Jurnal DINAMIS Vol 21 Nomor 2 Desember 2024
P-ISSN : 1693-3605, E-ISSN : 2722-0109, pp. 71-77

Perbandingan Protokol PPTP dan SSTP untuk Optimalisasi Jaringan VPN menggunakan metode DMVPN

Ade Salman[1], Alam Rahmatulloh[1*]
[1]Program Studi Informatika
Fakultas Teknik
Universitas Siliwangi
Email: alam@unsil.ac.id *

ABSTRACT

Organizations using Virtual Private Network (VPN) are essential to keep their network connections secure and efficient in the current era of digitalization. this research aims to study and compare two VPN protocols in terms of security, memory usage, and CPU speed of PPTP and SSTP protocols, considering how they improve the security and performance of applications. PPTP networks are known for being easy to use but have a lower level of security, SSTP offers flexibility in communication between nodes with strong encryption using certificates for encryption. The performance, scalability, and security of both protocols were evaluated using the DMVPN method. The results show that SSTP is more effective and secure for organizations with complex network requirements with 10% attack vulnerability accuracy, while PPTP is better for easier use with lower security levels with 70% vulnerability accuracy when used in complex networks. Both protocols can use memory resources with a 30% difference in memory usage where PPTP requires 20% of the total memory used in the client while SSTP requires 50% of the total memory in the client, this can make a reference for companies that will use VPN networks.

Keywords *SSTP,DMVPN, security, PPTP, VPN*.

I. Pendahuluan

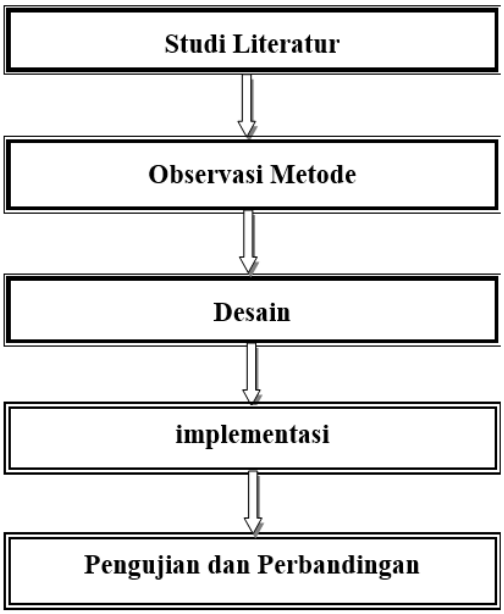
Keamanan data dan privasi pengguna sangat penting bagi organisasi dan individu di dunia yang semakin terhubung [1][2]. Salah satu solusi yang populer untuk melindungi pengiriman paket data yang dikirim melalui jaringan publik adalah *Virtual Private Network* (VPN) [3][4][5]. Jaringan *Virtual Private* adalah solusi umum untuk memastikan kerahasiaan, integritas, dan ketersediaan saat melakukan koneksi internet jarak jauh antara berbagai situs [6]. Untuk jaringan VPN, dua protokol yang paling umum adalah *Secure Socket Tunneling Protocol* (SSTP) dan *Point-to-Point Tunneling Protocol* (PPTP). Kedua protokol ini memiliki banyak keunggulan dan kelemahan dalam hal keamanan dan kinerja [7][8]. PPTP dan SSTP merupakan dua protokol VPN yang umum digunakan dalam perbandingan metode optimalisasi jaringan VPN [9]. PPTP menawarkan fleksibilitas dan skalabilitas yang lebih baik dibandingkan dengan SSTP, terutama dalam pengaturan jaringan yang kompleks [10][11][12].

PPTP masih banyak digunakan karena kemudahan dan kecepatan implementasinya, tetapi banyak penelitian menunjukkan bahwa SSTP memberikan tingkat keamanan yang lebih tinggi [12]. Terdapat tantangan terkait dengan kompleksitas konfigurasi DMVPN (*Dynamic Multipoint Virtual Privat Network*) menggunkan protokol SSTP yang mungkin tidak dapat diatasi oleh semua organisasi [13].

DMVPN menggunkan protokol SSTP memungkinkan untuk di terapkan dalam optimalisasi jaringan VPN [14]. Analisis komparatif diperlukan untuk mengetahui perbandingan antara protokol PPTP dan SSTP dengan fokus pada aspek keamanan, performa, dan kemudahan implementasi Dengan memahami manfaat dan kekurangan masing-masing pendekatan, penelitian ini dapat memberikan pengetahuan yang bermanfaat dalam optimalisasi keamanan jaringan VPN[15]. Hasil analisis ini dapat menjadi referensi bagi organisasi dalam membuat keputusan yang lebih tepat terkait implementasi jaringan VPN di lingkungan mereka.

II. Metode Penelitian

Penelitian yang dilakukan menggunakan pendekatan metode eksperimental untuk membandingkan kinerja protokol PPTP dan SSTP saat mengoptimalkan jaringan VPN dengan metode DMVPN. Metode ini melibatkan proses studi litelatur, observasi metode, desain, implementasi, pengujian dan perbandingan dua protokol seperti yang di tampilkan dalam gambar 1.



Gambar 1. Metode Penelitian

2.1 Studi Litelatur

Tahapan ini sebagai landasan untuk memahami konsep dasar kedua teknologi VPN yang akan dibandingkan untuk optimalisasi, yaitu protokol SSTP dan PPTP. Dilakukan pengumpulan dan mempelajari penelitian, sebelummnya yang membahas mengenai optimalisasi jaringan VPN.

Studi tentang optimalisasi jaringan VPN telah banyak dilakukan untuk mengoptimalkan jaringan VPN dengan berbagai cara dan teknik, baik dari sisi keamanan, efisiensi dan penggunaan *resource*, seperti yang di lakukan [16] menggunakan metode DMVPN dengan pendekatan routing OSPF(*Open Shortest Path First*) mendapatkan hasil efisiensi penggunaan memori dibawah 20% senhingga *free memory* nya sekitar 95%, kemudian pada penelitian [17] yang melakukan perbandingan kualitas jaringan VPN pada VOIP (*Voice Over Internet Protocol*) mendapati hasil dengan menggunakan penerapan ZRTP (*Zimmermann Real Time Transport Protocol*) di VPN mempunyai pengaruh besar 1,18 % dan 3,23 dalam kecepatan *bandwidth*, dan pada penelitian [18] tentang Analisis Efektivitas Protokol PPTP pada jaringan VPN menunjukan adanya peningkatan keandalan jaringan dan keamanan transmisi data, terakhir pada penelitian [19] yang melakukan analisis keamanan VPN menggunakan OpenVPN menunjukan Penyebaran *sniffing* data yang tidak dapat mengidentifikasi ID penerima seperti *username* dan *password* ditandai dengan penurunan pada efektifitas jaringan dengan *delay* parameter meningkat dari 51,4ms menjadi 463,4 ms, kehilangan paket meningkat dari awalnya 7,8% menjadi sebesar 20,2%, *throughput* menurun dari awalnya 82,8% menjadi sebesar 71,6%, dan *bandwidth* turun dari awalnya 64786,6 bit/s menjadi kesil sebesar 55589 bit/s.

Penelitian-penelitian yang telah dilakukan sebelumnya dalam optimalisasi jaringan VPN dijadikan tumpuan untuk melakukan penelitian selanjutnya dalam optimalisasi jaringan VPN, dalam hal ini peningkatan keamanan data yang dikirimkan, dan efisiensi penggunaan *resource* memori dan CPU(*Central Processing Unit*).

2.2 Observasi Metode

Setelah mendapatkan pemahaman dari literatur, tahap ini bertujuan untuk mengamati bagaimana kedua protokol bekerja di lingkungan nyata, dengan mengamati langsung atau melalui pengukuran terhadap parameter jaringan seperti penggunaan *resource* , stabilitas, dan keamanan data. Observasi bisa dilakukan dalam kondisi yang telah diatur sedemikian rupa untuk melihat performa SSTP dan PPTP dalam kondisi infrastruktur jaringan yang sama. Metode yang digunakan dalam perbandingan protokol PPTP dan SSTP di jaringan VPN menggunakan DMVPN.

Dynamic Multipoint VPN (DMVPN) adalah teknologi jaringan yang dirancang untuk meningkatkan fleksibilitas dan efisiensi VPN melalui tiga fase pengembangan. Fase 1 hanya mendukung komunikasi antara *spoke* dan *hub*, di mana semua lalu lintas harus melewati *hub*. Fase 2 memungkinkan koneksi langsung antar *Poin to point* menggunakan *tunneling* mGRE, yang memerlukan data perutean lengkap pada setiap *point*, tentuya dapat membatasi skalabilitas pada jaringan besar. Fase 3 menyempurnakan fase sebelumnya dengan menambahkan fungsi pengalihan dan pintasan NHRP untuk meningkatkan pembaruan perutean dan skalabilitas [20]. Dalam konteks penelitian ini ketiga fase ini menjadi kerangka analisis untuk mengevaluasi efektivitas PPTP dan SSTP dalam

Corresponding Author: alam@unsil.ac.id Received on: November 2024 Accepted on: Desember 2024

aspek keamanan, efisiensi dan penggunaan *resource* pada jaringan VPN modern.

2.3 Desain

Berdasarkan hasil observasi dan tinjauan pustaka, dilakukan perancangan skenario pengujian untuk membandingkan Protokol SSTP dan PPTP menggunakan metode DMVPN. Skenario dirancang dengan hati-hati agar pengujian mencakup semua aspek penting, seperti efisiensi penggunaan memori dan keamanan pengiriman data, dengan membuat eksperimen desain infrastruktur yang akan di implementasikan yaitu ada satu server dua router dan dua *client* yang akan mengirimkan data ke server.

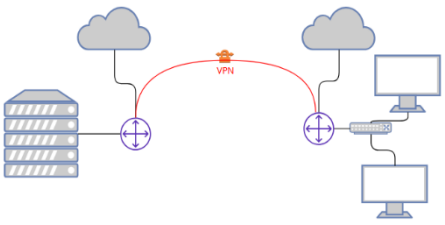
2.4 Implementasi

Tahap implementasi, akan menerapkan desain yang telah dibuat untuk menguji kedua protokol di lingkungan jaringan yang nyata. SSTP dan PPTP dikonfigurasi di perangkat router Mikrotik, kemudian diuji di bawah skenario yang telah dirancang. Implementasi disekemakan ada dua router mikrotik yang digunakan, mikrotik kesatu sebagai server dan mikrotik kedua sebagai *client* dan ada dua komputer yang dapat mengakses server menggunakan jaringan VPN.

2.5 Pengujian dan Perbandingan

Metode pengujian menggunakan *tools capture trafik* yaitu *wireshark* dengan melihat enkripsi dari data yang di kirimkan, dilakukan pendekatan sistematis yaitu pengujian pengukuran kinerja khususnya dalam evaluasi efisiensi sumber daya dan pengujian keamanan yang dapat menguji dan membandingkan dua protokol jaringan VPN (SSTP dan PPTP). Setiap tahapan membantu dalam mengidentifikasi kelebihan dan kekurangan dari kedua teknologi tersebut, serta memberikan hasil yang dapat digunakan organisasi atau perusahaan dalam memilih solusi VPN yang paling tepat untuk kebutuhan optimalisasi jaringan.

III. Hasil dan Pembahasan



Gambar 2. Desain jaringan VPN [6]

III.1 Analisis protokol PPTP

Optimalisasi protokol PPTP menggunakan metode DMVPN untuk mengetahui penggunaan memori, dan keamanan data yang dikirimkan. Gambar 2 merupakan topologi infrastruktur jaringan yang digunakan dalam analisis jaringan VPN dengan protokol PPTP.

Dari gambar 2 merupakan desain infrastruktur VPN yang akan dilakukan analisis untuk protokol PPTP menggunakan metode DMVPN, terdapat 2 *client* yang akan mengakses server menggunakan jaringan VPN Untuk di analisis penggunaan memory dan CPU serta melakukan analisis keamanan data yang dikirimkan.

III.2 Penggunaan memori dan CPU protokol PPTP

Analisis dilakukan untuk mengetahui informasi memori yang digunakan oleh jaringan VPN menggunakan protokol PPTP di komputer *Client*. Hasil monitor untuk proses pppd (*Point-to-Point Protocol Daemon*) layanan VPN menunjukkan penggunaan sumber daya yang sangat rendah. Hasil ini menunjukkan bahwa pada saat pengukuran, pppd tidak memberikan beban berat pada sistem, mengindikasikan bahwa tidak ada lalu lintas data yang signifikan.

Tabel 1. penggunaan memori dan cpu protokol pptp

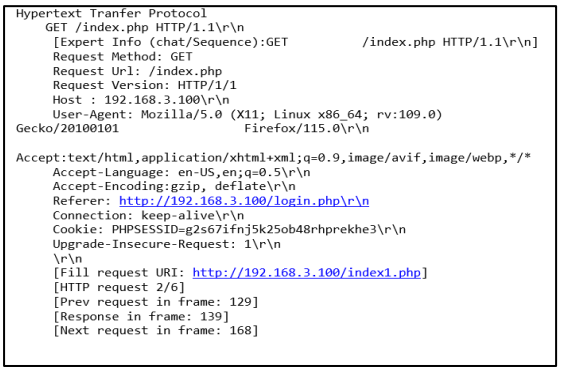
Parameter	Nilai	keterangan
PID	223698	ID proses pppd
Penggunaan CPU	0.0%	Tudak ada aktifitas
Penggunaan *memory*	9088 KiB	0.2% dari total memori
Tortal *memory* sistem	3925.0 MiB	Memori yang tersedia
Free memory	814.9 MiB	Memori tidak terpakai
Cache memory	1782.3 MiB	Memori yang digunakan caching
Waktu cpu	00:00.02	Waktu CPU yang digunakan saat mulai

Tabel 1 menunjukan bahwa penggunakan memori dan CPU yang digunkan oleh jaringan VPN dengan menggunakan protokol PPTP untuk penggunaan memory 9mb dan penggunaan CPU nya 0.0%.

Corresponding Author: alam@unsil.ac.id Received on: November 2024 Accepted on: Desember 2024

III.3 Analisis Keamanan Protokol PPTP

Analisis keamanan dilakukan untuk mengetahui kerentanan ketika menggunkan protokol PPTP pada jaringan VPN. Melakukan skema dengan mengakses *webeite* yang ada di server dari komputer *client* yang tidak satu jaringan LAN kantor pusat.



Gambar 3. Hasil capture pengiriman Data menggunakan Protokol PPTP

Hasil *capture packet* menunjukkan kelemahan signifikan dalam penggunaan PPTP dengan di tandai tidak adanya enkripsi yang menampilkan *cookie* saat mengakses sebuah website di server dan ketika melakukan pengiriman data ke server. Protokol PPTP memiliki kelemahan pada otentikasi, yaitu MS-CHAPv2, yang rentan terhadap serangan *brute force*, sehingga memungkinkan data terenkripsi dibuka oleh pihak yang tidak berwenang. Selain itu, penggunaan *cookie* dalam proses pengiriman data sering kali dilakukan dalam format *plaintext*, yang meningkatkan risiko pencurian data. Sementara fitur *keep-alive* yang mempertahankan koneksi tetap terbuka tanpa enkripsi dapat menjadi celah keamanan yang rentan terhadap serangan *brute force* kelemahan-kelemahan tersebut terdapat pada tabel 2. Secara keseluruhan, kelemahan-kelemahan ini menunjukkan pentingnya menerapkan protokol keamanan yang lebih kuat untuk melindungi data dari ancaman siber.

Tabel 2. Kerentanan protokol pptp

Aspek	Kelemahan	dampak
PPTP	Rentan menggunakan *brute force* (MS-CHAPv2) [21].	Data terenkripsi dapat di buka
Cookie	Data dikirim dalam *plaintext [22].*	Data bisa di curi
Keep-alive	Koneksi terbuka tanpa enkripsi [18].	Berpotensi serangan *brute force*

III.4 Analisis protokol PPTP

Optimalisasi protokol SSTP menggunakan metode DMVPN untuk mengetahui penggunaan memori, dan keamanan data yang dikirimkan. Desain topoogi yang digunakan pada gambar 2 merupakan topologi sistem jaringan VPN yang digunakan untuk analisis optimalisasi jaringan VPN dengan protokol SSTP menggunakan metode DMVPN.

III.5 Penggunaan memori dan CPU protokol SSTP

Analisis dilakukan untuk mengetahui informasi mengenai penggunaan memori yang di gunakan jaringan VPN dengan protokol SSTP. Ditunjukkan perbedaan yang signifikan dalam penggunaan memori dan CPU pada jaringan VPN yang menggunakan protokol SSTP melalui prosessvchost.exe. Secara keseluruhan, layanan VPN SSTP ini berjalan dengan baik dengan penggunaan memori yang relatif kecil dan beban CPU yang rendah, sebagian besar proses tidak mencatat penggunaan CPU, dengan beberapa proses menggunakan memori aktif (*working set*) hingga 26840 KB, dan memori *private* berkisar antara 9896 KB dan 30580 KB.

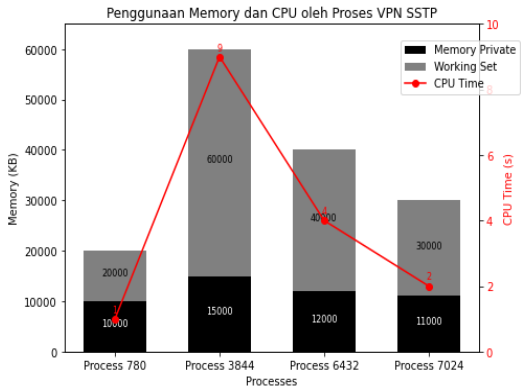
Tabel 3. penggunaan memori dan cpu protokol sstp

Proses	Memori private	Working set	CPU Time	Keterangan penggunaan
svchost.exe (Id 780)	9,896	15,332	0.00	rendah
svchost.exe (Id 3844)	30,580	26,840	9.16	Tinggi
svchost.exe (Id 6432)	6,296	14,076	2.11	Normal
svchost.exe (Id 7024)	4,228	13,744	0.52	rendah
svchost.exe	Variasi (Rata-rata: 8,000)	Variasi (Rata-rata: 12,000)	Minor	bervariasi

Corresponding Author: alam@unsil.ac.id Received on: November 2024 Accepted on: Desember 2024

Dari tabel 3, *working set* yang merupakan kumpulan halaman memori yang digunakan oleh proses aktif, membantu sistem operasi mengelola memori dengan efisien dan menjaga data yang sering diakses tetap di memori fisik untuk meningkatkan performa, Memori *privat* adalah jumlah memori yang dialokasikan secara eksklusif untuk suatu proses dan mencakup semua data serta kode yang diperlukan oleh proses tersebut, Keduanya penting dalam pengelolaan memori. *Working set* mencerminkan aktivitas penggunaan memori, sedangkan memori *privat* yang tinggi dapat menunjukkan kebutuhan sumber daya besar atau potensi kebocoran memori.

Gambar 5 menunjukkan penggunaan memori dan waktu CPU oleh beberapa proses yang terkait dengan koneksi VPN SSTP. Setiap proses memiliki dua komponen memori yaitu memori *privat*, yang merupakan memori eksklusif untuk proses, dan *working set*, memori aktif yang digunakan proses. *Working set* ditumpuk di atas memori *privat* untuk menampilkan total memori yang digunakan. Garis merah menggambarkan waktu CPU, dengan proses yang memiliki CPU *time* lebih tinggi menunjukkan intensitas pemrosesan yang lebih besar. Grafik ini memvisualisasikan efisiensi penggunaan memori dan CPU oleh masing-masing proses VPN.



Gambar 5. Penggunaan Memory dan CPU Protokol SSTP

III.6 Analisis Keamanan Protokol SSTP

Analisis keamanan paket yang dikirimkan atau yang di minta ke sebuah server di kantor pusat harus menggunakan keamaman yang tinggi ketika menggunakan jaringan VPN. Akan dilakukan skema pengujian keamanan jaringan VPN menggunakan protokol SSTP yang mengacu pada gambar 2 topologi jaringan VPN dalam rangka menguji dan mengevaluasi keamanan yang digunakan oleh protokol SSTP.

Gambar 6. menunjukkan penggunaan protokol *http post* untuk mengirim data terenkripsi melalui x-www-form-urlencoded ke server dengan protokol http, Meskipun lalu lintas VPN dienkripsi menggunakan SSTP (*Secure Socket Tunneling Protocol*), data yang dikirimkan ke server tanpa protokol aman seperti https tetap berpotensi terekspos di sisi server. sstp melindungi data saat *transit*, namun keamanan *end-to-end* tidak terjamin jika server tidak menggunakan protokol aman, sehingga informasi sensitif dapat terekspos pada *endpoint* server tersebut.

```
˅Hpertext Tranfer Protocol
   ˅POST //netCut/billengine4.php HTTP/1.0\r\n
    [Expert Info (Chat/Sequence): POST //netCut/billengine4.php
HTTP/1.0\r\n]
Reuest Method: POST
Request URL: //netCut/billengine4.php
Request Version: HTTP/1.0
User-Agent: netcut\r\n
Content-Type: a[[lication/x-WWw-from-urlencoded\r\n
˅Content-Length: 981\r\n
   [Content length: 981]
Accept: */*\r\n
Connection: Close\r\n
Host: api.arcai.com\r\n
\r\n
[Fullrequest URI: http://api.arcai.com//netCut/billengine4.php]
[HTTP request 1/1]
[Response in frame: 9336]
File Data: 981 bytes

˅HTML Form URL Encoded: application/x-www-from-urlencoded
  ˅[truncated]From item: "K" = "NeguZrkxkpmtUKfv/VQZCU
        em1Uen1KEsUFIVBJBcX3CjwuykD8XyW3HdhVWByIvR4HT
        +vVw5KsBhY/Uqf44XUB7XwU"
    Key: k
    value [truncated]:NeguZrkxkpmtUKfv/VQZCUem1Uen1KEsUFIVBJ
        BcX3CjwuykD8XyW3HdhVWByIvR4HT+vVw5KsBhY/Uqf44XUB7XwU
˅[truncated] form item: "r" ="5pmbEX9+uWfQRR09z1n8Pr9Lu3tVcKx8J
                Xudj/rw7Ex81F8Ak6T/EUhUdSNH+kINTKyODKtlZzDn
                PfiHmb6t9uofaXB"
    key: r
    value [truncated]: 5pmbEX9+uWfQRR09z1n8Pr9Lu3tVcKx8JXUdj
                /rw7Ex81F8Ak6T/EUhUdSNH+kINTKyODKtlZzDnPf
                iHmb6t9uofaXB
```

Gambar 6. Hasil captur pengiriman data menggunakan Protokol SSTP

III.7 Perbandingan Protokol PPTP dan SSTP

Analisis perbandingan protokol PPTP dan SSTP menggunakan metode DMVPN di perlukan untuk mengetehui protokol mana yang lebih efisien dalam penggunaan memori dan CPU juga kekuatan keamanan data yang dikirimkan atau diterima dari sebuah server.

Tabel 4. Perbandingan rotokol pptp dan sstp

Kriteria	PPTP	SSTP
Keaman Data	40 %	90%
Penggunaan memori	20%	50%
Penggunaan CPU	10%	40%
konfigurasi	30%	80%
Kerentanan	70%	10%

Tabel 4 menunjukkan perbedaan yang signifikan antara protokol PPTP dan SSTP dalam hal penggunaan memori dan keamanan data dalam jaringan VPN yang menggunakan metode DMVPN. PPTP memiliki tingkat keamanan yang rendah pada 40%, membuatnya lebih rentan terhadap serangan, sementara SSTP memiliki tingkat keamanan yang tinggi pada 90% karena penggunaan SSL (*Secure Sockets Layer*) yang kuat. Penggunaan memori, PPTP lebih efisien 20% dengan hasil 9 MB, sedangkan SSTP memerlukan lebih banyak sumber daya 50%, sebanding dengan keamanan yang lebih baik. Selain itu, PPTP menunjukkan penggunaan CPU yang lebih rendah 10%, sementara SSTP memerlukan lebih banyak daya pemrosesan 40% karena enkripsi yang kompleks. Meskipun PPTP lebih efektif, SSTP memiliki kompleksitas yang lebih tinggi 80%, tetapi memiliki lebih sedikit kelemahan keamanan 10%, dibandingkan dengan PPTP yang memiliki banyak kelemahan 70% tetapi mempunyai konfigurasi yang mudah sebesar 30%, Secara keseluruhan. Berdasarkan analisis perbedaan antara PPTP dan SSTP, perusahaan disarankan menggunakan SSTP untuk membangun jaringan VPN, terutama jika keamanan data menjadi prioritas utama. Meskipun memerlukan lebih banyak sumber daya seperti memori dan CPU, SSTP menawarkan tingkat keamanan yang jauh lebih tinggi berkat penggunaan SSL yang kuat, sehingga lebih andal dalam melindungi data sensitif selama transmisi.

IV. Kesimpulan

Penelitian ini menganalisis perbandingan protokol PPTP dan SSTP pada jaringan VPN menggunakan metode DMVPN. Hasilnya menunjukkan bahwa PPTP lebih efisien dalam penggunaan memori sebesar 20% dan CPU 10%, serta mudah dikonfigurasi. Namun, PPTP memiliki tingkat keamanan yang rendah, sehingga rentan terhadap ancaman. Sebaliknya, SSTP menawarkan tingkat keamanan tinggi karena menggunakan enkripsi SSL yang kuat, meskipun membutuhkan sumber daya lebih besar. Berdasarkan analisis ini, SSTP direkomendasikan sebagai pilihan yang lebih aman untuk melindungi data sensitif dalam jaringan VPN, meskipun memiliki kompleksitas konfigurasi yang lebih tinggi.

Saran untuk penelitian selanjutnya, dapat melakukan analisis terhadap protokol VPN lainnya, seperti L2TP/IPsec, IKEv2, dan OpenVPN, Ini akan memberikan gambaran lebih lengkap tentang efisiensi *resource* yang digunakan dan keamanan. Pengujian dapat mencakup berbagai kondisi perangkat keras dan kondisi jaringan untuk menilai latensi, *throughput*, dan keandalan. Faktor-faktor seperti kemudahan konfigurasi dan manajemen serta konsekuensi kebijakan keamanan juga harus dipertimbangkan. Metode komprehensif ini akan membantu menghasilkan rekomendasi yang lebih sesuai untuk protokol VPN yang sesuai dengan kebutuhan pengguna atau organisasi.

V. Daftar Pustaka

[1] M. Betty Yel and M. K. M Nasution, “KEAMANAN INFORMASI DATA PRIBADI PADA MEDIA SOSIAL,” *JIK)*, vol. 6, no. 1, 2022.

[2] Sari, Yosi Nofita, Irfan, Dedy, Huda, and Asrul, “Network Security Analysis Using Virtual Private Network in Vocational School,” *Jurnal Paedagogy*, vol. 9, no. 3, p. 582, Jul. 2022, doi: 10.33394/jp.v9i3.5346.

[3] M. A. Gunawan and S. Wardhana, “Implementasi dan Perbandingan Keamanan PPTP dan L2TP/IPsec VPN (Virtual Private Network),” vol. 6, no. 1.

[4] K. Pruthviraj, “Scalable Dynamic And Multipoint Virtual Private Network Using Internet Protocol Security For An Enterprise Network,” 2020.

[5] Claude, Mukatshung, Nawej, and Shengzhi Du, *Virtual Private Network’s Impact on Network Performance*. IEEE, 2020.

[6] H. M. Marah, J. R. Khalil, A. Elarabi, and M. Ilyas, “DMVPN Network Performance Based on Dynamic Routing Protocols and Basic IPsec Encryption,” Institute of Electrical and Electronics Engineers Inc., Jun. 2021. doi: 10.1109/ICECCE52056.2021.9514142.

[7] P. Venkateswari and T. Purusothaman, “Comparative Study Of Protocols Used For Establishing Vpn,” 2020.

[8] N. Sri, J. Kusuma, G. Sastrawangsa, I. Puritan, and W. Adh, “Rancang Bangun Server Network Attached Storage (NAS) Sebagai Penyimpanan Data Terpusat Studi Kasus SMAN 1 Denpasar.”

[9] Prayogi, Hadi, Febri, and Aulia, “Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan,” *Jurnal*

Corresponding Author: alam@unsil.ac.id Received on: November 2024 Accepted on: Desember 2024

KomtekInfo, pp. 169–175, Aug. 2021, doi: 10.35134/komtekinfo.v8i3.128.

[10] B. Shi, "Computer network information security protection based on virtual private network," in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Oct. 2020. doi: 10.1088/1742-6596/1646/1/012121.

[11] T. Ghozali, W. A. Azels, and M. Siregar, "Optimizing Secure Communication in Distributed Corporate Networks through PPTP and IPSec VPN Protocols," 2022.

[12] Ariyadi and Agung Prabowo, "Perbandingan Kinerja Virtual Private Network Antara Vpn Tunnel Dan Internet Protocols Security," *JURNAL INOVTEK POLITEKNIK BENGKULU*, vol. 6, no. 1, pp. 2527–9866, 2021.

[13] Jay Bryan, Lawas, Allan, Vivero, and Ankit Sharma, *Network Performance Evaluation of VPN Protocols (SSTP and IKEv2)*, vol. 16. IEEE, 2020.

[14] Babkin and Stroganova, *Evaluation and Optimization of Virtual Private Network*, vol. 19. IEEE, 2020.

[15] R. Azhar, H. Santoso, and B. Krismono, "Pengaruh Implementasi Kernel Based Virtual Machine Pada Server Vps Terhadap Pemakaian Cpu Memory Dan Harddisk," 2022. [Online]. Available: http://e-journal.stmiklombok.ac.id/index.php/jireISSN.2620-6900

[16] J. Juliansah and Y. Akbar, "Optimalisasi Kinerja Jaringan VPN Dengan Metode DMVPN," *Jurnal Indonesia : Manajemen Informatika dan Komunikasi*, vol. 4, no. 3, pp. 1788–1798, Sep. 2023, doi: 10.35870/jimik.v4i3.412.

[17] Yogi Noviantoro, "Analisa Perbandingan Antar Kualitas Jaringan VPN IP Security Dan ZRTP Pada Voice Over Internet Protocol," 2022.

[18] D. N. Amadi, A. Budiman, and P. Utomo, "Analysis of the effectiveness of VPN and PPTP Protocol in E-Link Health Report Application Using NDLC Method," *Journal of Information Systems and Informatics*, vol. 6, no. 2, pp. 949–958, Jun. 2024, doi: 10.51519/journalisi.v6i2.746.

[19] M. Iqbal and I. Riadi, "Analysis of Security Virtual Private Network (VPN) Using OpenVPN," 2020.

[20] B. Mohamed, R. Alasem, M. Mansour, and N. Ben Saud, "Comparative Analysis of DMVPN Phase 3 Performance Across Dynamic Routing Protocols," 2024.

[21] R. A. Putra, H. Supendar, and R. Fahlapi, "Perancangan Virtual Private Network Dengan Metode PPTP Menggunakan Mikrotik," *Jurnal Komputer Antartika*, vol. 1, 2023, [Online]. Available: https://ejournal.mediaantartika.id/index.php/jka

[22] A. T. Atmoko, A. Surya Budiman, and N. Nuraeni, "Perancangan Dan Pengembangan Virtual Private Network (VPN) Menggunakan PPTP," 2024.

Corresponding Author: alam@unsil.ac.id Received on: November 2024 Accepted on: Desember 2024