Informatics, Science, and Technologies Journal

Vol 12 No 2 (2022) **Jurnal GERBANG STMIK Bani Saleh**
ISSN : 0853 – 6376
E-ISSN : 2622 – 3708

PENERAPAN LAYANAN PUBLIK MENGGUNAKAN SECURE SOCKET TUNNELING PROTOKOL (SSTP)

Subandri[1], Khusnul Khotimah[2], Kresno Murti Prabowo[3]
[1]Teknik Informatika, STMIK Bani Saleh, andrisubandri@ymail.com
[2]Teknik Informatika, STMIK Bani Saleh, unulj28@gmail.com
[3]Teknik Informatika, STMIK Bani Saleh, kresnomurti1991@gmail.com

Abstrak

Internet merupakan sumber kehidupan bagi manusia di zaman yang serba canggih. Dasar utama dari internet pada browser yaitu website dengan protokol HTTP. Semua dapat dilakukan lewat website dengan mudah, mulai dari mencari berita, komunikasi, berbelanja dan lain sebagainya. Terkadang, apapun yang diakses membutuhkan data pribadi sebagai penjamin suatu akun. Maka dibutuhkannya keamanan agar data pribadi tidak disalahgunakan oleh orang yang tidak bertanggungjawab.

Sebuah teknologi VPN dapa tmengamankan jaringan. Banyak jenis yang terdapat pada VPN, salah satunya yaitu SSTP disertai sertifikat SSL. Tujuan dari penelitian ini adalah untuk mengamankan data pribadi pada protokol HTTP dengan menggunakan metode SSTP bersertifikat SSL. Dengan begitu, diharapkan data pribadi tidak dapat terlihat oleh aplikasi *sniffing* yaitu Wireshark.

Kata Kunci: *VPN, SSTP, HTTP, Wireshark*

Abstract

Internet merupakan sumber kehidupan bagi manusia di zaman yang serba canggih. Dasar utama dari internet pada browser yaitu website dengan protokol HTTP. Semua dapat dilakukan lewat website dengan mudah, mulai dari mencari berita, komunikasi, berbelanja dan lain sebagainya. Terkadang, apapun yang diakses membutuhkan data pribadi sebagai penjamin suatu akun. Maka dibutuhkannya keamanan agar data pribadi tidak disalahgunakan oleh orang yang tidak bertanggungjawab.

Sebuah teknologi VPN dapa tmengamankan jaringan. Banyak jenis yang terdapat pada VPN, salah satunya yaitu SSTP disertai sertifikat SSL. Tujuan dari penelitian ini adalah untuk mengamankan data pribadi pada protokol HTTP dengan menggunakan metode SSTP bersertifikat SSL. Dengan begitu, diharapkan data pribadi tidak dapat terlihat oleh aplikasi *sniffing* yaitu Wireshark.

Keywords: *VPN, SSTP, HTTP, Wireshark*

Vol 12 No 2 (2022) **Jurnal GERBANG STMIK Bani Saleh**
ISSN : 0853 – 6376
E-ISSN : 2622 – 3708

I. Pendahuluan

Semakin bertambahnya waktu bertambah pula teknologi dari bidang jaringan, termasuk dalam mengakses internet. Semua bias kita lakukan di internet seperti belajar, belanja, mencari artikel, hingga absensi. Pada umumnya layanan publik yang biasa kita gunakan adalah HTTP (*Hypertext Transfer Protocol)*. Pada website HTTP ini kurang aman karena tidak memiliki fitur enkripsi seperti HTTPS (*Hypertext Transfer Protocol Secure*). Oleh karena itu, HTTP bias terdeteksi oleh aplikasi Wireshark.

Wireshark adalah sebuah aplikasi analisis yang memudahkan dalam monitoring jaringan. Semua konektivitas dapat dilihat secara terbuka karena tujuan dari Wireshark untuk monitoring paket data. Maka dari itu untuk mengamankannyakita perlu menggunakan VPN.

VPN *(Virtual Private Network)* adalah sebuah metode membangun jaringan berupa terowongan yang antar perangkatnya (node) memanfaatkan koneksi internet untuk saling berkomunikasi. Seolah – olah perangkat computer terhubung langsung oleh jaringan publikdengan membangun jalur khusus atau protocol tunneling sehingga koneksi point–to–point virtual pada VPN membuat lebih aman dalam pengiriman data yang bersifat informasi karena terdapat enkripsi didalamnya. Banyak macam pilihan metode VPN, salah satunyayaitu SSTP.

SSTP (*Secure Socket Tunneling Protocol*) adalah sebuah metode yang memanfaatkan enkripsinya yaitu SSL (*Secure Socket Layer*) untuk mengamankan paket data melalui jalur VPN. SSL sendiri perlu ditambahkan pada masing–masing router agar PC yang terhubung dengan router terenkripsi saat mengakses website HTTP. SSL bisa didapat dengan berlangganan kepada penyedia hosting atau membuat sertifikat sendiri pada Router OS mulai dari versi 6 karena sudah ditambahkan fitur untuk membuat sertifikat SSL.

II. Landasan Teori

2.1. Jaringan Komputer

Pada tahun 1940-an di Amerika yang digagas oleh sebuah proyek pengembangan komputer MODEL I di Laboratorium Bell dan group riset Universitas Hardvard yang dipimpin professor Howard Aiken melahirkan konsep jaringan komputer. 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 bisa dijalankan dalam sebuah computer dengan kaidah antrian.

Pada tahun 1950-an jenis komputer mulai berkembang sampai terciptanya super computer, maka sebuah computer harus melayani beberapa tempat yang tersedia (terminal), untuk itu ditemukan konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (Time Sharing System). Dengan ini pertama kalinya terbentuk jaringan (network) computer diaplikasikan. Sistem TSS menghubungkan beberapa terminal secara seri kesebuah perangkat (host) komputer. Proses TSS antara teknologi komputer dan teknologi telekomunikasi terlihat perpaduan yang pada awalnya berkembang sendiri – sendiri.

2.1.1. Jenis Jaringan

Penghubungan antar perangkat tergantung ruang lingkup wilayah dan kebutuhan, peneliti memerlukan beberapa jenis jaringan computer yaitu

Vol 12 No 2 (2022) **Jurnal GERBANG STMIK Bani Saleh**
ISSN : 0853 – 6376
E-ISSN : 2622 – 3708

2.1.1.1. Internet

Pada tahun 1960-an penelitian yang ditugaskan oleh Pemerintah Federal Amerika Serikat untuk membangun komunikasi yang kuat dan toleran terhadap kesalahan dengan jaringan komputer. ARPANET merupakan jaringan precursor utama yang awalnya berfungsi sebagai tulang punggung untuk interkoneksi jaringan akademik dan militer regional pada 1980-an. Pendanaan National Science Foundation Network sebagai tulang punggung baru pada 1980-an, serta pendanaan swata untuk ekstensi komersial lainnya, mendorong partisipasi dunia dalam pengembangan teknologi jaringan baru, dan penggabungan banyak jaringan.

Internet merupakan keharusan yang dimiliki setiap pengguna untuk media komunikasi dan pertukaran data. Penciptaan jaringan komputer terbesar oleh manusia adalah Internet karena ruang lingkupnya mencakup hingga ujung dunia. Siapapun dapat mengakses internet dengan perangkat komputer, seperti PC, laptop, smartphone, tablet, TV, dan sebagainya. Internet juga salah satu fasilitas umum yang terdapat pada warnet, cybercafe, hotspot, dan lain-lain.

2.1.1.2. Local Area Network (LAN)

Pada akhir 1960-an melakukan penelitian karena meningkatnya permintaan dan penggunaan komputer di Universitas dan Laboratorium, hasilnya menyediakan kebutuhan interkoneksi kecepatan tinggi antara system komputer. Tahun 1970 ada sebuah laporan dari Laboratorium Radiasi Lawrence yang merinci pertumbuhan jaringan “Gurita” mereka memberikan indikasi yang baik tentang situasi tersebut.

Local Area Network mencakup wilayah yang relative kecil, seperti sekolah, kantor, maupun rumah. Teknologi yang paling umum digunakan untuk jaringan area local yaitu Ethernet dan Wi-Fi. Oleh sebab itu media penghubungannya pun ada yang secara fisik (kabel) dan tanpa kabel (nirkabel).

2.1.1.3. Virtual Private Network (VPN)

Teknologi ini dikembangkan untuk menyediakan akses ke aplikasi dan sumber daya perusahaan untuk pengguna jarak jauh atau seluler, dan kekantor cabang. Untuk keamanan, koneksi jaringan pribadi dapat dibuat menggunakan protokol tunneling berlapis terenkripsi, dan pengguna mungkin diharuskan melewati berbagai metode otentikasi untuk mendapatkan aksesnya.

Jaringan pribadi maya dibuat dengan membuat koneksi poin ke poin maya melalui penggunaan sirkuit khusus atau dengan protocol terowongan melalui jaringan yang ada sehingga dapat diakses dari jarak jauh. Contoh implementasi adalah ketika seorang administrator mengelola beberapa kantor di lokasi yang berbeda sehingga menggunakan VPN bisa membangun sebuah link antar kantor dengan memanfaatkan jaringan internet yang sudah ada.

2.2. Router Mikrotik

Router merupakan sebuah alat yang menghubungkan dua jaringan atau lebih untuk meneruskan paket data dari satu jaringan ke jaringan lainnya. Mikrotik adalah sebuah perusahaan berkantor pusat di Latvia, yang dibentuk oleh Johnson Trully dan Armin Riekstins. Router sendiri memiliki system

Vol 12 No 2 (2022) **Jurnal GERBANG STMIK Bani Saleh**
ISSN : 0853 – 6376
E-ISSN : 2622 – 3708

operasi RouterOS yang diperuntukan sebagai network router. Router OS dapat digunakan untuk menjadikan komputer bisa menjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan *wireless*.

Administrasi bisa dilakukan melalui Windows Application (WinBox) dan penginstalasiannya dapat dilakukan pada standard computer PC (Personal Computer). Router berfungsi untuk mengelola lalu lintas data dan menghubungkan jaringan LAN kedalam suatu jaringan WAN. Tabel routing dapat mencatat semua alamat dalam jaringan karena router dapat menentukan jalur terbaik. Beberapa fitur yang bisa digunakan router Mikrotik seperti, Routing, Hotspot, PPTP, IPsec, DHCP, Web Proxy, SNMP, Tunnel, Firewall dan NAT.

2.3. Tunneling

Tunneling adalah dasar dari VPN untuk membuat suatu jaringan private melalui jaringan internet. Tunneling juga merupakan enkapsulasi atau pembungkusan suatu protocol kedalam paket protokol.

Tunneling menyediakan suatu koneksi point – to – point logis sepanjang jaringan IP yang bersifat *connectionless*. Proses transfer data dari satu jaringan kejaringan lain memanfaatkan jaringan internet secara terselubung (*Tunneling*). Ketika paket berjalan menuju ke node tujuan, paket ini melalui jalur yang disebut tunnel.

2.4. Secure Socket Tunneling Protocol (SSTP)

Secure Socket Tunneling Protocol adalah tembusan protokol yang tersedia pada *platform Microsoft*. Pada protocol ini dikombinasi dengan teknologi SSL dan TCP (*Transmission Control Protocol*) sehingga menggunakan port 443. Port tersebut juga seperti website yang secure (HTTPS). SSTP merupakan bentuk VPN tunnel yang melalui saluran SSL v3.0 untuk mengirimkan traffic PPP atau L2TP. SSL menyediakan *transport-level security* dengan *key-negotiation*, enkripsi dan *traffic integrity checking*.

SSTP *server* harus diotentikasi selama fase SSL sehingga 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*.

2.5. Wireshark

Wireshark adalah perangkat lunak penganalisis protocol jaringan dan banyak digunakan di dunia karena membantu para analis dalam melihat apa yang terjadi di jaringan pada tingkat mikroskopis dan merupakan standar *de facto* (dan sering kali *de jure*) di banyak perusahaan komersial, pemerintahan, dan pendidikan. Wireshark berkembang pesat berkat kontribusi sukarela dari pakar jaringan seluruh dunia dan merupakan kelanjutan dari proyek yang dimulai oleh Gerald Combs pada tahun 1998.

Wireshark adalah sebuah perangkat lunak yang memudahkan para analis untuk monitoring jaringan. Penulis menggunakan Wireshark untuk uji coba *sniffing* berupa akun *username* dan *password* dengan memanfaatkan fitur *TCP Stream*.

2.6. Microsoft Management Console (MMC)

Vol 12 No 2 (2022) **Jurnal GERBANG STMIK Bani Saleh**
ISSN : 0853 – 6376
E-ISSN : 2622 – 3708

Microsoft Management Console adalah sebuah perangkat lunak pembantu yang pada awalnya diperkenalkan dalam Windows NT 4.0 Option Pack yang menawarkan sebuah tempat untuk menyimpan semua perangkat bantu administrasi system operasi secara terintegrasi. *Snap-in* adalah sebuah komponen yang menyediakan beberapa kemampuan manajemen *server*, jaringan, atau aplikasi yang dapatdigunakan oleh administrator sehingga hamper semua program aplikasi yang tergabung dalam *Microsoft Back Office* menggunakan program ini untuk melakukan administrasi sistem.*Snap-in* yang paling sering digunakan adalah *Computer Management*, yang tersedia di dalam folder *Administrative Tools* dalam *Control Panel*. *Computer Management* berisi kumpulan beberapa *snap-in*, yang meliputi *Device Manager*, *Disk Management*, *Disk Defragmenter*, *Services Console*, dan lain-lain.

III. Analisis dan Perancangan Sistem

3.1. Analisis Jaringan

Jaringan yang digunakan pada penelitian ini adalah sebuah jaringan yang memiliki beberapa klien menggunakan metode VPN SSTP yang diterapkan di Topologi Bus. Pemanfaatan metode VPN SSTP diharapkan klien saat mengakses protokol HTTP terenkripsi oleh SSL yang terpasang pada perangkat klien dan router server.

3.1.1. Infrastruktur Fisik

Perangkat fisik menjadi factor utama dalam komunikasi antara satu perangkat dengan perangkat lainnya yang terhubung dengan jaringan internet. Pada penelitian ini menggunakan beberapa spesifikasi perangkat keras seperti berikut:

3.1.1.1. Hardware

a. Laptop

Laptop merupakan perangkat yang biasa digunakan untuk mengelola data atau komunikasi yang hasil outputnya bisa berupa tulisan dan gambar yang ditampilkan layar monitor. Penulis menggunakan 1 laptop dan Client yang dihubungkan dengan kabel UTP RJ45 guna untuk pengetesan saat mengakses website HTTP.

b. Router

Perangkat jaringan yang penulis gunakan yaitu router. Router merupakan alat untuk mengelola lalu lintas jaringan karena terdapat tabel routing yang dapat mencatat semua alamat dalam jaringan. Berbagai macam brand router yang ada, salah satu yang penulis gunakan yaitu Mikrotik. Penulis menggunakan RB941-2^{nD}-TC versi 6.48.6 yang nantinya terhubung dengan jaringan public menggunakan interface WLAN yang mendapatkan IP secara *dynamic* dan klien yang menggunakan VPN SSTP.

3.1.1.2. Media

Media merupakan penghubung perangkat keperangkat lainnya dengan jalur yang dibutuhkan. Berbagai macam jalur yang digunakan, ada yang menggunakan secara fisik (kabel) atau tanpa kabel (*nirkabel*). Berikut adalah media penghubung yang penulis gunakan:

Vol 12 No 2 (2022) **Jurnal GERBANG STMIK Bani Saleh**
ISSN : 0853 – 6376
E-ISSN : 2622 – 3708

a. Konektor UTP

Dalam penggunaan suatu perangkat, dibutuhkan media penghubung agar bisa saling berkomunikasi. Berbagai macam kabel jaringan yang bisa digunakan. Pada penelitian ini penulis menggunakan kabel UTP untuk menghubungkan antara router dengan PC sehingga memudahkan dalam konfigurasi. Berbagai macam jenis yang dapat digunakan, salah satunya yaitu RJ45. Penulis menggunakan RJ45 karena port jaringan yang tersedia pada Laptop jenis RJ45, dengan demikian dapat dihubungkan ke router yang digunakan.

b. Wireless

Wireless merupakan jalur telekomunikasi antar satu perangkat dengan perangkat yang lain tanpa menggunakan kabel (*nirkabel*). Saat ini banyak laptop atau telepon sellular digunakan sebagai hotspot atau penambat jaringan yang di sebarkan keperangkat lain untuk mengakses internet. Router menggunakan media wireless untuk mendapatkan akses ke internet. Dengan begitu, router dapat mendistribusikan jaringan keperangkat lain dengan konektor RJ45 dan *virtual tunneling*.

3.1.2. Infrastruktur Software

Penulis membutuhkan infrastruktur software untuk mengendalikan perangkat Router. Maka yang penulis gunakan yaitu:

a. Winbox

WinBox adalah sebuah perangkat lunak untuk mengelola, mengatur, dan konfigurasi Mikrotik Router OS menggunakan Mac Address atau protokol IP yang berbasis GUI (*Graphical User Interface*). Penulis mengkonfigurasi Router menggunakan Winbox yang terhubung dengan kabel UTP jenis RJ45.

b. Microsoft Management Console (MMC)

*Microsoft Management Console*atau MMC adalah sebuah perangkat lunak yang menyediakan tempat untuk menyimpan dan membantu administrasi system operasi secara terintegrasi. *Snap-in* adalah sebuah komponen yang digunakan untuk menambahkan komponen, salah satunya yaitu sertifikat. Penulis menambahkan sertifikat pada perangkat laptop agar saling terhubung antar perangkat dengan Router yang nantinya sertifikat tersebut dapat menerjemahkan paket data yang diakses melalui port HTTP.

c. Chrome

Banyak aplikasi browser yang bisa digunakan, salah satunya Chrome. Chrome merupakan aplikasi browser yang dikembangkan oleh Google. Banyak yang bisa dilakukan salah satunya yaitu pencarian website.

Website adalah sekumpulan halaman web yang saling berhubungan dengan berisikan informasi. Salah satu layanan yang berada pada website yaitu HTTP (*Hypertext Transfer Protocol*). Penulis menggunakan HTTP karena mudah untuk mendapatkan informasi data penting yang disimpan pada server web dengan menggunakan *software* Wireshark. Oleh

Vol 12 No 2 (2022) **Jurnal GERBANG STMIK Bani Saleh**
ISSN : 0853 – 6376
E-ISSN : 2622 – 3708

karenaitu, dengan memanfaatkan metode VPN SSTP dapat memberikan keamanan untuk data-data tersebut.

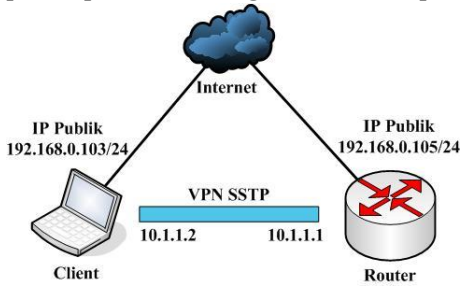
d. Wireshark

Wireshark adalah sebuah perangkat lunak yang memudahkan para analis untuk monitoring jaringan. Penulis menggunakan Wireshark untuk uji coba *sniffing* berupa akun *username* dan *password* dengan memanfaatkan fitur *TCP Stream*.

3.2. PerancanganJaringan

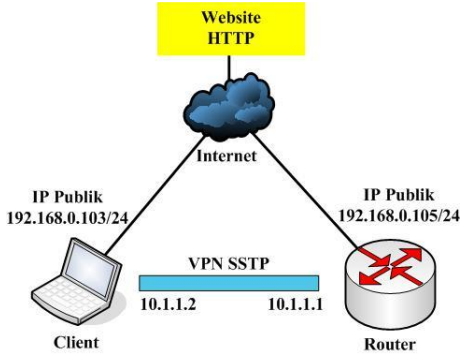
3.2.1. Topologi

Topologi merupakan sebuah metode yang membentuk suatu hubungan antar 1 komputer dengan perangkat lainnya menggunakan media kabel atau tanpa kabel (*nirkabel*) yang terhubung oleh jaringan internet. Topologi menjadi patokan untuk pengalamatan, gambaran penempatan serta bagaimana antar perangkat bisa saling terhubung.



Penulis menggunakan topologi pada gambar diatas yang merupakan jenis Topologi Bus. Pada umumnya dalam topologi bus menggunakan media kabel untuk penginstalasiannya, tetapi penulis hanya awalan saja menggunakan kabel untuk menghubungkan SSTP antara router dengan laptop. Setelah sudah terhubung menggunakan *tunneling*, maka kabel tidak diperlukan lagi karena pada saat laptop mengakses website HTTP otomatis melewati jalur SSTP.

3.2.2. Gambar Jaringan Logical



Internet merupakan bagian penting untuk mengakses port HTTP. Seperti gambar topologi (), internet yang didapat oleh Router berasal dari *hotspot* telepon selullar yang dihubungkan menggunakan interface WLAN yang tersedia. Port atau ether1 pada Router mengarah ke laptop / perangkat *client* melalui media UTP RJ45. Saat perangkat mengakses HTTP dipaksamelewatijalur*tunnel*sehinggaterenkripsi oleh sertifikat SSL yang telah di buat dan

Vol 12 No 2 (2022) **Jurnal GERBANG STMIK Bani Saleh**
ISSN : 0853 – 6376
E-ISSN : 2622 – 3708

ditambahkan pada SSTP Server serta laptop melalui perangkat *software Microsoft Management Console* (MMC).

Setelah sertifikat ditambahkan ke perangkat *client*, dibutuh jaringan tambahan yang menghubungkan perangkat *client* ke router yaitu membuat koneksi VPN yang bertipe SSTP beserta *user* dan *password* yang sudah dibuat Router pada PPP *Secret*. Agar bisa saling terhubung pada menu SSTP Server gunakan sertifikat yang sudah dibuat (CA) agar laptop dapat terhubung.

Untuk memastikan apakah laptop sudah terhubung dengan Router, bisa terlihat pada fitur PPP *Interface* dengan tanda DR (*Dyamic Running*) yang artinya terhubung secara dinamis dan bersifat aktif atau pada fitur PPP *Active Connections* dengan tanda L (*Local*).

3.2.3. Pengalamatan

IP Address merupakan alamat unik setiap host / perangkat yang terkoneksi oleh jaringan yang berbasis TCP/IP. IP Addess terbagi menjadi 2 versi, yaitu IPv4 (*Internet Protocol Version* 4) dan IPv6 (*Internet Protocol Version* 6). Pada penelitian ini penulis menggunakan IPv4 yang terbentuk dari 32 binary bits. IP publik yang digunakan kedua Router berasal dari *hotspot telephone celluler* agar terhubung satu dengan yang lainnya. Dengan konteks penelitian ini, untuk menghubungkannya secara aman yang melalui IP Publik dibutuhkan VPN. Pengalamatan VPN sendiri ada 2, yaitu parameter *local address* dan *remote address*. *Local address* untuk IP SSTP *router*, sedangkan *Remote address* untuk perangkat *client* (Laptop). Untuk detail pengalamatan yang digunakan seperti berikut:

Perangkat	Interface	IP Address
Wifi Rumah	Wireless	192.168.0.1/24
Router	WLAN	192.168.0.105/24
	VPN-SSTP	100.100.100.1
Laptop	Wifi	192.168.0.104/24
	VPN-SSTP	100.100.100.250

Pada Laptop menggunakan VPN akan mendapatkan range ip 100.100.100.2 – 100.100.100.250 karena sudah mengkoneksikan untuk jalur komunikasi melewati *virtual tunneling* dengan IP Pool yang sudah di tentukan.

IV. Hasil dan Pembahasan

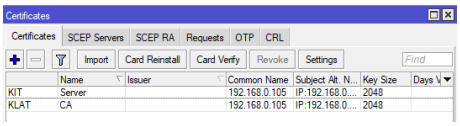
4.1. Pengkoneksian SSTP

4.1.1. Server

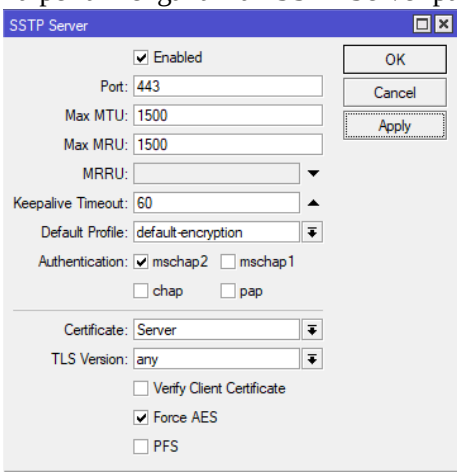
Penulis menggunakan aplikasi Winbox untuk monitoring jaringan yang terhubung, membua tsertifikat SSL dan jenis jaringan yang terhubung dengan Router Os. Awal mula agar router mendapatkan internet, penulis menggunakan interface WLAN untuk dikoneksikan dengan *Wi-Fi* rumah. Untuk mendapatkan IP secara otomatis (*dynamic*) maka menambahkan

Vol 12 No 2 (2022) **Jurnal GERBANG STMIK Bani Saleh**
ISSN : 0853 – 6376
E-ISSN : 2622 – 3708

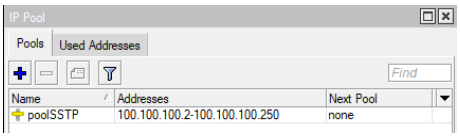
IP DHCP Client. Agar Laptop klien terhubung dengan SSTP, diperlukan sertifikat sebagai otentikasi dan keamanan.



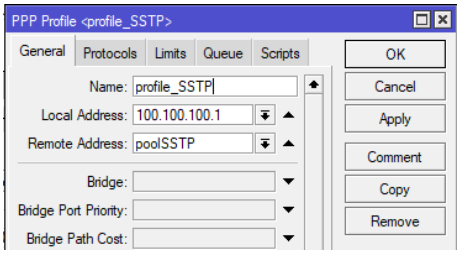
Setelah itu membuat sertifikat pada menu System > Certificates. Sertifikat yang dibuat (CA) akan di import yang nantinya di pasang pada perangkat client melalui aplikasi software MMC (*Microsoft Management Console*). Untuk menghubungkan perangkat client dan Router dengan jalur yang aman, maka perlu mengaktifkan SSTP Server pada menu PPP.



Klien SSTP bisa lebih dari satu, maka penulis menambahkan IP Pool agar banyak jumlah host tersedia yang bisa digunakan banyak klien.

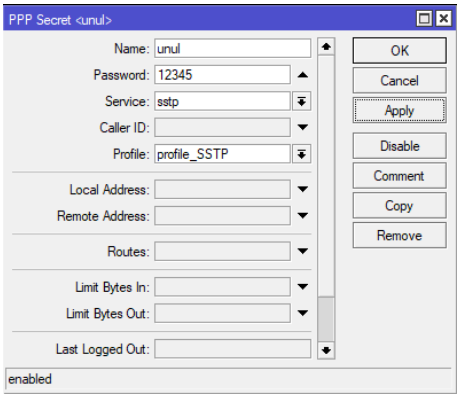


Selanjutnya membuat PPP Profile baru dengan remote address yang sudah dibuat pada IP Pool.



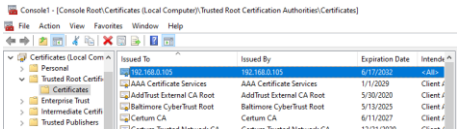
Berikutnya membuat PPP secret untuk klien mendapatkan otentikasi menggunakan name dan password yang dibuat disertai Profile yang sudah dibuat.

Vol 12 No 2 (2022) **Jurnal GERBANG STMIK Bani Saleh**
ISSN : 0853 – 6376
E-ISSN : 2622 – 3708

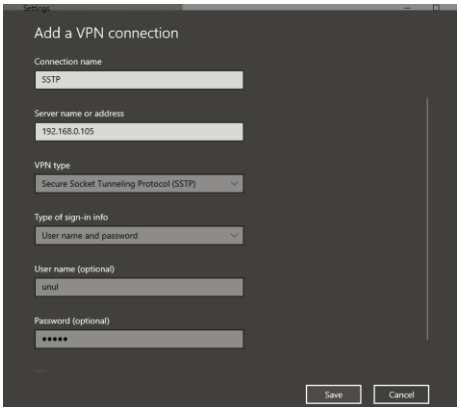


4.1.2. Client

Penulis menggunakan *Microsoft Management Console* untuk menambahkan sertifikat SSL yang sudah dibuat pada *router* agar penghubungan laptop dengan *router* melewati jalur *tunneling* SSTP sehingga mendapatkan enkripsi saat mengakses website dengan protokol HTTP. Caranya tekan tombol *windows* + R > ketik mmc, Lalu pilih *Add/Remove Snap-in* untuk meng-*install* sertifikat yang sebelumnya sudah di download pada menu Files *router*. *Import* sertifikat CA dan hasilnya seperti berikut

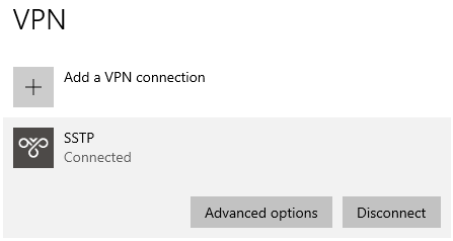


Setelah sertifikat ter-*install* pada perangkat klien, Langkah selanjutnya membuat koneksi VPN pada laptop dengan tipe SSTP beserta user dan password yang sudah dibuat pada menu PPP *Secretsrouter.*



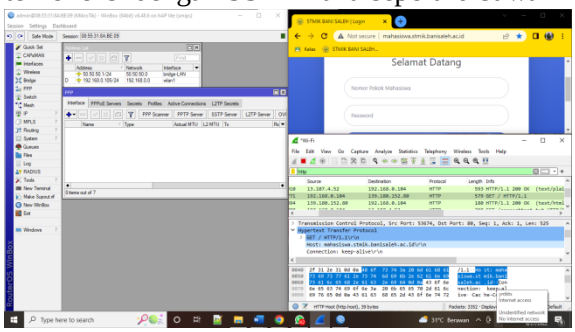
Dengan ini perangkat klien mendapatkan enkripsi secara optimal oleh SSTP dengan jalur *tunneling*.

Vol 12 No 2 (2022) **Jurnal GERBANG STMIK Bani Saleh**
ISSN : 0853 – 6376
E-ISSN : 2622 – 3708

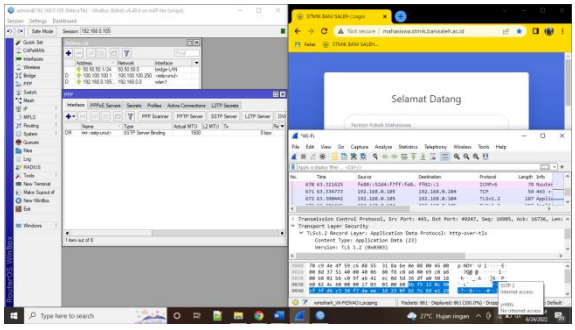


4.2. Hasil Pengujian

Penulis menggunakan website http://mahasiswa.stmik.banisaleh.ac.id/ merupakan url mahasiswa/I STMIK Bani Saleh untuk mendapatkan informasi perkuliahan, rincian pembayaran, hingga panduan skripsi. Tujuan penulis mengenkripsikan website tersebut agar tidak disalahgunakan oleh orang yang tidak bertanggungjawab seperti pengubahan password, mendapatkan informasi pribadi dan penyalahgunaan biodata yang tertera. Uji coba pendeteksian paket data sebelum dan sesudah melewati SSTP dapat dilihat menggunakan aplikasi Wireshark. Sebelum perangkat klien terkoneksi dengan SSTP maka seperti dibawah



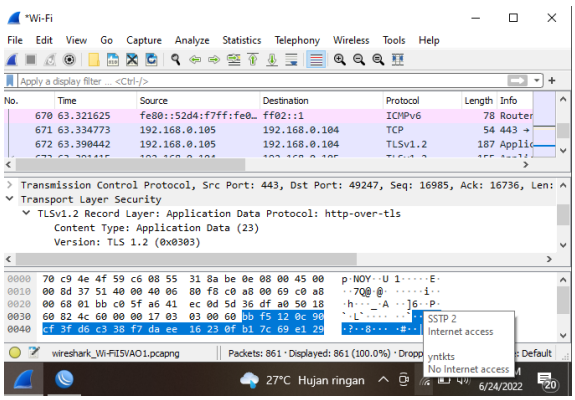
Hasil diatas sangat terlihat jelas bahwa IP yang mengakses (*source*), tujuan (*destination*), protokol yang diakses serta info apa saja yang terdapat pada protocol tersebut. Secara terbuka username dan password yang dimasukkan pengguna tidak terenkripsi sama sekali. Namun, setelah perangkat menggunakan jalur VPN dengan metode SSTP yang disertai oleh enkripsi SSL maka hasilnya seperti berikut



Untuk melihat dienkripsi seperti apa yang dilakukan oleh SSL maka dapat dilihat dengan mencari protokol TLS dan hasilnya seperti berikut

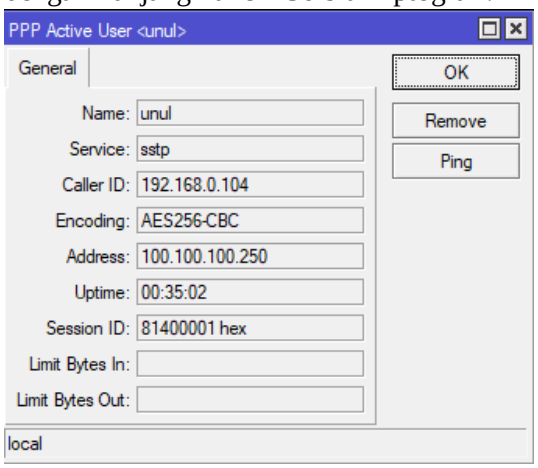
Informatics, Science, and Technologies Journal

Vol 12 No 2 (2022) **Jurnal GERBANG STMIK Bani Saleh**
ISSN : 0853 – 6376
E-ISSN : 2622 – 3708

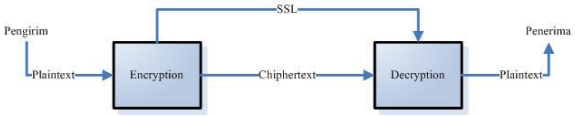


4.3. Pembahasan

Seperti yang terlihat pada gambar (), paket data pada protokol HTTP akan terenkripsi oleh SSL karena menjalankan enkripsi encoding AES256 yang menerjemahkan isi paket data seperti diatas dan sangat sulit untuk diuraikan. Pada menu *Active Connections* seperti dibawah ini tertulis encoding dengan TLS (*Transport Layer Security*) AES dengan tombol 256 yang artinya paket data terenkripsi dengan Panjang kunci 256 bit kriptografi.



Encoding adalah proses konversi informasi dari suatu sumber (objek) menjadi data, yang selanjutnya dikrim ke penerima atau pengamat. AES sendiri merupakan varian dari cipher blok Rijndael yang dikembangan oleh dua kriptografer Belgia, Joan Daemen dan Vincent Rijmen. Angka 256 merupakan bit Panjang kunci kriptografi dari varian AES yang kemungkinan paket data terdeteksi sangat kecil.



Jadi encoding mengenkripsi semua paket data yang di akses pengguna agar saat peretas (*sniffer*) meng-*sniffing* jaringan yang dipakai pengguna tidak dapat mendeteksi apa yang pengguna akses.

V. Penutup

5.1. Kesimpulan

Vol 12 No 2 (2022) **Jurnal GERBANG STMIK Bani Saleh**
ISSN : 0853 – 6376
E-ISSN : 2622 – 3708

Berdasarkan penelitian yang telah dilakukan dapat disimpulkans ebagai berikut:

1. Dengan menggunakan SSTP yang dilengkapi oleh SSL, paket data yang melalui HTTP tidak terdeteksi sedikitpun oleh Wireshark.
2. Paket data HTTP terenkripsi oleh SSL/TLS dengan encoding AES265.
3. Penggunaan SSL pada SSTP sangat bermanfaat untuk domain HTTP karena bisa mensetarakan dengan HTTPS.

5.2. Saran

Penulis sangat berharap dapat dijadikan suatu patokan untuk lebih lanjut mengembangkan tingkat enkripsi saat menggunakan domain berbasis HTTP. Penelitian ini masih berupa jaringan lokal (*local network*), tetapi metode ini bisa diterapkan pada jaringan publik (public network) jika memiliki IP publik. Masih banyak metode dari VPN dengan tingkatan enkripsi yang lebih baik sehingga dapat digunakan sesuai kebutuhan.

DAFTAR PUSTAKA

Citraweb Solusi Teknologi, P. (2013). *Pemilihan Tipe VPN*. PT. Citraweb Solusi Teknologi. https://mikrotik.co.id/artikel/61/

Citraweb Solusi Teknologi, P. (2016). *Koneksi SSTP dengan Mobile Client*. PT. Citraweb Solusi Teknologi. https://mikrotik.co.id/artikel/206/

Combs, G. (2020). *About Wireshark*. Wireshark. https://www.wireshark.org/

Farly, K. A., Najoan, X. B. N., & Lumenta, A. S. M. (2017). Perancangan dan Implementasi VPN Server dengan menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Studi Kasus Kampus Universitas Sam Ratulangi. *E-Journal Teknik Informatika Vol 11, No.1 (2017) Tekno*, *11*(1). https://ejournal.unsrat.ac.id/index.php/informatika/article/view/16745/16261

Hariyadi, I. P., & Azhar, R. (2017). Pengamanan Layanan Private Cloud Storage Menggunakan HTTPS, IPTables dan SSTP. *Seminar Nasional TIK dan Ilmu Sosial*. https://journal.universitasbumigora.ac.id/index.php/sociotech2017/article/view/286

Rasuanda, M., & Haeruddin. (2020). Perbandingan Performa VPN Menggunakan PPTP Dan SSTP Over SSL Dengan Metode Quality of Service. *Journal of Information System and Technology*, *01*(02), 110–123. https://journal.uib.ac.id/index.php/joint/article/download/4314/1116

Tim Dukungan SSL.com. (2021). *Apa Itu Certificate Authority (CA)?* SSL.com; SSL.com. https://www.ssl.com/id/faqs/apa-itu-otoritas-sertifikat/

Wikipedia. (2017a). *Jaringan Pribadi Virtual*. Wikimedia Foundation; Wikipedia. https://id.wikipedia.org/wiki/Kode

Wikipedia. (2017b). *Microsoft Management Console*. Wikimedia Foundation. https://id.wikipedia.org/wiki/Microsoft_Management_Console

Wikipedia. (2020). *Standar Enkripsi Lanjutan*. Wikimedia Foundation. https://id.wikipedia.org/wiki/Standar_Enkripsi_Lanjutan

Vol 12 No 2 (2022) **Jurnal GERBANG STMIK Bani Saleh**
ISSN : 0853 – 6376
E-ISSN : 2622 – 3708

Wikipedia. (2021a). *Jaringan Area Lokal*. Wikimedia Foundation. https://id.wikipedia.org/wiki/Jaringan_area_lokal

Wikipedia. (2021b). *MikroTik*. Wikimedia Foundation. https://id.wikipedia.org/wiki/MikroTik

Wikipedia. (2022a). *Internet*. Wikimedia Foundation. https://id.wikipedia.org/wiki/Internet

Wikipedia. (2022b). *Jaringan Komputer*. Wikimedia Foundation. https://id.wikipedia.org/wiki/Jaringan_komputer

Wikipedia. (2022c). *Kode*. Wikimedia Foundation. https://id.wikipedia.org/wiki/Kode

Wikipedia. (2022d). *Penghala*. Wikimedia Foundation. https://id.wikipedia.org/wiki/Penghala

Wikipedia. (2022e). *Secure Socket Tunneling Protocol*. Wikimedia Foundation. https://en.wikipedia.org/wiki/Secure_Socket_Tunneling_Protocol