BAB II
DASAR TEORI

2.1 KAJIAN PUSTAKA

Berikut beberapa penelitian yang dapat dijadikan acuan oleh peneliti dapat dilihat pada Tabel 2.1.

Tabel 2.1 Kajian Pustaka

No	Penulis	Judul Penelitian	Tahun	Hasil
1	Kaseger Arthur Farly, Xaverius B. N. Najoan, Arie S. M. Lumenta	Perancangan dan Implementasi VPN *Server* dengan menggunakan Protokol SSTP (*Secure Socket Tunneling Protocol*) Studi Kasus Kampus Universitas Sam Ratulangi	2017	Meneliti tentang bagaimana cara menghilangkan atau mengurangi berbagai tindak pencurian data informasi yang dilakukan melalui jaringan internet. VPN dipilih karena dapat menjamin keamanan dalam proses pengiriman data melalui jaringan internet. Berdasarkan hasil dari prosedur penelitian yang dilakukan menghasilkan sebuah produk VPN Server yang dapat diakses menggunakan jaringan internet, 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. Berdasarkan pengujian *Packet Loss* pada kedua

				protokol bahwa *Packet Loss* tergantug pada jumlah data dan kecepatan koneksi internet. Semakin sedikit data yang dikirimkan dan kecepatan internet 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.
2	Moezes Rasuanda, Haeruddin	Perbandingan Performa VPN Menggunakan PPTP dan SSTP *Over* SSL dengan Metode *Quality of Service*	2020	Membahas tentang perbandingan performa dari kedua protokol VPN yang sudah ditentukan yaitu protokol PPTP dan SSL, dengan menggunakan metode *Quality of Service* yang dimana metode ini adalah cara untuk mengukur seberapa baiknya jaringan tersebut dan juga memastikan pengguna mendapatkan kualitas dari servis yang terbaik. Menurut hasil penelitian yang dilaksanakan dapat

				disimpulkan bahwa kedua protokol mempunyai kelebihan dibidangnya masing-masing, serta juga memiliki kekurangan masing-masing diantaranya, VPN PPTP memiliki kelebihan yaitu mendukung semua sistem operasi desktop dan seluler, *set up* konfigurasi sederhana, dan memiliki kecepatan yang baik, kekurangannya mudah untuk diblokir oleh ISP karena tingkat enkripsi tidak begitu tinggi. Sedangkan VPN SSTP memiliki kelebihan mampu menembus *firewall*, dan terdukung penuh oleh sistem operasi Windows. Sedangkan kekurangan dari VPN ini ialah tidak bisa melakukan *backdoor*, dan sementara masih terfungsi hanya pada platform *Windows.*
3	Muhammad Naufal	Analisa Quality of Service Jaringan Vpn Menggunakan Protokol SSTP Dan	2018	Membahas tentang analisa QoS pada jaringan VPN berbasis protokol *Open*VPN dan SSTP yang menggunakan layanan FTP (*File Transfer Protocol)* dan video *streaming*. Pada penelitian ini ditemukan bahwa *delay* dan *jitter*

		*Open*VPN		pada *Open*VPN lebih kecil dibandingkan dengan SSTP pada layanan FTP, sedangkan pada video *streaming* keduanya sama. Selain itu, *throughput* pada *Open*VPN lebih besar dari SSTP saat menggunakan layanan FTP, sedangkan saat menggunakan video *streaming* keduanya bernilai sama. Adapun *packet loss* antara SSTP dan *Open*VPN bernilai sama pada layanan FTP maupun *video streaming.*
4	Chairul Umam, Emilia Roza, Irfan	Perancangan Jaringan Keamanan *Virtual Private Network* (VPN) *Site to Site*	2016	Meneliti tentang cara mengamankan data menggunakan protokol IPSec (*Internet Protocol Security*) pada VPN. Dari 2 kali penyerangan oleh *Man In The Middle Attack* dan *bruteforce* VPN PPTP di perusahaan "X" dapat memperlambat waktu untuk memecahkan kode *username* dan *password* dengan waktu 5 detik dengan menggunakan kode *password* lebih dari sama dengan (≥) 8-10 digit. Dari hasil yang telah didapat dapat disimpulkan bahwa model jaringan VPN *Site to Site* akan mewujudkan akses data yang

				aman bagi perusahaan serta membuat jaringan yang terjamin keamanannya dari serangan *Man In The Middle Attack* dan *Bruteforce*. Dengan menggunakan *password* 8-10 digit akan dapat memperlambat serangan *hacker* untuk membaca *username* dan *password* selama 5 detik. Dengan waktu selama 5 detik, *admin* harus mampu memutus serangan tersebut dengan *Wireshark.*
5	Nurcahyo Budi Nugroho, Zulfian Azmi, Saiful Nur Arif	Aplikasi Keamanan Email Menggunakan Algoritma RC4	2016	Membahas tentang bagaimana cara mengamankan keamanan pesan pada *email.* Dalam penelitian ini penulis menggunakan Algoritma kriptografi *Rivest Code* 4 (RC4) yang merupakan salah satu algoritma kunci simetris dibuat oleh RSA Data *Security Inc* (RSADSI) yang berbentuk stream *chipper* yang memproses unit atau *input* data, pesan atau informasi pada satu saat. Kesimpulan yang dapat diambil setelah melakukan penelitian adalah pada *body e-mail* bisa di *enkripsi* dan di dekripsi dengan valid dan berjalan baik menggunakan algoritma RC4.

				Sistem yang dibuat sudah mampu memenuhi kebutuhan aplikasi *e-mail client* yang menerapkan kriptografi RC4. Aplikasi *E-mail Client* ini langsung menampilkan *Form* Koneksi sehingga memudahkan dan cara kerja aplikasi ini sangat cepat dalam mengirimkan *E-mail* tanpa harus membuka *browser*.

2.2 JARINGAN KOMPUTER

Jaringan komputer merupakan sistem yang menghubungkan beberapa komputer untuk berbagi informasi (data) dan sumber daya [6]. Untuk membuat sebuah jaringan, beberapa komputer dengan lainnya disambungkan menggunakan media kabel atau nirkabel. Selain itu, perangkat lunak atau *software* juga diperlukan sebagai pendeteksi perangkat yang berada di satu jaringan. Fungsi dari jaringan komputer yang paling sederhana adalah memudahkan beban kerja perangkat untuk menjalankan sebuah program. Selain itu fungsi lainnya adalah mampu menghemat sumber daya.

2.2.1 Macam-macam Jaringan Komputer

Menurut [7] dalam jurnalnya menuliskan bahwa ada beberapa macam-macam jaringan komputer, akan tetapi penulis hanya mengambil 4 contoh yang biasa digunakan diantaranya :

a) *Local Area Network* (LAN)

Sebuah jaringan yang menghubungkan perangkat dalam yang memiliki jarak berdekatan dan menggunakan kabel sebagai saluran utamanya. Karena jaringan LAN tidak bergantung pada sinyal maka kecepatan yang dihasilkan sangat stabil dibanding *Wireless Local Area Network* (WLAN).

b) *Wireless Local Area Network* (WLAN)

Sebuah jaringan yang bisa dibilang sama dengan jaringan LAN, akan tetapi jaringan jenis ini menggunakan pancaran sinyal radio yang dimana tingkat kecepatan bergantung pada jarak dari *router* ke *device* pengguna atau bisa disebut dengan jaringan tanpa kabel.

c) *Wide Area Network* (WAN)

Jenis jaringan yang menghubungkan beberapa perangkat, komputer, atau berbagai macam tipe jaringan lainnya (seperti LAN dan WLAN), dalam jangkauan yang cukup jauh. WAN juga bisa digunakan untuk mencakup program-program di beberapa negara berbeda.

d) *Personal Area Network* (PAN)

Jaringan komputer yang biasanya menghubungkan berbagai perlengkapan elektronik milik pribadi yang dikelola oleh orang itu sendiri. Contoh : menghubungkan printer ke komputer atau menghubungkan komputer dengan *speaker Bluetooth*.

2.2.2 Kegunaan Jaringan Komputer

Menurut penelitian [8] jaringan komputer memiliki beberapa kemampuan diantaranya :

a) *Resource Sharing*, dengan adanya jaringan komputer, berbagi *resource* bisa dilakukan tanpa terkendala jarak. *Resource sharing* meliputi :

`1. Data *Sharing*, dapat berbagi data dengan mudah seperti, dokumen, video dll.

2. Hardware Sharing, contohnya satu *printer* bisa digunakan oleh beberapa komputer sekaligus.

1. *Internet Access Sharing*, jaringan komputer memungkinkan beberapa komputer berbagi satu koneksi internet.

b) *Connectivity and Communication*, komunikasi antar *user* bisa terjadi ketika terdapat jaringan yang sudah terbentuk atau sudah terhubung.

c) *Data Security and Management*, data akan menjadi lebih aman dan lebih mudah apabila disimpan secara tepusat menggunakan *Shared Server*. Dengan cara seperti itu, karyawan akan lebih mudah dalam mencari data. *Administrator* juga

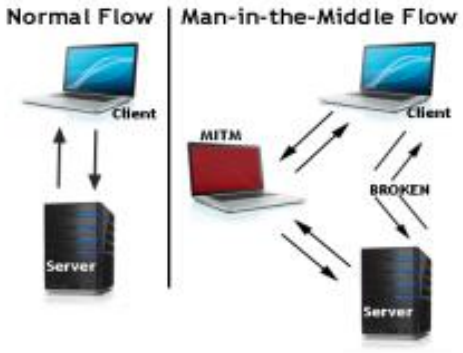
dapat memastikan bahwa data di *backup* secara *regular,* serta memungkinkan untuk menerapkan *security* dengan cara menentukan siapa yang boleh membaca atau menulis data yang bersifat penting.

2.3 SERANGAN JARINGAN

Menurut penelitian [9] menjelaskan bahwa biasanya serangan terhadap keamanan jaringan VPN antara lain :

a) Man In The Middle Attack

Main In The Middle Attack (MITM) adalah serangan dimana *attacker* berada di tengah bebas mendengarkan dan mengubah percakapan antara dua pihak. Serangan *Main In The Middle Attack* suatu tipe serangan yang memanfaatkan kelemahan *Internet Protocol.* Konsep dasar serangan ini adalah penyerang berada di tengah-tengah atau diantara dua komputer yang saling berkomunikasi, sehingga secara teknis memungkinkan penyerang untuk melihat, mengubah, dan mengontrol data yang dikirim antar dua komputer tersebut, mesin penyerang secara fisik tidak harus terletak diantara dua komputer, namun rute -paket yang dikirimkan atau ditujukan kepada *host* lain harus melalui mesin penyerang. Serangan *Main in the Middle Attack* dapat dilihat pada gambar 2.1 dibawah ini:



Gambar 2.1 Serangan *Main In The Middle Attack* [9]

Ada beberapa macam serangan kejahatan di dunia maya yang termasuk dalam kegiatan *Main In The Middle* antara lain sebagai berikut :

1. *Sniffer,* dikenal juga sebagai *Network Analyzers* atau *Ethernet Sniffer* adalah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer. Aplikasi ini

menangkap tiap-tiap paket dan menguraikan isi dari *Request for Comments* (RFC) atau spesifikasi yang lain.

2. *Spoofing,* situasi dimana seseorang berhasil menyamar sebagai *user* dengan memalsukan data.
3. *Interception,* ancaman terhadap *secrecy* yang dimana pihak ketiga yang tidak berhak dapat mengakses informasi dari dalam sistem komputer.
4. *Modification,* ancaman terhadap *integrity* dimana pihak ketiga yang tidak berhak dapat mengakses dan mengubah suatu informasi.
5. *Fabrication,* menambahkan objek atau informasi palsu pada informasi yang asli, sehingga data atau informasi berubah.

b) Bruteforce

Bruteforce attack adalah metode peretasan yang dilakukan menggunakan cara *trial* dan *error* untuk memecahkan kata sandi, kredensial *login*, maupun kunci *enkripsi*. Upaya yang dilakukan dalam serangan ini adalah melakukan tindakan secara paksa secara berlebihan untuk mendapatkan akses ke suatu akun [10]. Peretas akan mencoba beberapa nama pengguna dan kata sandi sehingga menemukan informasi *login* yang benar. *Password* dapat dibongkar dengan menggunakan program yang disebut *Password Cracker*. Program *Password Cracker* adalah program yang mencoba membuka sebuah *password* yang telah ter-*enkripsi* dengan menggunakan sebuah algoritma tertentu dengan cara mencoba semua kemungkinan [9].

c) *Denial of Service* (DoS)

DoS dapat diartikan sebagai serangan yang dilakukan dengan cara memenuhi lalu lintas jaringan internet pada server, sistem atau jaringan. Konsep yang digunakan adalah dengan membuat lalu lintas server berjalan dengan beban yang berat sampai tidak bisa lagi menampung koneksi dari *user* lain (*overload*). Konsep DoS dibagi menjadi 3 tipe , yaitu sebagai berikut :

1. *Request Flooding,* Teknik yang digunakan dengan memperbanyak *request,* akibatnya pengguna lain yang sudah saling terhubung tidak dapat dilayani.
2. *Traffic Flooding,* Teknik yang digunakan dengan cara memperbanyak data.
3. Mengubah sistem konfigurasi.

2.4 KEAMANAN JARINGAN

Keamanan jaringan adalah suatu cara yang digunakan untuk memberikan perlindungan terhadap sistem agar terhindar dari serangan pihak-pihak yang tidak bertanggung jawab yang ingin melakukan pencurian data. Tujuannya adalah untuk melindungi data yang telah tersimpan didalam database. Dengan adanya *network security*, resiko tersebut dapat dikurangi. Suatu jaringan didesain sebagai komunikasi data *highway* dengan tujuan meningkatkan akses ke sistem komputer, sementara keamanan didesain untuk mengontrol akses. Penyediaan *network security* adalah sebagai aksi penyeimbang antara *open acces* dengan *security* [11].

2.5 *VIRTUAL PRIVATE NETWORK* (VPN)

VPN merupakan salah satu alat yang dibuat untuk membangun jalur komunikasi yang aman antara *client* dan *remote* server melalui jaringan publik. VPN digunakan untuk menghubungkan dua titik dengan satu kabel atau satu jalur internet yang terhubung langsung meskipun secara fisik jauh [1]. VPN dapat menghubungkan dua buah kantor dengan menggunakan IP lokal yang sama, dimana IP lokal disini dapat mengakses *file server* lokal yang ada di kantor cabang lain atau printer cabang lain menggunakan VPN. Dalam pemasangan VPN IP server menggunakan IP lokal bukan IP publik. VPN dicetuskan pertama kali oleh seorang karyawan *Microsoft* pada Tahun 1996 dengan tujuan untuk menghubungkan dua komputer dengan metode *peer-to-peer tunnelling protocol* (PPTP) [12].

Cara kerja VPN adalah menyembunyikan alamat *Internet Protocol* (IP *address*) dengan mengubah jalur koneksi untuk melewati sebuah server milik sebuah penyedia VPN yang berada di lokasi berbeda. Singkatnya, VPN mengubah data-data menjadi angka yang tidak beraturan sehingga tidak sembarang orang dapat mengambil informasi di dalamnya. VPN memiliki beberapa fungsi diantaranya :

a. Mengamankan identitas pribadi, *enkripsi* data yang dilakukan VPN akan menghalangi pihak-pihak ketiga dari membaca informasi pribadi.

b. Membuka situs yang diblokir,
c. Mengamankan data di jaringan publik,
d. Meng-*enkripsi* data, saat menggunakan VPN seluruh data pribadi akan di-*enkripsi*. *Enkripsi* adalah proses penyamaran data menjadi angka dan huruf acak sehingga tidak dapat dibaca secara langsung. Untuk membaca data tersebut, diperlukan kunci *enkripsi* sehingga hanya pihak-pihak tertentu yang dapat membaca data tersebut.
e. Mengakses konten regional, dengan adanya VPN dapat mengatur lokasi dari berbagai wilayah untuk mengakses konten regional daerah tersebut.

VPN juga memiliki beberapa kelebihan dan kekurangan, diantaranya dapat dilihat pada Tabel 2.2

Tabel 2.2 Kelebihan dan Kekurangan VPN [12]

Kelebihan VPN	Kekurangan VPN
Informasi pribadi terjaga	Kecepatan internet berkurang
Keamanan koneksi yang lebih baik	Sambungan internet tidak stabil
Dapat mengakses web yang diblokir	Adanya batas penggunaan VPN
Membuka akses ke konten regional	Memerlukan pengaturan manual

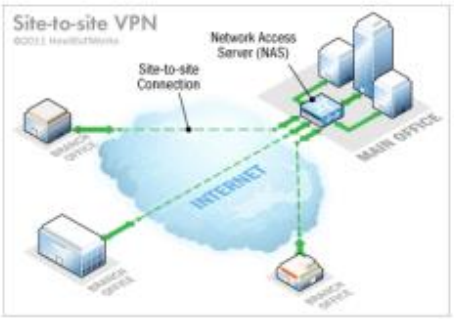
2.5.1 Tipe-tipe VPN

Secara umum VPN terbagi menjadi beberapa macam, yang sering digunakan ada 2 macam yaitu :

a. *Remote-Access* VPN, dikenal sebagai *Virtual Private Dial-Up Network* (VPDN) koneksi *user-to-LAN* yang digunakan oleh perusahaan untuk para pekerjanya yang membutuhkan koneksi ke jaringan mereka dari berbagai lokasi *remote*. Berikut dapat dilihat gambar 2.2 VPN *Remote Access* di bawah ini:

Gambar 2.2 VPN *Remote Access* [8]

b. *Site-to-Site* VPN, dengan adanya penggunaan perlengkapan *dedicated* dan *enkripsi* skala besar, sebuah perusahaan dapat mengkoneksikan *multi site* tetap melalui sebuah jaringan publik seperti internet [9]. Berikut dapat dilihat gambar 2.3 VPN *Site-to-Site* di bawah ini:



Gambar 2.3 VPN *Site-to-Site* [8]

2.5.2 Metode *Security* VPN

Dalam menjalankan pekerjaannya VPN memiliki beberapa metode security, diantaranya :

1. *Firewall*

Sebuah sistem keamanan pada jaringan komputer yang memiliki tugas untuk melindungi komputer dari serangan virus, *malware*, dan jenis serangan lainnya yang dapat membahayakan sebuah sistem. *Firewall* juga dapat diset untuk melindungi *port-port* koneksi terbuka, memeriksa tipe paket-paket mana yang perlu diteruskan, dan protoko-protokol mana yang diizinkan. *Firewall* terbagi menjadi beberapa macam diantaranya :

a. *Next-generation firewall,* terbagi menjadi 3 fitur utama yaitu, pemeriksaan detail paket, mengevaluasi sumber dari paket, dan menentukan penilaian identitas. *Firewall* jenis ini memiliki 3 jenis yaitu, perangkat keras (*hardware),* perangkat lunak (*software*), dan *cloud.*
b. *Packet-Filtering firewall,* berjalan dengan cara memeriksa paket sistem. Proses pemeriksaan meliputi IP *address,* nomor *port,* tipe, dan lainnya. Kelebihannya adalah ringan dan tidak mempengaruhi performa dari sistem.
c. *Proxy firewall,* disebut juga dengan *application-level gateaway. Firewall* ini bekerja dengan memproses sumber paket beserta isi paketnya. Pada *firewall* ini dapat memberikan keamanan akan tetapi hal ini dapat memperlambat kinerja sistem.
d. *Stateful inspection firewall,* memiliki fungsi memeriksa sumber paket dan membuka isi paket itu sendiri . *Firewall* ini bisa dibilang sama seperti dengan *proxy firewall* [13].

2. Enkripsi (*Encryption)*

Metode yang digunakan untuk mengubah informasi menjadi kode rahasia yang menyembunyikan makna sebenarnya dari informasi tersebut. Enkripsi juga dapat diartikan sebagai proses penyandian (*encoding*) data yang diambil dari satu komputer ke komputer lain. Data yang disandikan ke bentuk tertentu yang tidak mudah untuk dibaca dan hanya penerima yang sah saja yang dapat mengembalikan sandi ke bentuk semula, atau disebut juga dengan *encode* [9]. Ilmu mengenkripsi dan mendeskripsi informasi disebut dengan kriptograsi. Dalam komputasi, data yang terenkripsi juga dikenal sebagai *plaintext,* dan data yang terenkripsi disebut *ciphertext.* Rumus yang digunakan untuk menyandikan disebut dengan enkripsi atau sandi [14].

3. *Internet Protocol Security Protocol* (IP*Sec*)

Menurut [15] adalah sebuah protokol yang digunakan untuk mengamankan transmisi datagram dalam sebuah *ineternetwork* berbasis TCP/IP. Mendefinisikan beberapa standar untuk melakukan enkripsi data dan juga integritas data pada lapisan kedua *Reference Model* (*Internetwork* layer). IP*sec* melakukan *enkripsi* terhadap data

pada lapisan yang sama dengan protokol IP dan menggunakan teknik *tunneling* untuk mengirimkan informasi melalui jaringan Internet atau dalam jaringan Intranet secara aman. IPSec mendukung dua buah sesi komunikasi keamanan yakni :

a. Protokol *Authentication Header* (AH), menawarkan autentifikasi pengguna dan perlindungan dari beberapa serangan juga menyediakan fungsi autentikasi serta integritas terhadap data. Informasi AH dimasukkan ke dalam *header* paket IP yang dikirimkan dan digunakan secara sendirian atau bersamaan dengan protokol *Encapsulating Security Payload*.
b. Protocol *Encapsulating Security Payload* (ESP), protokol ini melakukan enkapsulasi serta enkripsi data pengguna untuk meningkatkan kerahasiaan data [9].
4. Server AAA (*Authentication, Authori-zation and Accounting*) banyak di-implementasikan untuk memberikan akses yang lebih aman dalam sebuah *environment remote-remote* VPN.

Teknologi VPN didukung oleh beberapa protokol keamanan salah satunya adalah *Remote Authentication Dial-In User Service* (RADIUS). *Radius server* digunakan dalam implementasi *remote-access* VPN karena pada RADIUS terdapat fungsi *authentication* (siapa anda), *athorizathion* (apa yang boleh dilakukan) dan *accounting* (apa yang sebenarnya dilakukan) [16]. Pada proses *authentication* menawarkan proses otentikasi *user, authorizthion* menawarkan *access control* untuk *user* dan *accounting* digunakan untuk melacak konsumsi *network-resorce* yang dilakukan *user*. Dengan adanya proses mekanisme tersebut dapat meningkatkan sistem keamanan jaringan [8].

2.5.3 Macam-macam VPN

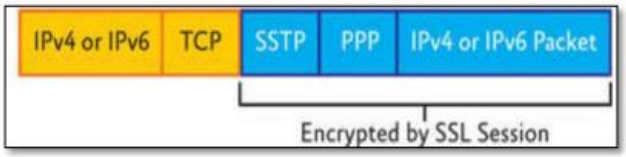
Berikut beberapa jenis VPN di Mikrotik :

a. PPTP, komunikasi PPTP menggunakan protokol TCP port 1723 dan menggunakan IP protokol 47/GRE untuk enkapsulasi datanya.
b. SSTP, komunikasi SSTP menggunakan TCP port 443 (SSL), sama halnya seperti *website* yang *secure* (http).

c. L2TP, komunikasi L2TP menggunakan UDP port 1701. *Network security* protokol dan enkripsi yang digunakan untuk autentikasi sama dengan PPTP. Biasanya untuk keamanan yang lebih baik, L2TP dikombinasikan dengan IPSec menjadi L2TP/IPSec.
d. OpenVPN, secara *default Open*VPN menggunakan UDP port 1194 dan dibutuhkan *certificate* pada masing-masing perangkat untuk terkoneksi [1].

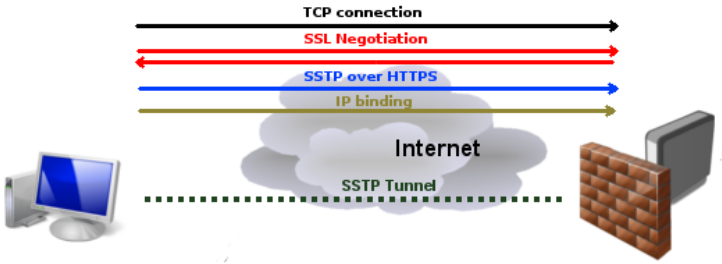
2.6 *SOURCE SOCKET TUNELLING* (SSTP)

Jenis VPN ini hampir sama dengan jenis VPN PPTP hanya saja SSTP ini merupakan tembusan protokol yang tersedia pada *platform Microsoft.* Protokol ini berbasis pada kombinasi kedua teknologi yakni *Secure Socket Layer* (SSL) dan *Transmitter Control Protocol* (TCP). Teknologi SSL menjaminkan transportasi dan integritas lalu lintas. SSL pada server dikonfigurasikan sedemikian rupa sehingga hanya metode *enkripsi* terkuatlah yang diaktifkan [18]. VPN ini memanfaatkan *port* yang sama dengan HTTPS yaitu port TCP 443 dimana seolah-olah aksesnya ke *website* HTTPS sehingga jarang sekali *port* ini diblokir. SSTP juga dapat terkonek apabila *server* dan IP publiknya berbeda. Akan tetapi SSTP tidak sefleksibel PPTP karena untuk saat ini tidak semua fitur *operating system* menyediakan fitur SSTP *client* [19]. Berikut dapat dilihat pada gambar 2.4 mengenai struktur paket SSTP dibawah ini:



Gambar 2.4 Struktur Paket SSTP [18]

Gambar 2.4 menunjukkan SSTP mengenkapsulasi *frame* PPP dalam bentuk IP datagram yang nantinya akan dikirimkan melalui jaringan. SSTP menggunakan koneksi TCP (melalui port 443) untuk manajemen *tunne*l-nya. Sedangkan untuk *enkripsi* menggunakan SSL milik protokol HTTPS [4].



Gambar 2.5 Mekanisme Koneksi SSTP [18]

Mekanisme koneksi SSTP pada Gambar 2.5 adalah sebagai berikut :

- Sambungan TCP terbentuk dari *client* ke *server* (secara *default* pada port 443).
- SSL memvalidasi sertifikat server. Jika sertifikat adalah koneksi yang valid dibuat maka koneksi akan dilanjutkan.
- Klien mengirimkan paket kontrol SSTP dalam sesi HTTPS yang menetapkan SSTP di kedua sisi.
- Negosiasi PPP atas SSTP *client* mengotentikasi ke *server* dan mengikat alamat IP ke i*nterface* SSTP.
- Terowongan SSTP sekarang sudah ada dan enkapsulasi paket bisa dimulai [18].

SSTP memiliki beberapa kelebihan diantaranya :

a. Mampu menerobos banyak *firewall.*
b. Taraf keamanannya tergantung dari sandi, akan tetapi umumnya sudah cukup aman.
c. Terintegrasi secara penuh ke dalam *system* operasi windows.
d. Didukung oleh *Microsoft* [5].

2.6.1 IP Public

Ip Public adalah alamat *ip* yang digunakan dalam jaringan internet. *Ip* ini diakses melalui jaringan internet secara langsung. *Ip public* didapat dari mendaftarkan diri ke salah satu ISP. Perangkat yang menggunakan alamat *ip public* seperti *web server, mailserver, DNS Server, game server* dan perangkat lain yang dapat diakses melalui jaringan internet [8].

2.6.2 IP Private

Ip private adalah alamat *ip* yang digunakan pada jaringan lokal. Untuk dapat terhubung ke internet maka diperlukannya router yang mempunyai kemampuan dapat melakukan (*Network Address Translation)* NAT. Dengan kata lain *ip private* dapat terkoneksi dengan internet menggunakan *ip public* yang terkoneksi secara langsung ke internet. Meskipun sudah terkoneksi internet alamat *ip private* tidak bisa diakses langsung dari jaringan internet. Contoh perangkat yang terhubung ke jaringan LAN seperti, printer, komputer, dll [8].

2.6.3 Enkripsi Algoritma RC4

Algoritma *Kriptografi Rivest Code* 4 merupakan algoritma yang dibuat oleh RSA Data *Security Inc* (RSADSI) yang berbentuk *stream cheaper.* RC4 menggunakan Panjang kunci dari 1 sampai 256 *byte* yang digunakan untuk menginisialisasikan *table* sepanjang 256 *byte.* RC4 merupakan jenis *stream chipper* yang digunakan untuk memproses *unit* atau *input* data pada satu saat. Cara *enkripsi* atau deskripsi ini dapat dilaksanakan pada panjangnya *variable.* Tidak harus menunggu sejumlah data tertentu untuk diproses atau menambahkan *byte* untuk di-*enkripsi* [20].

2.7 ROUTER

Router beroperasi pada lapisan jaringan 3 dari model OSI *layer*. *Router* mampu menghubungkan jaringan yang sama dan yang berbeda. Dalam *router* terdapat alamat jaringan sendiri serta menjadi *node* dalam jaringan. *Node* lain mengirim paket ke *router,* yang kemudian isi paket akan diperiksa lalu diteruskan dengan tepat. Router juga dapat digunakan untuk menentukan rute terpendek ke suatu tujuan dan menggunakannya [8].

2.8 WIRESHARK

Alat yang digunakan untuk menganalisa kinerja jaringan termasuk protokol didalamnya. *Interface* yang digunakan pada aplikasi *Wireshark* adalah *Graphical User Interface* (GUI) atau tampilan grafis. Semua jenis paket informasi atau data

dapat ditangkap dan dianalisa dengan mudah. Sehingga banyak tool ini digunakan untuk *sniffing* (memperoleh informasi penting seperti *password, e-mail,* atau *account* lain) [9].