

ANALISIS PERBANDINGAN KINERJA LAYANAN *LAYER 2 TUNNELING PROTOCOL* DAN *SECURE SOCKET TUNNELING PROTOCOL* PADA JARINGAN *VIRTUAL PRIVATE NETWORK*

Mislaini¹, Muhammad Syahroni², Amir D³

^{1,2,3}) Prodi Teknologi Rekayasa Jaringan telekomunikasi

Jurusan Teknik Elektro Politeknik Negeri Lhokseumawe

Email: mislaini2003@gmail.com¹, msyahroni@pnl.ac.id², Amird@pnl.ac.id³

ABSTRAK

Kinerja layanan jaringan VPN adalah kemampuan sistem untuk menyediakan koneksi yang aman dan efisien melalui jaringan publik. Penelitian ini bertujuan untuk menganalisa perbandingan kinerja *Layer 2 Tunneling Protocol* dan *Secure Socket Tunneling Protocol* terhadap kualitas layanan jaringan. Pada penelitian ini dibutuhkan beberapa pengujian, yaitu yang pertama melakukan pengujian terhadap konektivitas antar *site*, kemudian pengujian terhadap kualitas layanan pada VPN L2TP dan VPN SSTP. Dimana yang diuji adalah parameter dari *Quality of Service* seperti *throughput*, *delay*, *packet loss* dan juga keamanan jaringan. Pada pengukuran *throughput*, protokol VPN yang lebih unggul adalah SSTP dimana rata-rata kecepatan transfer data mencapai 1260 kbps, sedangkan L2TP hanya 774 kbps. Pada pengukuran *delay*, protokol VPN yang lebih unggul adalah SSTP dimana rata-rata waktu yang dibutuhkan dalam mengirimkan paket hanya 6,19 ms, sedangkan L2TP membutuhkan waktu lebih lama yaitu 9,817 ms. Pada pengukuran *packet loss*, protokol VPN yang lebih unggul adalah L2TP dimana persentase paket data yang hilang hanya sebesar 0,34% sedangkan SSTP mencapai 0,80%. Pada pengujian keamanan jaringan, kinerja kedua protokol tersebut sama-sama sangat baik dalam mengamankan data, sehingga *username* dan *password* akun SIAKAD tidak dapat terbaca oleh Wireshark.

Kata kunci: VPN, L2TP, SSTP, *throughput*, *delay*, *packet loss*, keamanan

I. PENDAHULUAN

Penelitian ini dilatarbelakangi oleh permasalahan dalam memilih protokol yang efektif terhadap kinerja layanan jaringan VPN (*Virtual Private Network*). Kinerja layanan jaringan VPN adalah kemampuan sistem untuk menyediakan koneksi yang aman dan efisien melalui jaringan publik. VPN adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal.

VPN ini memiliki beberapa jenis yang protokol yang umum digunakan, yaitu L2TP (*Layer 2 Tunneling Protocol*) dan SSTP (*Secure Socket Tunneling Protocol*). L2TP bekerja dengan menggabungkan fitur dari dua protokol, yaitu *Layer 2 Forwarding* (L2F) dan *Point-to-Point Tunneling Protocol* (PPTP). L2TP bekerja dengan membungkus data dalam lapisan tambahan yang memungkinkan lalu lintas untuk melewati jaringan yang berbeda dengan aman. Sedangkan SSTP adalah sebuah tunnel yang menggunakan TCP pada port 443. Untuk memanfaatkan SSTP secara optimal, diperlukan penggunaan sertifikat SSL untuk mengamankan koneksi antara server dan klien. Masing-masing VPN itu memiliki keunggulan dan kinerja masing-masing.

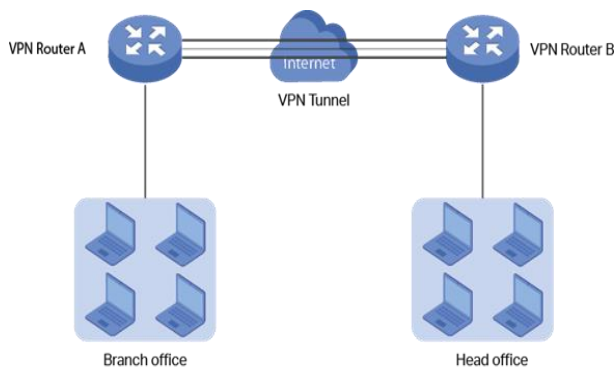
Kinerja layanan ini digunakan sebagai alat ukur untuk menentukan kualitas layanan VPN, oleh sebab itu diperlukan pengujian terhadap kinerja layanan jaringan pada protokol L2TP dan SSTP untuk membandingkan kinerja layanan jaringan dua buah protokol tersebut.

II. TINJAUAN PUSTAKA

A. VPN (*Virtual Private Network*)

VPN adalah sebuah proses dimana jaringan umum diamankan kemudian difungsikan menjadi sebuah jaringan privat. Sebuah VPN tidak didefinisikan oleh rangkaian khusus atau router, tetapi didefinisikan oleh mekanisme keamanan dan prosedur-prosedur yang hanya mengizinkan penggunaannya yang ditunjuk akses ke VPN dan informasi yang mengalir melaluiya [1]. Penggunaan VPN semakin meluas karena perusahaan-perusahaan besar mulai mengembangkan jaringan bisnis mereka, sehingga keamanan jaringan menjadi faktor penting untuk menjaga konektivitas lokal dengan cabang atau anak perusahaan yang berlokasi jauh dari pusat. Dengan menggunakan VPN, jaringan publik dapat diubah menjadi jaringan privat, sehingga kemungkinan pihak lain untuk mengakses data tanpa izin menjadi sangat kecil [2].

VPN memiliki beberapa tipe yang dapat dirancang untuk memenuhi kebutuhan yang berbeda dalam mengakses jaringan, di antara yang paling populer adalah *Remote-Access* VPN dan *Site-to-Site* VPN. Namun pada penelitian ini penulis hanya menggunakan skema jaringan *site-to-site* VPN yang menghubungkan dua atau lebih jaringan lokal yang terpisah secara geografis. Dengan penggunaan perlengkapan *dedicated* dan enkripsi skala besar, sebuah perusahaan dapat mengkoneksikan *multi-site* tetap melalui sebuah jaringan publik seperti internet [3].



Gbr. 1 Skema jaringan Site-to-site VPN

Proses konfigurasi VPN melibatkan pengaturan perangkat pada server dan klien untuk memastikan koneksi yang terenkripsi dan aman.

1. VPN Server

VPN Server adalah sebuah perangkat jaringan yang menjalankan perangkat lunak server. Fungsi-fungsi utama pada VPN servers yaitu menerima *request* dari koneksi VPN, melakukan negosiasi kebutuhan koneksi dan parameter, melakukan autentikasi dan otorisasi pada VPN *clients*, menerima data dari *client* atau meneruskan *request* data yang dilakukan *client*, serta berlaku sebagai titik akhir (*end point*) pada VPN tunnel dan koneksi [4].

2. VPN Client

VPN *client* adalah perangkat lokal maupun jarak jauh yang melakukan sebuah koneksi VPN pada sebuah VPN *server*, dan melakukan *login* pada sebuah jaringan jarak jauh setelah diautentikasi pada VPN *server*, yang kemudian dapat melakukan komunikasi [5].

B. L2TP (Layer 2 Tunneling Protocol)

L2TP merupakan hasil pengembangan dari protokol PPTP plus L2F. Protokol keamanan jaringan dan enkripsi yang digunakan untuk otentikasi sama dengan PPTP. Namun, untuk melakukan panggilan/komunikasi, L2TP menggunakan UDP port 1701 [6]. Biasanya untuk keamanan yang lebih baik, L2TP dikombinasikan dengan IPSec, menjadi L2TP/IPSec. Contohnya untuk sistem operasi Windows, secara *default* OS Windows menggunakan L2TP/IPSec. Namun, konsekuensinya tentu saja konfigurasi yang harus dilakukan tidak semudah saat menggunakan PPTP. Sisi *client* pun harus sudah mendukung IPSec ketika menerapkan L2TP/IPSec. Dari segi enkripsi, tentu enkripsi pada L2TP/IPSec memiliki tingkat keamanan yang lebih tinggi daripada PPTP yang menggunakan MPPE [7].

C. SSTP (Secure Socket Tunneling Protocol)

SSTP adalah sebuah tunel PPP yang berjalan di atas kanal TLS 1.0. Protokol ini menggunakan TCP pada port 443. Untuk memanfaatkan SSTP secara optimal, diperlukan penggunaan sertifikat SSL untuk mengamankan koneksi antara server dan klien. Dengan menggunakan SSL, paket data yang dikirimkan dapat diamankan sehingga memungkinkan kedua perangkat

dalam jaringan melakukan negosiasi, enkripsi, dan pengecekan lalu lintas data [8]. 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 [9].

D. QoS (Quality of Service)

Quality of Service adalah sebuah metode yang digunakan untuk mengukur dan mengelola kemampuan sebuah jaringan dengan tujuan untuk memberikan layanan jaringan yang lebih baik, sehingga dapat memenuhi kebutuhan dari suatu layanan. Parameter-digunakan dalam mengukur *Quality of Service* meliputi *throughput*, *packet loss*, *delay* [10].

1. Throughput

Throughput adalah jumlah kedatangan paket yang berhasil tiba ditujuan, atau ukuran seberapa cepat kita mengirim data melalui jaringan yang diukur dalam bps (*bit per second*). Rumus untuk menghitung *throughput* dapat dilihat pada persamaan 1 berikut.

$$\text{Throughput} = \frac{\text{Jumlah data yang dikirim}}{\text{Waktu pengiriman data}} \quad (1)$$

Kategori *throughput* ditampilkan pada Tabel 1 berikut ini.

TABEL I
Peringkat dan kriteria Throughput (TIPHON, 1999)

Indeks	Throughput (bps)	Kategori
4	>2,1 Mbps	Sangat baik
3	1200 kbps – 2,1 Mbps	Baik
2	700 – 1200 kbps	Cukup Baik
1	338 – 700 kbps	Kurang Baik
0	0 – 338 kbps	Buruk

2. Delay

Delay adalah waktu yang dibutuhkan oleh sebuah paket untuk mencapai tujuan, yang disebabkan oleh antrian, atau pengambilan rute alternatif untuk menghindari kemacetan. Rumus untuk menghitung *delay* dapat dilihat pada persamaan 2 berikut.

$$\text{Rata-rata delay} = \frac{\text{Total delay}}{\text{Total paket yang diterima}} \quad (2)$$

Adapun peringkat dan kriteria *delay* diperlihatkan pada Tabel II berikut:

TABEL II
Peringkat dan kriteria Delay (TIPHON, 1999)

Indeks	Delay (ms)	Kategori
4	<150	Sangat baik
3	150 – 300	Baik
2	300 – 450	Cukup Baik
1	>450	Kurang Baik

3. Packet Loss

Packet loss adalah paket yang hilang atau paket yang tertunda dikarenakan banyak faktor, misalkan penurunan jaringan atau melebihi batas standarisasi dari jaringan tersebut. Rumus

untuk menghitung *packet loss* dapat dilihat pada persamaan 3 berikut.

$$\text{Packet loss} = \frac{\text{Paket dikirim} - \text{paket diterima}}{\text{Paket dikirim}} \times 100\% \quad (3)$$

Adapun peringkat dan kriteria *packet loss* diperlihatkan pada Tabel 3.

TABEL III
Peringkat dan kriteria Packet Loss (TIPHON, 1999)

Indeks	Packet Loss (%)	Kategori
4	0%	Sangat baik
3	3%	Baik
2	15%	Cukup Baik
1	25%	Kurang Baik

E. Keamanan Jaringan

Keamanan jaringan didefinisikan sebagai sebuah implementasi dari keamanan, kebijakan, serta proses dalam mencegah sebuah jalan masuk atau akses untuk masuk tanpa izin ke dalam sebuah jaringan atau sumber daya data untuk melakukan perubahan, pencurian, kerusakan data atau sumber daya. VPN merupakan salah satu metode untuk mengamankan sebuah jaringan dari berbagai jenis gangguan dari luar sebuah jaringan [11].

Dengan adanya VPN maka keamanan sebuah jaringan menjadi lebih terjamin sehingga pengguna tidak perlu khawatir untuk mengakses data keluar dan masuk, karena sekalipun ada pengguna lain mengakses jaringan public yang sama namun pengguna tersebut berada diluar dari VPN maka tidak bisa mengakses sumber daya data dari pengguna utama yang menaruh VPN didalam jaringan tersebut, karena VPN membuat jaringan sendiri didalam jaringan tersebut.

F. Router Mikrotik

Router adalah perangkat yang menghubungkan dua atau lebih jaringan untuk meneruskan paket data dari satu jaringan ke jaringan lainnya. Mikrotik adalah sebuah perusahaan yang berbasis di Latvia, didirikan oleh Johnson Trully dan Armin Riekstins [12].

Mikrotik adalah sebutan pada perangkat dari sebuah perusahaan produsen router yang telah berhasil memproduksi router yang handal, mikrotik terdiri dari 2 macam yaitu perangkat keras (Mikrotik Router Board) dan perangkat lunak/ sistem operasi (Mikrotik Router OS) yang berbasis LINUX yang dapat diinstal pada komputer standar yang memiliki spesifikasi seperti router. Mikrotik router dapat dikonfigurasi dengan mode grafis untuk memudahkan administrator menggunakan aplikasi winbox [13].

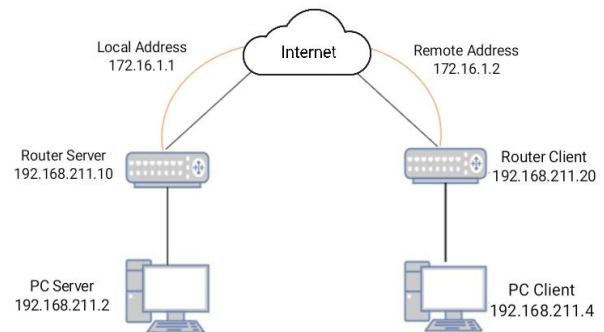
G. Wireshark

Wireshark adalah salah satu dari sekian banyak alat *Network Analyzer* yang banyak digunakan oleh Administrator Jaringan untuk menganalisis kinerja jaringan, termasuk protokol di dalamnya. [14]. Program ini dapat merakam semua paket yang lewat serta menyeleksi dan menampilkan data tersebut sedetail

mungkin, misalnya postingan komentar di blog atau bahkan *username* dan *password* [15].

III. METODOLOGI

Adapun skenario penelitian yang digunakan pada penelitian ini adalah sebagai berikut:



Gbr. 2 Skema jaringan VPN

Berdasarkan gambar 2, penelitian ini melakukan konfigurasi dua buah router Mikrotik yang berguna untuk menghubungkan dua *site* jaringan *local*, dua buah perangkat PC yang memiliki peran dalam proses komunikasi jaringan. Konfigurasi ini bertujuan mengamati hasil perbandingan kinerja layanan L2TP dan SSTP. Data-data tentang kinerja jaringan diukur dan diobservasi melalui PC.

Data hasil pengujian kemudian dihitung menggunakan persamaan *throughput*, *delay* dan *packet loss*. Setelah itu dilakukan juga pengujian terhadap keamanan jaringan dengan cara melakukan penjelajahan ke situs SIAKAD Politeknik Negeri Lhokseumawe yang mana masih menggunakan protokol HTTP untuk memantau apakah *username* dan *password* dapat tertangkap oleh wireshark atau tidak.

IV. HASIL DAN PEMBAHASAN

A. Pengujian *Quality of Service* VPN L2TP

1. *Throughput*

TABEL IV
Hasil pengujian Throughput VPN L2TP

Pengujian	Throughput	Indeks	Kategori
1	671 kbps	1	Kurang Baik
2	1.258 kbps	3	Baik
3	359 kbps	1	Kurang Baik
Rata-rata	744 kbps	2	Cukup Baik

2. *Delay*

TABEL V
Hasil pengujian Delay VPN L2TP

Pengujian	Delay	Indeks	Kategori
1	8,735 ms	4	Sangat baik
2	5,697 ms	4	Sangat baik
3	15,387 ms	4	Sangat baik
Rata-rata	9,817 ms	4	Sangat baik

3. *Packet Loss*

TABEL VI
Hasil pengujian Packet Loss VPN L2TP

Pengujian	Packet Loss	Indeks	Kategori
1	0,9 %	4	Sangat baik
2	0,1 %	4	Sangat baik
3	0,04 %	4	Sangat baik
Rata-rata	0,34 %	4	Sangat baik

B. Pengujian *Quality of Service* VPN SSTP1. *Throughput*TABEL VII
Hasil pengujian *Throughput* VPN SSTP

Pengujian	Throughput	Indeks	Kategori
1	1.400 kbps	3	Baik
2	900 kbps	2	Cukup Baik
3	1.500 kbps	3	Baik
Rata-rata	1.260 kbps	3	Baik

2. *Delay*TABEL VIII
Hasil pengujian *Delay* VPN SSTP

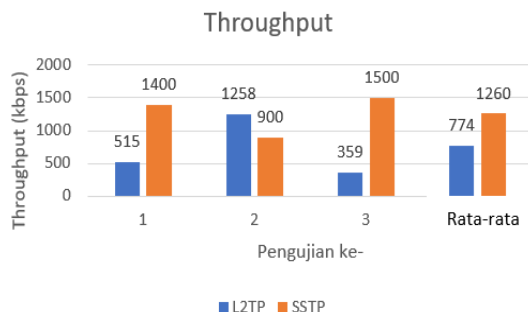
Pengujian	Delay	Indeks	Kategori
1	5,296 ms	4	Sangat baik
2	8,517 ms	4	Sangat baik
3	4,759 ms	4	Sangat baik
Rata-rata	6,190 ms	4	Sangat baik

3. *Packet Loss*TABEL IX
Hasil pengujian *Packet Loss* VPN SSTP

Pengujian	Packet Loss	Indeks	Kategori
1	1,13 %	4	Sangat baik
2	0,05 %	4	Sangat baik
3	1,22 %	4	Sangat baik
Rata-rata	0,8 %	4	Sangat baik

C. Perbandingan *Quality of Service* L2TP dan SSTP1. Perbandingan *Throughput*

Berikut adalah hasil perbandingan *throughput* pada protokol L2TP dan SSTP dalam bentuk grafik batang, dimana semakin tinggi nilai *throughput* maka semakin baik kinerja jaringan.

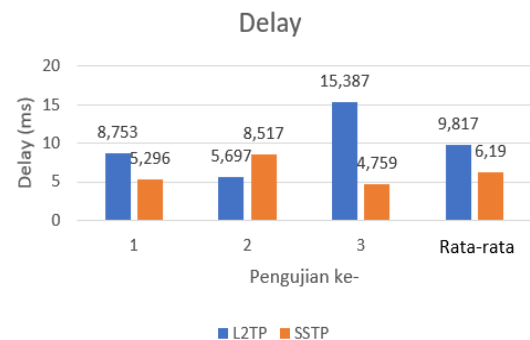


Gbr. 3 Grafik Perbandingan Throughput

Berdasarkan grafik pada gambar 3 tersebut dapat dianalisa bahwa pada pengujian pertama nilai *throughput* protokol SSTP lebih unggul dibandingkan dengan L2TP, dimana kecepatan transfer datanya mencapai 1400 kbps sedangkan L2TP hanya 515 kbps. Namun pada pengujian kedua, nilai *throughput* SSTP menurun drastis menjadi 900 kbps, sedangkan *throughput* L2TP meningkat menjadi 1.258 kbps. Pada pengujian ketiga, kinerja protokol SSTP kembali meningkat menjadi 1.500 kbps dan jauh lebih baik dari L2TP dimana kecepatan transfer datanya hanya 774 kbps. Sehingga rata-rata hasil perbandingan nilai *throughput* menunjukkan bahwa VPN SSTP cenderung memiliki kecepatan data lebih baik dan kinerja yang lebih stabil dibandingkan dengan L2TP.

2. Perbandingan *Delay*

Berikut adalah hasil perbandingan *delay* pada protokol L2TP dan SSTP dalam bentuk grafik, dimana semakin kecil *delay* maka semakin baik kinerja jaringan.

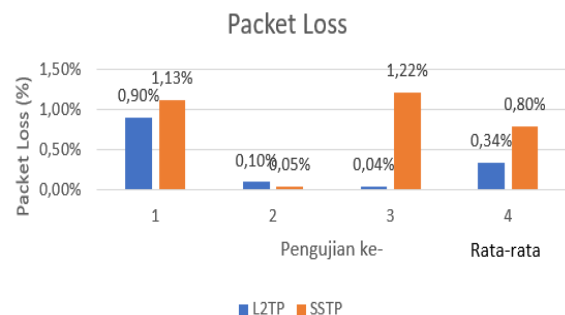


Gbr. 4 Grafik perbandingan Delay

Berdasarkan grafik pada gambar 4 tersebut dapat dianalisa bahwa, pada pengujian pertama tingkat *delay* pada protokol SSTP lebih rendah dari L2TP, yaitu hanya 5,296 ms yang menunjukkan bahwa kinerja layanan protokol SSTP lebih unggul. Namun pada pengujian kedua tingkat *delay* pada protokol SSTP meningkat menjadi 8,517 ms sedangkan *delay* pada L2TP menurun menjadi 5,697 ms sehingga pada pengujian kedua, kinerja protokol L2TP lebih unggul. Pada pengujian ketiga tingkat *delay* pada protokol SSTP kembali menurun drastis yaitu 4,759 ms, yang mana nilai tersebut berbanding jauh dengan *delay* pada L2TP yaitu 15,387 ms. Dari ketiga pengujian tersebut rata-rata hasil perbandingan tingkat *delay* menunjukkan kinerja jaringan VPN SSTP lebih stabil dibandingkan dengan L2TP.

3. Perbandingan *Packet Loss*

Berikut adalah hasil perbandingan *packet loss* pada protokol L2TP dan SSTP dalam bentuk grafik, dimana semakin kecil tingkat *packet loss* maka semakin baik kinerja jaringannya.



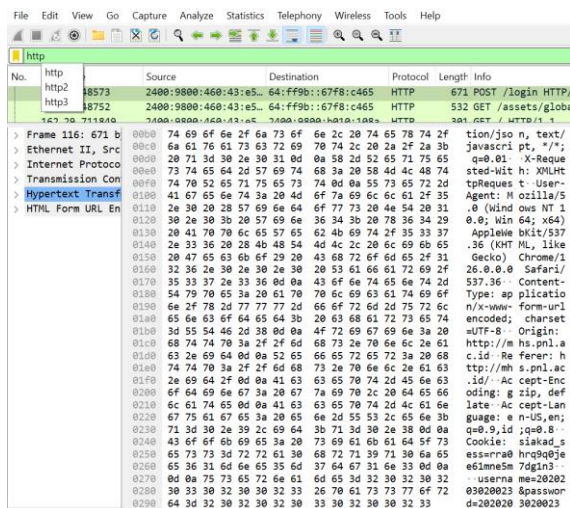
Gbr. 5 Grafik Perbandingan Packet Loss

Berdasarkan grafik pada gambar 5 tersebut dapat dianalisa bahwa, pada pengujian pertama tingkat *packet loss* pada SSTP lebih tinggi dibandingkan L2TP, dimana paket data yang hilang pada VPN SSTP adalah sebesar 1,13% sedangkan pada VPN L2TP hanya 0,90%. Hal ini menunjukkan bahwa kinerja L2TP dalam hal

menjaga paket data agar tidak hilang lebih unggul dibandingkan SSTP. Namun pada pengujian kedua kinerja kedua protokol tersebut meningkat hingga hampir tidak ada paket data yang hilang meskipun SSTP tampak lebih unggul karena paket data yang hilang hanya 0,05%. Pada pengujian ketiga tingkat *packet loss* pada VPN SSTP kembali meningkat drastis menjadi 1,22% sedangkan L2TP hanya 0,04% yang menunjukkan kinerja L2TP lebih unggul. Rata-rata hasil perbandingan tingkat *packet loss* menunjukkan bahwa protokol yang lebih unggul dalam menjaga paket data agar tidak hilang adalah L2TP.

D. Pengujian Keamanan VPN L2TP dan SSTP

Dalam pengujian keamanan jaringan VPN L2TP dan SSTP, peneliti menggunakan Wireshark untuk memantau lalu lintas data saat mengakses situs SIAKAD kampus Politeknik Negeri Lhokseumawe yang mana masih menggunakan protokol HTTP. Tujuan dari pengujian ini adalah untuk mengidentifikasi apakah informasi sensitif seperti *username* dan *password* dapat tertangkap dalam bentuk yang dapat dibaca atau tidak. Pada tahap awal, akan disajikan hasil tangkapan data saat mengakses situs tanpa menggunakan VPN.



Gbr. 6 Hasil tangkapan wireshark tanpa VPN

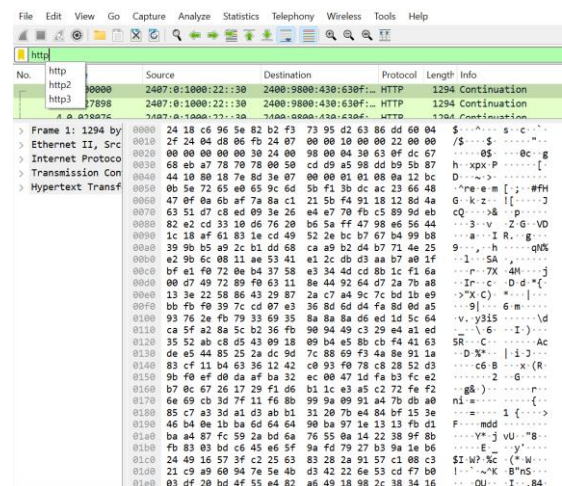
Berdasarkan hasil tangkapan *wireshark* pada gambar 6 dapat dianalisa bahwa saat mengakses SIAKAD tanpa menggunakan VPN, *username* dan *password* tertangkap oleh *wireshark* dalam bentuk teks biasa (*plain text*). Ini menunjukkan bahwa data dikirimkan tanpa enkripsi yang memadai sehingga informasi sensitif dapat dengan mudah dibaca.

Berikut ini akan disajikan hasil tangkapan data saat mengakses situs dengan menggunakan VPN L2TP dan SSTP:

1. Pengujian Keamanan VPN L2TP

Berdasarkan hasil *sniffing* pada situs SIAKAD Politeknik Negeri Lhokseumawe menggunakan *wireshark*, hasil pengujian keamanan pada

jaringan VPN menggunakan protokol L2TP di dapat dilihat pada gambar 7.

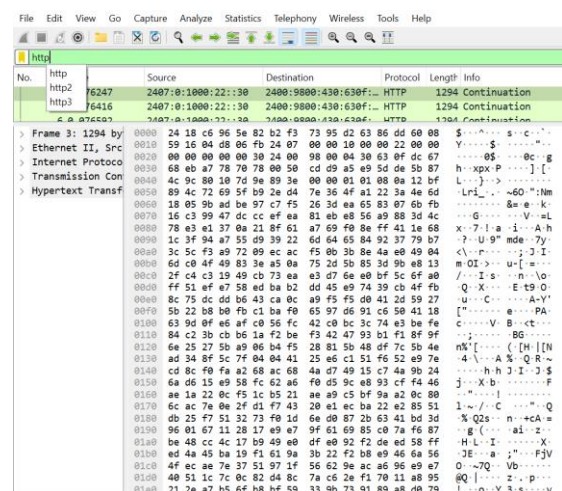


Gbr. 7 Hasil tangkapan wireshark VPN L2TP

Berdasarkan hasil pengujian yang dilakukan, data yang terekam oleh Wireshark hanya menampilkan simbol-simbol tak terbaca atau tidak dapat diinterpretasikan secara langsung. Hal ini menunjukkan bahwa meskipun protokol HTTP umumnya tidak mengenkripsi data, penggunaan VPN L2TP dengan kombinasi IPSec telah memberikan lapisan enkripsi tambahan yang mengaburkan informasi sensitif tersebut selama transmisi. Dengan demikian, hasil pengujian ini mengindikasikan bahwa penggunaan VPN L2TP mampu meningkatkan keamanan data selama akses ke situs yang masih menggunakan protokol jaringan yang kurang aman.

2. Pengujian Keamanan VPN SSTP

Berdasarkan hasil *sniffing* pada situs SIAKAD Politeknik Negeri Lhokseumawe menggunakan *wireshark*, hasil pengujian keamanan pada jaringan VPN menggunakan protokol SSTP di dapat dilihat pada gambar 8.



Gbr. 8 Hasil tangkapan wireshark VPN SSTP

Hasil tangkapan wireshark pada VPN SSTP juga menunjukkan bahwa data yang dikirimkan melalui jaringan tersebut telah mengalami proses enkripsi yang memadai, sehingga informasi sensitif seperti *username* dan *password* tidak dapat diakses secara langsung melalui alat analisis jaringan seperti Wireshark. Dengan kata lain, meskipun situs yang diakses masih menggunakan protokol HTTP yang tidak terenkripsi, penggunaan VPN SSTP dengan *certificate* SSL mampu memberikan lapisan keamanan tambahan yang efektif dalam melindungi kerahasiaan data. Hal ini menunjukkan bahwa VPN SSTP memiliki kemampuan yang baik dalam menjaga privasi dan keamanan data dalam kondisi pengujian yang dilakukan.

V. KESIMPULAN

Berdasarkan hasil pembahasan tentang analisis kinerja layanan L2TP (*Layer 2 Tunneling Protocol*) dan SSTP (*Secure Socket Tunneling Protocol*) maka dapat disimpulkan bahwa:

1. Pengujian konektivitas pada jaringan VPN menggunakan protokol L2TP dan SSTP dengan melakukan test ping antar perangkat telah berhasil dilakukan. Dengan berhasilnya pengiriman paket tersebut dapat dikatakan bahwa antara sisi *server* dan sisi *client* pada masing-masing jenis protokol VPN tersebut sudah saling terhubung dan dapat saling berkomunikasi.
2. Pada pengukuran *throughput*, protokol VPN yang lebih unggul adalah SSTP dimana rata-rata kecepatan transfer data mencapai 1260 kbps, sedangkan L2TP hanya 774 kbps.
3. Pada pengukuran *delay*, protokol VPN yang lebih unggul adalah SSTP dimana rata-rata waktu yang dibutuhkan dalam mengirimkan paket hanya 6,19 ms, sedangkan L2TP membutuhkan waktu lebih lama yaitu 9,817 ms.
4. Pada pengukuran *packet loss*, protokol VPN yang lebih unggul adalah L2TP dimana persentase paket data yang hilang hanya sebesar 0,34% sedangkan SSTP mencapai 0,80%.
5. Pada pengujian keamanan jaringan, kinerja kedua protokol tersebut sama-sama sangat baik dalam mengenkripsi data, sehingga *username* dan *password* akun SIAKAD tidak dapat terbaca oleh Wireshark.

REFERENSI

- [1] Mufida, E., Irawan, D., & Chrisnawati, G. (2017). **Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus Pada Yayasan Teratai Global Jakarta.** *Jurnal Matrik Vol. 16 No. 2*, 10.
- [2] Moezes Rasuanda, H. (2020). **Perbandingan Performa VPN Menggunakan PPTP dan SSTP Over SSL dengan Metode Quality of Service.** *Journal of Information System and Technology*, 110-123.
- [3] Umam, C., Roza, E., & Irfan. (2016). **Perancangan Jaringan Keamanan Virtual Private Network (VPN) Site to Site.** *Seminar Nasional TEKNOKA_FT UHAMKA*, 23-30.
- [4] Trihadi, S., Budianto, F., & Arifin, W. (n.d.). **Perancangan Virtual Private Network Dengan Server Linux Pada Pt. Dharma Guna Sakti.** 3.
- [5] Vicky Phang, E. S. (2021). **Perancangan Virtual Private Network dengan Protokol PPTP Menggunakan Mikrotik Untuk Kebutuhan Remote Access.** *Jurnal POLEKTRO*.
- [6] Alvin, M., & Wardhana, S. (n.d.). **Implementasi dan Perbandingan Keamanan PPTP dan L2TP/IPsec VPN.** *RESISTOR (Elektronika Kendali Telekomunikasi Tenaga Listrik Komputer) Vol. 6 No. 1*, 71-72.
- [7] Mustofa, T. A., Ausanta, E., & Triyono, J. (2019). **Perancangan Dan Implementasi Sistem Monitoring Jaringan Wi-Fi Menggunakan Mikromon Online Di Wisma Muslim Klitren Gondokusuman Yogyakarta.** *Jurnal Jarkom Vol. 7 No. 2*, 67.
- [8] Azhar, R. (2017). **Analisa QoS Pada Jaringan Site to Site VPN Menggunakan Protocol SSTP.** *Seminar Nasional TIK dan Ilmu Sosial*, 52-60.
- [9] Saijuna, D. G., Himamunanto, A. R., & Jatmika. (2020). **Analisis Perbandingan Performa SSTP dan PPTP pada VPN.** 4.
- [10] Habibah, F., Hanafi., & Syahroni, M. (2023). **Desain Dan Implementasi Jaringan Vpn Menggunakan Cisco Router Rv320 Di Laboratorium Jaringan Komputer Jurusan Teknik Elektro Politeknik Negeri Lhokseumawe.** *Jurnal TEKTRON*, 210-215.
- [11] Kurniawan, A. (2022). **Analisis Performansi Remote Access VPN Menggunakan PPTP dan L2TP untuk Kebutuhan Work From Home (WFH) bagi Karyawan PT Dunia Makmur Jaya.** *Jurnal Pendidikan Tambusai*.
- [12] Subandri, Khotimah, K., & Prabowo, K. M. (2022). **Penerapan Layanan Publik Menggunakan Secure Socket Tunneling Protocol.** *Jurnal GERBANG STMIK Bani Saleh*, 27-40.
- [13] Masroni, Pertiwi, A., & Suroso, A. (2021). **Merancang Dan Implementasi VPN PPTP Untuk Koneksi Client Server Aplikasi Keuangan IFAS.** *Jurnal Informatika*, 169.
- [14] Adji Putra Pamungkas, M. R. (2021). **Analisis Jaringan VPN Menggunakan PPTP dan L2TP Berbasis Mikrotik pada Diskominfo Kabupaten Muko Muko.** *Jurnal KomtekInfo*, 189-194.
- [15] Jabal Nur, L. R. (2021). **Simulasi Virtual Private Network (VPN) Menggunakan Secure Socket Tunneling Protocol (SSTP) pada Jaringan Kampus Unidayan Baubau.** *Jurnal Informatika*, 1-8.