun dan diajukan oleh

MARJONO UMAR
D421 15 023

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Program Studi Teknik Informatika Fakultas Teknik Universitas Hasanuddin pada tanggal 9 Februari 2022
dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama,	Pembimbing Pendamping
Dr. Eng. Muhammad Niswar, S.T.,M.IT.	Dr. Eng. Ady Wahyudi Paundu,S.T., M.T
Nip. 19730922 199903 1 001	Nip. 19750313 200912 1 003

Ketua Program Studi,

Dr. Amil Ahmad Ilham, S.T., M.IT
Nip. 19731010 199802 1 001

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama	: MARJONO UMAR
NIM	: D421 15 023
Program Studi	: TEKNIK INFORMATIKA
Jenjang	: S1

Menyatakan dengan ini bahwa karya tulisan saya berjudul

ANALISIS PERFORMA PROTOKOL *SECURE SOCKET TUNNELING PROTOCOL* DAN *LAYER TWO TUNNELING PROTOCOL / INTERNET PROTOCOL SECURITY* PADA *VIRTUAL PRIVATE NETWORK*

Adalah karya tulis saya sendiri dan bukan merupakan pengambilan alihan tulisan orang lain bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri.

Apabila dikemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan skripsi ini hasil karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Makassar,17 Februari 2022

Yang Menyatakan

MARJONO UMAR

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa karena berkat rahmat dan karunia-Nya sehingga skripsi yang berjudul "ANALISIS PERFORMA PROTOKOL SECURE SOCKET TUNNELING PROTOCOL DAN LAYER TWO TUNNELING PROTOCOL / INTERNET PROTOCOL SECURITY PADA VIRTUAL PRIVATE NETWORK" ini dapat diselesaikan sebagai salah satu syarat dalam menyelesaikan jenjang Strata-1 pada Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin.

Penulis menyadari bahwa dalam penyusunan dan penulisan laporan tugas akhir ini tidak lepas dari bantuan, bimbingan serta dukungan dari berbagai pihak, dari masa perkuliahan sampai dengan masa penyusunan tugas akhir. Oleh karena itu, penulis dengan senang hati menyampaikan terima kasih kepada:

1. **Tuhan Yang Maha Esa** atas semua berkat, karunia, serta pertolongan-Nya yang tiada batas, yang diberikan kepada penulis disetiap langkah dalam pembuatan program hingga penulisan laporan skripsi ini;
2. Kedua Orang tua penulis, Bapak **Alm. Umar P** dan Ibu **Hj. Johani** yang selalu memberikan dukungan, doa, dan semangat serta selalu sabar dalam mendidik;
3. Saudara penulis, **Marjani**, **Umriani**, **Marhadi**, **Ilham** dan **Nurhikmah** yang selalu memberikan dukungan, doa, dan semangat;
4. Bapak **Dr. Eng. Muhammad Niswar,ST., M.IT**., selaku pembimbing I dan Bapak **Dr. Eng. Ady Wahyudi Paundu, ST., MT.,** selaku pembimbing II yang

selalu menyediakan waktu, tenaga, pikiran dan perhatian yang luar biasa untuk mengarahkan penulis dalam penyusunan tugas akhir;

5. Bapak **Adnan, ST., M.T., Ph.D.,** dan **Bapak Iqra Aswad, ST., M.T.,** selaku dosen penguji yang telah memberikan saran dalam penyusunan tugas akhir;
6. Bapak **Dr. Amil Ahmad Ilham, ST., M.IT.,** selaku Ketua Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin atas bimbingannya selama masa perkuliahan penulis;
7. Para sahabat, **Fadhilah**, **Dila, Alfina, Arifa, Nazila, Ardiansyah, Muhtasan, Jenar, Zulkifli, Bayazid, Fathur, Imran** dan **Rijal** yang telah memberikan bantuan selama penelitian, penulisan dan diskusi *progress* penyusunan tugas akhir;
8. Teman-teman **HYPERV150R FT-UH** atas dukungan dan semangat yang diberikan selama ini;
9. Bapak **Robert** dan Bapak **Zainuddin** serta segenap Staf Departemen Teknik Informatika yang telah membantu penulis;
10. Orang-orang berpengaruh lainnya yang tidak sempat disebutkan oleh penulis;

Akhir kata, penulis berharap semoga Allah SWT. berkenan membalas segala kebaikan dari semua pihak yang telah banyak membantu. Semoga Tugas Akhir ini dapat memberikan manfaat bagi pengembangan ilmu. Aamiin.

Gowa, 14 September 2021

Penulis

ABSTRAK

Secure Socket Tunneling Protocol (SSTP) dan *Layer Two Tunneling Protocol/Internet Protocol Security* (L2TP/IPSec) merupakan jenis *Virtual Private Network* (VPN) yang telah banyak didukung oleh protokol jaringan untuk dapat diterapkan pada banyak perangkat jaringan komputer. Kedua metode tersebut diterapkan secara bergantian pada mikrotik. Setiap metode yang diterapkan, selanjutnya akan dianalisis dengan menggunakan aplikasi *Wireshark* dengan parameter *Quality of Service* (QoS) yang terdiri dari *delay, jitter, packet loss,* dan *throughput*. Pengujian dilakukan dengan menggunakan *tool apache benchmark* pada *client* untuk mengakses performa *dashboard web server apache* pada *server*. Hasil pengujian performa QoS untuk protokol SSTP dan L2TP/IPSec tidak ada yang terlalu signifikan sehingga masih dalam performa baik. *Delay* SSTP dan L2TP/IPSec hanya berkisaran 1.146667337 ms dan 1.289555881 ms. *Jitter* SSTP dan L2TP/IPSec hanya berkisaran 1.14674427 ms dan 1.28964983 ms. *Packet Loss* SSTP dan L2TP/IPSec hanya berkisaran 0.660319 % dan 0.522113 %. *Throughput* SSTP dan L2TP/IPSec hanya berkisaran 7023.115103 bps dan 6236.246435 bps.

Kata Kunci: VPN, *Tunneling*, SSTP, L2TP, QoS.

ABSTRACT

Secure Socket Tunneling Protocol (SSTP) and *Layer Two Tunneling Protocol/Internet Protocol Security* (L2TP/IPSec) are types of *Virtual Private Network* (VPN) that have been widely supported by network protocols to be applied to many computer network devices. The two methods are applied alternately to the proxy. Each method applied will then be analyzed using the *Wireshark* with *Quality of Service* (QoS) parameters consisting of *delay*, *jitter, packet loss,* and *throughput*. Testing is done by using *the Apache Benchmark tool* on *client* to access the performance *of the Apache web server dashboard* on *the server*. The QoS performance test results for the SSTP and L2TP/IPSec protocols are not too significant so they are still in good performance. *delays* only ranged from 1.146667337 ms and 1.289555881 ms. *jitter* only ranged from 1.14674427 ms and 1.28964983 ms. *Packet Loss* only ranged from 0.660319 % and 0.522113 %. *The throughput* of SSTP and L2TP/IPSec only ranges from 7023.15103 bps and 6236.246435 bps.

Keywords: VPN, *Tunneling*, SSTP, L2TP, QoS.

DAFTAR ISI

KATA PENGANTAR iii

ABSTRAK v

ABSTRACT vi

DAFTAR ISI vii

DAFTAR GAMBAR ix

DAFTAR TABEL x

DAFTAR GRAFIK xi

BAB I PENDAHULUAN 1

1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Tujuan Penelitian 3
1.4 Manfaat Penelitian 3
1.5 Batasan Masalah Penelitian 3
1.6 Sistematika Penulisan 3

BAB II TINJAUAN PUSTAKA 5

2.1 Jaringan Komputer 5
2.2 Virtual Private Network (VPN) 7
2.3 Tunneling 8
2.4 Secure Socket Tunneling Protocol (SSTP) 8
2.5 Layer Two Tunneling Protocol (L2TP) 10
2.6 Internet Protocol Security (IPSec) 11
2.7 Quality of Service (QoS) 12
2.7.1 Delay 13

2.7.2 Jitter 13
2.7.3 Packet Loss 14
2.7.4 Throughput 15
BAB III METODOLOGI PENELITIAN 17
3.1 Tahapan Penelitian 17
3.2 Waktu dan Lokasi Penelitian 19
3.3 Instrumen Penelitian 19
3.4 Tahap Persiapan 20
3.5. Gambaran Umum Sistem 20
3.6. Desain Topologi 21
3.7. Pengujian Performa 23
BAB IV HASIL DAN PEMBAHASAN 25
4.1 Hasil Pengujian 25
4.1.1 Delay 28
4.1.2 Jitter 30
4.1.3 Packet Loss 32
4.1.4 Throughput 35
4.2 Pembahasan 37
BAB V PENUTUP 40
5.1 Kesimpulan 40
5.2 Saran 40
DAFTAR PUSTAKA 42
LAMPIRAN 44

DAFTAR GAMBAR

Gambar 2. 1 Arsitektur Jaringan Komputer *peer-to-peer* 6

Gambar 2. 2 Arsitektur Jaringan Komputer *client-server* 6

Gambar 2. 3 Konsep VPN 7

Gambar 2. 4 Ilustrasi *tunneling* 8

Gambar 2. 5 *Secure Socket Tunneling Protocol* 10

Gambar 2. 6 *Layer Two Tunneling Protocol* 11

Gambar 2. 7 *lnternet Protocol Security* 12

Gambar 3. 1 Diagram Tahapan Penelitian 17

Gambar 3. 2 Diagram alur penelitian Implementasi SSTP dan L2TP/IPSec 21

Gambar 3. 3 Topologi Protokol SSTP dan L2TP/IPSec 22

Gambar 4. 1 Contoh hasil rekaman data *wireshark* protokol SSTP dan L2TP/IPSec dalam format *excel* 25

Gambar 4. 2 Contoh hasil *apache benchmark* 27

Gambar 4. 3 *Packet Structure* Protokol SSTP 37

Gambar 4. 4 *Packet Structure* Protokol L2TP/IPSec 38

DAFTAR TABEL

Tabel 2. 1 *Delay* 13

Tabel 2. 2 *Jitter* 14

Tabel 2. 3 *Packet Loss* 15

Tabel 4. 1 Nilai *delay* protokol SSTP dan L2TP/IPSec 29

Tabel 4. 2 Nilai *jitter* protokol SSTP dan L2TP/IPSec 31

Tabel 4. 3 Nilai total paket dan paket diterima protokol SSTP dan L2TP/IPSec 32

Tabel 4. 4 Nilai *packet loss* protokol SSTP dan L2TP/IPSec 33

Tabel 4. 5 Nilai *throughput* protokol SSTP dan L2TP/IPSec 36

DAFTAR GRAFIK

Grafik 4. 1 Perbandingan *delay* protokol SSTP dan L2TP/IPSec.....29

Grafik 4. 2 Perbandingan *jitter* protokol SSTP dan L2TP/IPSec.....31

Grafik 4. 3 Perbandingan *packet loss* protokol SSTP dan L2TP/IPSec.....34

Grafik 4. 4 Perbandingan *throughput* protokol SSTP dan L2TP/IPSec.....36

BAB I

PENDAHULUAN

1.1 Latar Belakang

Secara umum jaringan terbagi dalam dua area, yaitu jaringan publik dan jaringan lokal. Jaringan publik merupakan jaringan yang menghubungkan *interface* jaringan secara global, sedangkan untuk jaringan lokal merupakan jaringan yang menghubungkan *client-client* dalam satu jaringan lokal, seperti instansi atau perkantoran. Jaringan lokal dan publik merupakan jaringan yang saling terhubung, namun ada beberapa batasan-batasan yang mengatur koneksi antara dua jaringan tersebut.

VPN (*Virtual Private Network*) adalah sebuah teknologi komunikasi yang terkoneksi ke jaringan publik dan menggunakannya untuk bergabung ke jaringan lokal, dengan cara tersebut maka akan diperoleh hak dan pengaturan yang sama seperti halnya berada di dalam kantor atau jaringan itu sendiri, walaupun sebenarnya menggunakan jaringan publik. Jaringan VPN merupakan jaringan yang dibangun di atas sebuah *tunnel*.

Tunnel VPN memiliki fungsi sebagai jalur yang bertanggungjawab atas keamanan dari data yang berjalan di dalamnya. Pengujian dilakukan dengan cara membandingkan performa masing-masing *tunnel.* Pengujian performa dilakukan menggunakan beberapa parameter QoS (*Quality of Service*) untuk memperoleh kualitas dari *tunnel.* Proses enkripsi dan dekripsi pada VPN membuat *delay* di dalam

jaringan bertambah karena proses ini juga membutuhkan waktu. Keamanan data pada VPN pada akhirnya akan berpengaruh pada performansi QoS (*Quality of Service*).

Untuk membangun VPN dengan metode SSTP diperlukan sertifikat SSL (*Secure Sockets Layer*) di masing-masing perangkat. Komunikasi SSTP (*Secure Socket Tunneling Protocol*) menggunakan TCP (*Transmission Control Protocol*) *port* 443. L2TP (*Layer Two Tunneling Protocol*) merupakan pengembangan dari PPTP (*Point to Point Tunneling Protocol*) ditambah L2F (*Layer 2 Forwarding*). *Network security Protocol* dan enkripsi yang digunakan untuk autentikasi sama dengan PPTP. Akan tetapi untuk melakukan komunikasi, L2TP menggunakan UDP (*User Datagram Protocol*) *port* 1701. Biasanya untuk keamanan yang lebih baik, L2TP dikombinasikan dengan IPSec, menjadi L2TP/IPSec

Berdasarkan permasalahan yang ada, maka dalam Tugas Akhir ini akan dilakukan implementasi dan analisis performa protokol SSTP (*Secure Socket Tunneling Protocol*) dan protokol L2TP/IPSec (*Layer Two Tunneling Protocol/Internet Protocol Security*) dengan pemodelan jaringan VPN terhadap parameter QoS, sehingga dapat diketahui perbandingan performa protokol VPN terhadap QoS (*Quality of Service*).

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka rumusan masalah pada tugas akhir ini adalah:

1. Bagaimana perbandingan performa QoS dari protokol SSTP dan L2TP/IPSec pada VPN?

1.3 Tujuan Penelitian

Tujuan dari tugas akhir ini adalah :

1. Membandingkan performa QoS dari protokol SSTP dan L2TP/IPSec pada VPN.

1.4 Manfaat Penelitian

Manfaat dari tugas akhir ini adalah :

1. Bagi Masyarakat, dapat menjadi bahan perbandingan dalam menggunakan protokol pada VPN.
2. Bagi Peneliti, dapat digunakan untuk menambah pengetahuan dan sebagai referensi mengenai protokol pada VPN.
3. Bagi Institusi pendidikan, dapat digunakan sebagai referensi dalam pembangunan sebuah jaringan pada VPN.

1.5 Batasan Masalah Penelitian

Yang menjadi batasan masalah dalam tugas akhir ini adalah :

1. Membandingkan performa protokol SSTP dan L2TP/IPSec
2. Parameter QoS yang digunakan adalah *delay, jitter, packet loss* dan *throughput.*

1.6 Sistematika Penulisan

Untuk memberikan gambaran singkat mengenai isi tulisan secara keseluruhan, maka akan diuraikan beberapa tahapan dari penulisan secara sistematis, yaitu :

BAB I PENDAHULUAN

Bab ini menguraikan secara umum mengenai hal yang menyangkut latar belakang, perumusan masalah dan batasan masalah, tujuan, manfaat, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi teori-teori tentang hal-hal yang berhubungan dengan sistem yang dianalisis, antara lain mengenai modul praktikum, metode yang digunakan, hingga bahasa yang digunakan dalam analisis tersebut.

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentang tahapan penelitian, waktu dan lokasi penelitian, instrumen penelitian, tahap persiapan, gambaran umum sistem, skenario pengujian dan analisis performa.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi tentang hasil performa serta pembahasan yang disertai pemaparan hasil penelitian.

BAB V PENUTUP

Bab ini berisi tentang kesimpulan yang didapatkan berdasarkan hasil penelitian yang telah dilakukan serta saran-saran untuk pengembangan lebih lanjut.

BAB II
TINJAUAN PUSTAKA

2.1 Jaringan Komputer

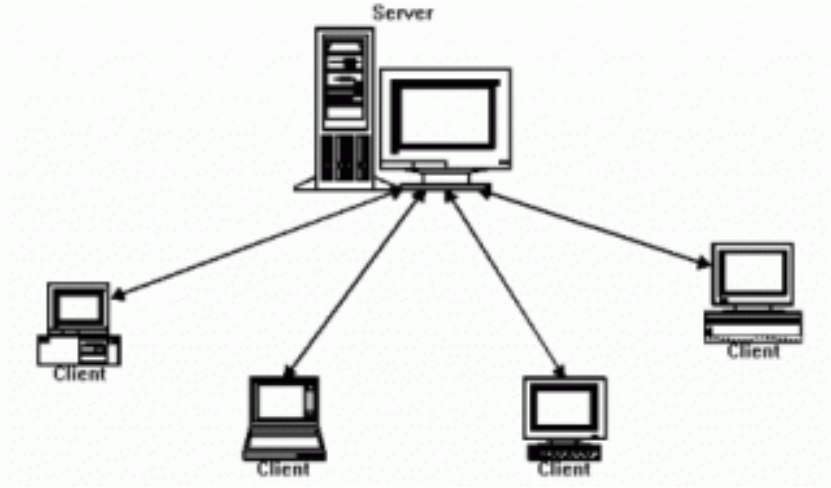
Konsep jaringan komputer lahir pada tahun 1940-an di Amerika dari sebuah proyek pengembangan komputer MODEL I di Laboratorium Bell dan group riset Harvard University yang dipimpin oleh professor H. Aiken. Pada mulanya proyek tersebut hanyalah ingin memanfaatkan sebuah perangkat komputer yang harus dipakai bersama. Untuk mengerjakan beberapa proses tanpa banyak membuang waktu kosong dibuatlah proses beruntun (*Batch Processing*), sehingga beberapa program bias dijalankan dalam sebuah komputer dengan kaidah antrian (Kustanto dan Saputro, 2015).

Di tahun 1950-an ketika jenis komputer mulai membesar sampai terciptanya super komputer, maka sebuah komputer mesti melayani beberapa terminal. Untuk itu ditemukan konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (*Time Sharing System*), maka untuk pertama kali bentuk jaringan (*network*) komputer diaplikasikan. Pada sistem TSS beberapa terminal terhubung secara seri ke sebuah *host* komputer. Dalam proses TSS mulai nampak perpaduan teknologi komputer dan teknologi telekomunikasi yang pada awalnya berkembang sendiri (Kustanto dan Saputro, 2015).

Pada jaringan komputer terbagi menjadi dua berdasarkan fungsinya, yaitu *peer-to-peer* dan *client-server*.

Gambar 2. 1 Arsitektur Jaringan Komputer *peer-to-peer*

Peer-to-peer yaitu jaringan komputer dimana setiap *host* dapat menjadi *server* dan juga menjadi *client* secara bersamaan. Secara hierarki kedudukan masing-masing komputer sama.



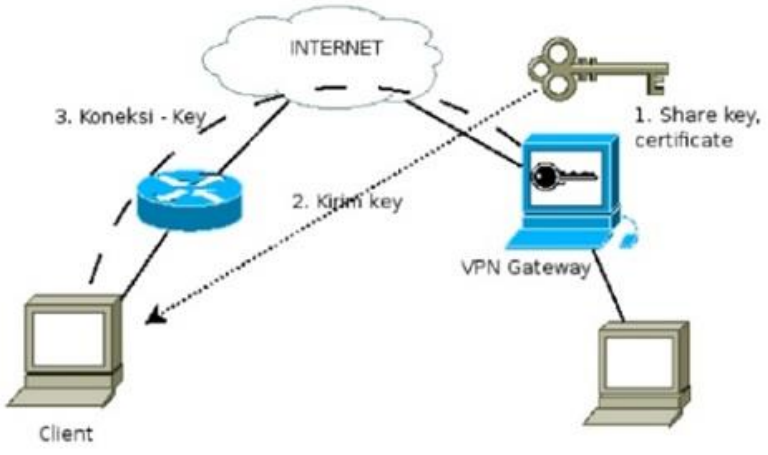
Gambar 2. 2 Arsitektur Jaringan Komputer *client-server*

Client-server yaitu komputer dengan adanya komputer yang didedikasikan khusus sebagai *server* dan dapat diakses oleh beberapa *client*. Secara hierarki kedudukan komputer *server* ada di atas komputer *client*.

2.2 Virtual Private Network (VPN)

VPN merupakan sebuah metode untuk membangun jaringan yang menghubungkan antar jaringan secara aman dengan memanfaatkan jaringan publik. Contoh implementasi adalah ketika anda mengelola *network* yang terdiri dari beberapa kantor di lokasi yang berbeda. Akan membutuhkan biaya yang besar jika kita kemudian membangun *link wireless* atau *fiber optic* padahal bisa jadi antar kantor berada di luar atau bahkan pulau yang berbeda (Kaseger, 2017).

Dengan VPN, kita bisa membangun sebuah *link* antar kantor dengan memanfaatkan jaringan internet yang sudah ada. *Link* yang terbentuk dinamakan dengan enkripsi sehingga meminimalisir kemungkinan data akan di akses oleh orang yang tidak bertanggungjawab (Kaseger, 2017).

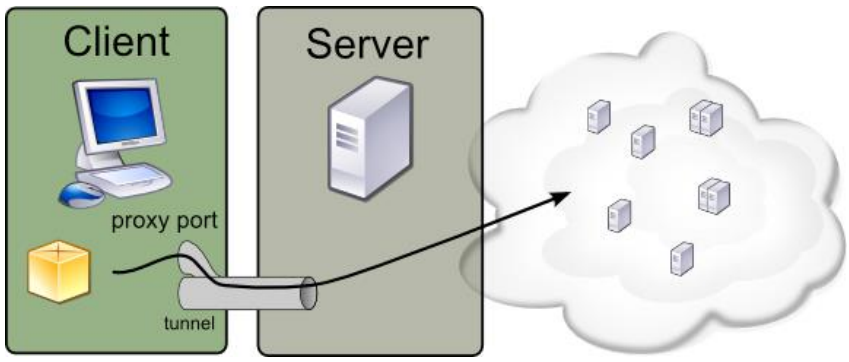


Gambar 2. 3 Konsep VPN

2.3 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 (Aldo, 2015).

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 jalur yang disebut *tunnel.*



Gambar 2. 4 Ilustrasi *tunneling*

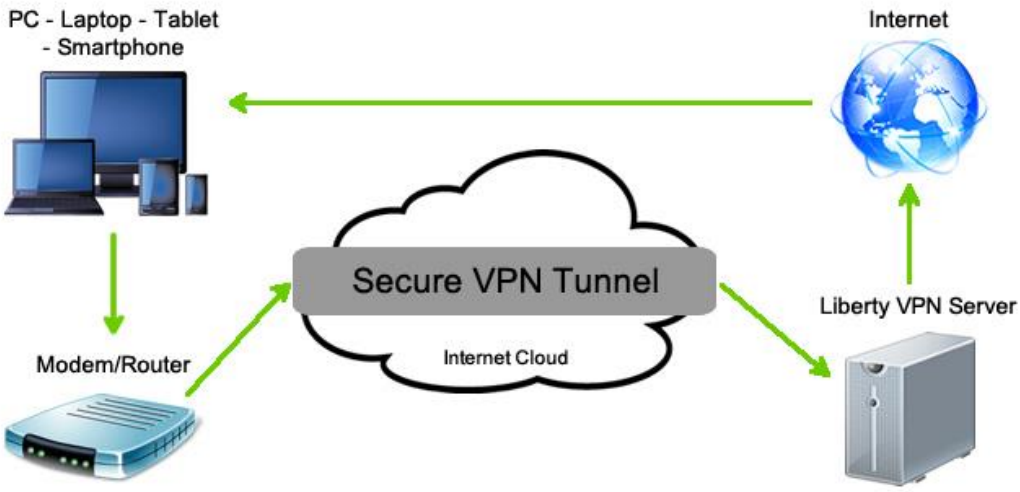
2.4 Secure Socket Tunneling Protocol (SSTP)

Secure Socket Tunneling Protocol adalah tembusan protokol yang tersedia pada *platform Microsoft.* Protokol ini berbasis pada kombinasi kedua teknologi SSL dan TCP. Teknlogi SSL menjaminkan tingkat keamanan transportasi dan integritas

lalu lintas, SSL pada *server* dikonfigurasikan sedemikian rupa sehingga hanya metode enkripsi terkuatlah yang diaktifkan. Sejak sesi SSTP, dalam kenyataannya sebuah sesi HTTPS, SSTP mungkin bisa digunakan melalui *firewall* atau ISP *throttling.* Di sisi lain, sejak SSTP beroperasi melalui TCP, dalam beberapa kasus akan dikendalikan IKEv2 atau protokol berbasis UDP lainnya. Secara keseluruhan, SSTP adalah pilihan terbaik dan dapat membantu menyelesaikan masalah konektivitas ataupun masalah kecepatan yang dimiliki. (Kaseger, 2017).

SSTP adalah protokol VPN yang stabil dan mudah digunakan, terutama disebabkan integrasinya ke dalam *windows*. SSTP adalah bentuk VPN *tunnel* yang menyediakan mekanisme untuk mengirimkan *traffic* PPP atau L2TP melalui sebuah saluran SSL 3.0. SSL menyediakan *transport-level security* dengan *key-negotiation*, enkripsi dan *traffic integrity checking.* Penggunaan SSL melalui *port* TCP 443 mengizinkan SSTP untuk melewati secara virtual semua *firewall* dan *proxy server* kecuali untuk otentikasi *web server* (Kaseger, 2017).

SSTP *server* harus diotentikasi selama fase SSL. SSTP *client* dapat secara opsional diotentikasi selama fase SSL, dan harus diotentikasi selama fase PPP. Penggunaan PPP mendukung metode otentikasi secara umum seperti EAP-TLS dan MS-CHAP. SSTP dapat diterapkan di *linux*, BSD, dan *windows.*

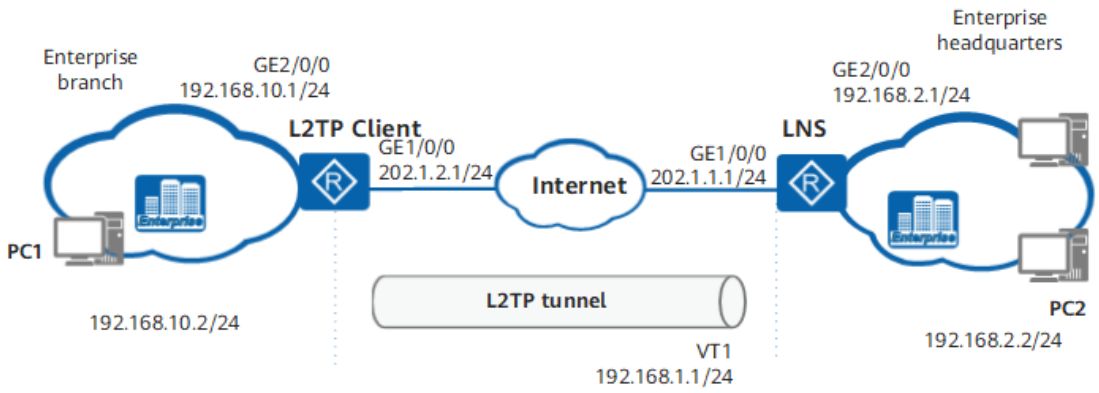


Gambar 2. 5 *Secure Socket Tunneling Protocol*

2.5 Layer Two Tunneling Protocol (L2TP)

L2TP merupakan *tunneling* protokol yang memadukan dua buah *tunneling* protokol yaitu *Layer 2 Forwarding* milik *Cisco* dan PPTP yang dimiliki oleh *Microsoft.* L2TP umumnya digunakan untuk membuat *Virtual Private Dial Network* (VPDN) yang dapat membawa semua jenis protokol komunikasi di dalamnya dan biasanya menggunakan *port* 1702 dengan protokol UDP (Fikri dkk 2016).

Terdapat dua model *tunnel* yang dikenal, yaitu *compulsory* dan *voluntary*. Perbedaan utama keduanya terletak pada *endpoint tunnel*-mya. Pada *compulsory tunnel*, ujung *tunnel* berada pada ISP, sedangkan *voluntary*, ujung *tunnel* berada pada *clien remote.*



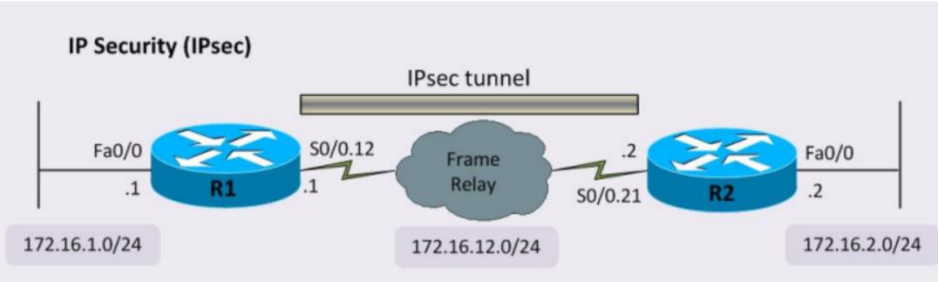
Gambar 2. 6 *Layer Two Tunneling Protocol*

2.6 Internet Protocol Security (IPSec)

IPSec merupakan *tunneling protocol* yang bekerja pada layer 3. IPSec menyediakan layanan sekuritas pada IP layer dengan mengizinkan sistem untuk memilih *protocol* keamanan yang diperlukan, algoritma apa yang akan digunakan pada layanan, dan menempatkan kunci kriptografi yang diperlukan untuk menyediakan layanan yang diminta. IPSec bekerja dengan tiga cara, yaitu *Network-to-network, Host-to-network dan Host-to-host* (Sahni dan Lukman, 2012).

IPSec adalah pengembangan dari protokol IP yang bertujuan untuk meyediakan keamanan pada suatu IP dan *layer* yang berada di atasnya. Pada dasarnya paket IP tidak memiliki keamanan, sehingga tidak ada jaminan bahwa paket yang diterima sama dengan paket ketika ditansmisikan oleh si pengirim paket. Paket IP yang tidak memiliki keamanan atau *security*, sangat mudah untuk diketahui isinya

dan alamat IP itu sendiri. IPSec adalah metode yang bertujuan untuk menjaga keamanan IP diagram ketika paket ditansmisikan pada *traffic.* Sehingga IPSec menjadi suatu mekanisme yang diimplementasika pada VPN. IPSec berada pada *layer 3* OSI yaitu *network layer* sehingga dapat mengamankan data dari *layer* yang berada di atasnya (Sridevi, 2013).



Gambar 2. 7 *lnternet Protocol Security*

2.7 Quality of Service (QoS)

Dari segi *networking,* QoS mengacu kepada kemampuan memberikan pelayanan berbeda kepada lau lintas jaringan dengan kelas-kelas yang berbeda. Tujuan akhir dari QoS adalah memberikan *network service* yang lebih baik dan terencana dengan *dedicated bandwidth*, *jitter* dan *latency* yang terkontrol dan meningkatkan *loss* karakteristik. Berikut adalah penjelasan mengenai parameter-parameter yang digunakan dalam penilaian QoS yang baik (Iskandar, 2015).

2.7.1 Delay

Delay adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak media fisik, kongesti atau juga waktu proses lama. Menurut versi TIPHON, besarnya *delay* dapat diklasifikasikan seperti yang ditunjukkan pada Tabel 2.1 (Iskandar, 2015).

Kategori	*Delay*	Indeks
Sangat Bagus	<150 ms	4
Bagus	150 s/d 300 ms	3
Sedang	300 s/d 450 ms	2
Jelek	>450 ms	1

Tabel 2. 1 *Delay*

Untuk mengukur *delay* digunakan persamaan.

$$Delay = \frac{Total\ delay}{Total\ paket\ yang\ diterima}$$

2.7.2 Jitter

Jitter atau variasi *delay* adalah variasi dari *delay* atau selisih antara *delay* pertama dengan *delay* selanjutnya. Jika variasi *delay* dalam transmisi terlalu lebar, maka akan mempengaruhi kualitas data yang ditransmisikan. Jumlah toleransi *jitter* dalam jaringan dipengaruhi oleh kedalaman dari *buffer jitter* dalam peralatan

jaringan. Jika *buffer jitter* tersedia lebih banyak, makan jaringan dapat mereduksi efek dari *jitter*.

Kategori	*Jitter*
Sangat Bagus	0 ms
Bagus	0 s/d 75 ms
Sedang	75 s/d 125 ms
Jelek	125 s/d 225 ms

Tabel 2. 2 *Jitter*

Untuk mengukur *jitter* digunakan persamaan

$$Jitter = \frac{Total\ Variasi\ Delay}{(Total\ Paket\ yang\ diterima - 1)}$$

Total variasi *delay* diperoleh dari penjumalahan

$$(delay\ 2 - delay\ 1) + (delay\ 3 - delay\ 2) + \cdots + (delay\ n - delay\ (n-1))$$

2.7.3 Packet Loss

Packet Loss merupakan parameter 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 efisiensi 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. Nilai *packet loss* sesuai dengan versi TIPHON ditunjukkan pada Tabel 2. 3.

Kategori	*Packet Loss*	Indeks
Sangat Bagus	0 %	4
Bagus	3 %	3
Sedang	15 %	2
Jelek	25 %	1

Tabel 2. 3 *Packet Loss*

Untuk mengukur *packet loss* digunakan persamaan

$$Packet\ Loss = \frac{Paket\ Total\ Tercapture - Paket\ Terkirim}{Paket\ Total\ Tercapture} \times 100\%$$

2.7.4 Throughput

Throughput yaitu kecepatan (*rate*) transfer data yng 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 (Iskandar, 2015).

Untuk mengukur *throughput* digunakan persamaan

$$Throughput = \frac{Jumlah\ Data\ yang\ di\ Kirim}{Lama\ Pengamatan}$$