

PERBANDINGAN KEAMANAN VPN IPSEC DAN SSL DALAM CISCO PACKET TRACER

**Clara Kresensia Panjaitan¹, Ahmad Naufal Habibi Lubis², Rut Kezia Imburi³, Dedy
Kiswanto⁴**

Universitas Negeri Medan

E-mail: clarapanjaitan82@gmail.com¹, ahmadnaufalhabibilbs@gmail.com²,
rutimburi@gmail.com³, dedykiswanto@unimed.ac.id⁴

Abstrak

Keamanan jaringan merupakan aspek krusial di era digital, terutama dalam melindungi pertukaran data melalui jaringan publik. Virtual Private Network (VPN) menjadi solusi utama dalam menciptakan komunikasi data yang aman dan terenkripsi. Penelitian ini bertujuan untuk menganalisis dan membandingkan tingkat keamanan antara dua protokol VPN yang umum digunakan, yaitu IPsec dan SSL, dengan memanfaatkan simulasi menggunakan Cisco Packet Tracer. Metode yang digunakan melibatkan konfigurasi dan pengujian koneksi pada dua skenario: VPN IPsec yang menggunakan tunnel antar-router serta VPN SSL yang dikonfigurasi pada ASA firewall dan diakses melalui web browser. Parameter analisis mencakup kemampuan enkripsi, otentikasi, ketahanan terhadap sniffing, serta kemudahan implementasi. Hasil penelitian menunjukkan bahwa VPN IPsec menawarkan tingkat keamanan yang lebih tinggi dengan enkripsi menyeluruh pada seluruh paket jaringan, cocok untuk koneksi site-to-site. Sementara itu, VPN SSL unggul dalam kemudahan implementasi dan fleksibilitas akses jarak jauh, meskipun memiliki keterbatasan dalam hal perlindungan menyeluruh. Kesimpulan dari penelitian ini menegaskan bahwa pemilihan protokol VPN harus disesuaikan dengan kebutuhan dan kondisi jaringan yang dihadapi.

Kata Kunci — VPN, IPsec, SSL, Keamanan Jaringan, Cisco Packet Tracer.

Abstract

Network security is a critical aspect in the digital era, particularly in protecting data exchange over public networks. Virtual Private Network (VPN) is a key solution in establishing secure and encrypted communication. This study aims to analyze and compare the security levels of two commonly used VPN protocols, namely IPsec and SSL, through simulation using Cisco Packet Tracer. The methodology involves configuring and testing VPN connections in two scenarios: IPsec VPN using a site-to-site tunnel between routers, and SSL VPN configured on an ASA firewall and accessed via a web browser. The analysis parameters include encryption capability, authentication method, resistance to sniffing, and ease of implementation. The results indicate that IPsec VPN provides a higher level of security by encrypting the entire network packet, making it suitable for site-to-site communication. On the other hand, SSL VPN offers advantages in ease of deployment and flexibility for remote access, although it is more limited in terms of comprehensive protection. The study concludes that the choice of VPN protocol should be aligned with the specific needs and conditions of the network environment.

Keywords — VPN, IPsec, SSL, Network Security, Cisco Packet Tracer.

1. PENDAHULUAN

Di era digital yang semakin berkembang, kebutuhan akan keamanan dalam jaringan komunikasi menjadi aspek yang sangat krusial. Perusahaan, institusi pemerintahan, serta pengguna individu semakin bergantung pada jaringan teknologi untuk berbagi data dan informasi. Namun, risiko serangan siber seperti pencurian data, penyadapan komunikasi,

dan akses tidak sah terus meningkat, sehingga solusi keamanan jaringan seperti Virtual Private Network (VPN) menjadi sangat penting [1].

VPN adalah teknologi yang memungkinkan pengguna membangun jaringan privat dalam infrastruktur jaringan publik, sehingga komunikasi data dapat lebih aman dan terenkripsi. Ada beberapa jenis VPN yang umum digunakan, di antaranya IPsec (Internet Protocol Security) dan SSL (Secure Socket Layer). IPsec bekerja pada lapisan jaringan (Network Layer) dan menggunakan mekanisme enkripsi kompleks untuk mengamankan komunikasi antara perangkat yang terhubung secara langsung. Sementara itu, SSL bekerja pada lapisan transport (Transport Layer) dan lebih fleksibel karena dapat digunakan melalui browser web tanpa perlu konfigurasi tambahan [2].

Dua jenis VPN yang paling umum digunakan adalah IPsec (Internet Protocol Security) dan SSL (Secure Socket Layer). IPsec beroperasi pada lapisan jaringan (Network Layer) dan menggunakan metode enkripsi menyeluruh yang memberikan perlindungan lebih kuat terhadap serangan man-in-the-middle dan eavesdropping [3]. Di sisi lain, SSL VPN beroperasi pada lapisan transport (Transport Layer) yang lebih fleksibel dan kompatibel dengan banyak perangkat, namun memiliki kelemahan dalam aspek keamanan tertentu.

Penelitian sebelumnya yang berjudul “Analisa konektivitas jaringan IPSEC dan OpenVPN pada jaringan berbasis IP dinamis” menunjukkan bahwa IPsec memiliki keunggulan dalam kinerja enkripsi tetapi memerlukan konfigurasi yang lebih kompleks dibandingkan dengan SSL. Selain itu, perbedaan alamat IP statistik dan dinamis dalam jaringan juga dapat mempengaruhi efektivitas kedua protokol ini. Studi tentang VPN berbasis IP dinamis menemukan bahwa IPsec tetap dapat diimplementasikan dengan optimal melalui metode konfigurasi yang sesuai [4].

Penelitian sebelumnya dengan judul “Perbandingan kinerja Virtual Private Network antara VPN Tunnel dan Internet Protocols Security” menunjukkan bahwa kedua jenis VPN ini memiliki keunggulan dan kelemahan masing-masing. IPsec dikenal memiliki tingkat keamanan yang lebih tinggi dengan enkripsi yang kuat, tetapi memerlukan konfigurasi yang lebih kompleks. Sebaliknya, SSL lebih mudah diterapkan dan lebih kompatibel dengan berbagai perangkat, tetapi memiliki keterbatasan dalam perlindungan terhadap serangan tertentu. Selain itu, penelitian lain juga membandingkan kinerja VPN berdasarkan parameter Quality of Service (QoS), seperti throughput, delay, packet loss, dan jitter, yang berpengaruh pada efisiensi komunikasi jaringan [5].

Dalam penelitian ini, perbandingan keamanan VPN berbasis IPsec dan SSL akan dilakukan dengan menggunakan Cisco Packet Tracer sebagai alat simulasi. Evaluasi akan mencakup aspek keamanan, kinerja, serta efektivitas dalam berbagai skenario penggunaan. Hasil penelitian ini diharapkan dapat memberikan wawasan yang lebih mendalam mengenai keunggulan dan kelemahan masing-masing protokol, serta membantu dalam pengambilan keputusan terkait implementasi VPN di berbagai lingkungan kerja.

Penelitian ini bertujuan untuk menganalisis dan membandingkan tingkat keamanan serta performa antara dua teknologi pengamanan jaringan, yaitu VPN berbasis IPsec dan SSL VPN. Dengan menggunakan simulasi di Cisco Packet Tracer.

2. METODE PENELITIAN

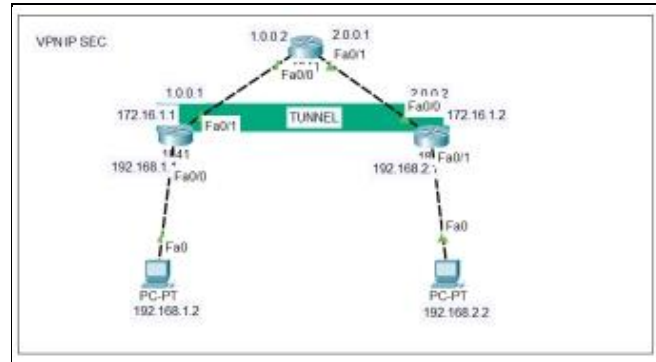
Penelitian ini menggunakan pendekatan simulasi menggunakan Cisco Packet Tracer, untuk menguji perbandingan keamanan antara VPN IPsec dan VPN SSL. Pengujian koneksi VPN IPsec dan VPN SSL yang menggunakan perintah "ping" dan akses melalui web browser.

3. HASIL DAN PEMBAHASAN

1. Ipsec

a. Topologi Jaringan

Dalam skenario VPN IPsec, digunakan tiga router yaitu R1, R2, dan R3 yang saling terhubung melalui jaringan publik yang disimulasikan menggunakan jaringan 1.0.0.0/8 dan 2.0.0.0/8. Dua jaringan lokal masing-masing terletak pada R1 (192.168.1.0/24) dan R3 (192.168.2.0/24), sedangkan R2 bertindak sebagai perantara jalur komunikasi antar kedua router ujung.



Gambar 1. Topologi IPsec

b. Konfigurasi VPN Ipsec

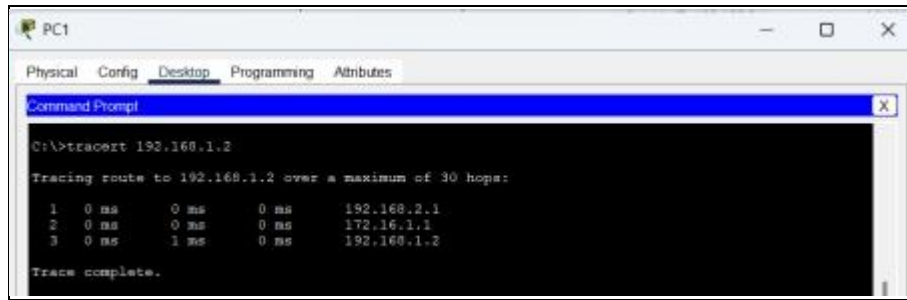
Konfigurasi VPN IPsec dimulai dengan penetapan Access List (ACL) pada masing-masing router untuk mendefinisikan jenis lalu lintas yang perlu diamankan melalui tunnel.

```
R1
Physical Config CLI Attributes
IOS Command Line Interface
interface Tunnel0
ip address 172.16.1.1 255.255.0.0
mtu 1476
tunnel source FastEthernet0/0
tunnel destination 2.0.0.2
!
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 1.0.0.1 255.0.0.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 1.0.0.2
ip route 192.168.2.0 255.255.255.0 172.16.1.2
!
```

Gambar 2. Konfigurasi Router 1

```
R2
Physical Config CLI Attributes
IOS Command Line Interface
interface FastEthernet0/0
ip address 1.0.0.2 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 2.0.0.1 255.0.0.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
```

Gambar 3. Konfigurasi Router 2

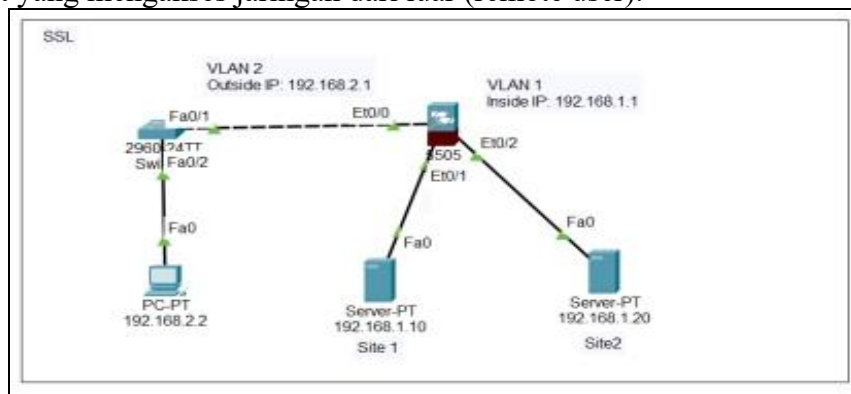


Gambar 7. Hasil perintah traceroute dari R1 ke R3 yang menunjukkan jalur paket melalui tunnel IPsec

2. SSL

a. Topologi Jaringan

Untuk skenario VPN SSL, digunakan sebuah ASA Firewall sebagai perangkat utama yang mengatur lalu lintas antara dua VLAN yang berbeda. VLAN 1 (inside) memiliki alamat jaringan 192.168.1.0/24 dan berisi dua server internal (Server1 dan Server2), sedangkan VLAN 2 (outside) memiliki jaringan 192.168.2.0/24 dan digunakan sebagai lokasi client yang mengakses jaringan dari luar (remote user).



Gambar 8. Topologi SSL

b. Konfigurasi VPN SSL

Konfigurasi dilakukan langsung pada ASA Firewall dengan mengaktifkan fitur webvpn. Proses ini meliputi pembuatan grup pengguna, pengaturan username dan password untuk autentikasi, serta konfigurasi tunneling berbasis HTTPS pada port tertentu. ASA juga dikonfigurasi untuk memberikan izin akses terbatas terhadap IP atau subnet tertentu dari jaringan internal. Setelah konfigurasi selesai, ASA akan menyediakan portal web bagi client yang ingin mengakses jaringan internal secara aman.



Gambar 9. Konfigurasi VPN SSL pada ASA Firewall

c. Pengujian VPN SSL

Pengujian dilakukan dengan mengakses portal VPN SSL dari sisi client (PC di VLAN 2) melalui web browser dengan mengunjungi alamat IP publik ASA. Setelah proses login berhasil, client dapat melihat dan mengakses resource jaringan internal, yaitu Server1 dan Server2 yang berada di VLAN 1.



Gambar 10. Uji coba pada server 1



Gambar 11. Uji coba pada server 2

Uji konektivitas dilakukan melalui browser dan command prompt, serta dibatasi oleh kebijakan akses yang telah diatur sebelumnya pada ASA. Hasil pengujian menunjukkan bahwa akses dari client berhasil dan data yang dikirimkan berjalan melalui koneksi yang telah dienkripsi menggunakan protokol SSL/TLS. Ini membuktikan

Perbandingan Keamanan VPN IPsec dan VPN SSL

Tabel 1. Perbandingan Keamanan VPN IPsec dan VPN SSL.

Fitur	VPN IPsec	VPN SSL
Layer OSI	Layer 3 (Network)	Layer 7 (Application)
Enkripsi	Seluruh paket IP	Lalu lintas berbasis aplikasi (web)
Tipe VPN	Site-to-site	Remote Access
Akses	Semua perangkat di jaringan lokal	Terbatas sesuai policy
Konfigurasi	Lebih kompleks	Lebih mudah
Autentikasi	Manual (pre-Shared Key)	User-based (Login Web)

KESIMPULAN

Berdasarkan hasil simulasi dan analisis konfigurasi VPN IPsec dan VPN SSL pada Cisco Packet Tracer, dapat disimpulkan bahwa masing-masing jenis VPN memiliki keunggulan tersendiri sesuai dengan kebutuhan jaringan. VPN IPsec terbukti memberikan tingkat keamanan yang lebih tinggi karena bekerja pada lapisan jaringan (network layer), sehingga seluruh trafik antar jaringan yang terhubung melalui tunnel akan dienkripsi secara menyeluruh. Hal ini menjadikannya sangat cocok untuk implementasi site-to-site VPN yang membutuhkan keamanan menyeluruh antar dua lokasi atau lebih.

Sebaliknya, VPN SSL menawarkan kemudahan dalam penggunaan dan fleksibilitas akses karena dapat dijalankan langsung melalui web browser tanpa memerlukan perangkat lunak tambahan. VPN jenis ini bekerja pada lapisan aplikasi dan lebih sesuai digunakan untuk kebutuhan remote access oleh pengguna individu ke sumber daya tertentu dalam jaringan. Dari sisi konfigurasi, VPN SSL lebih mudah dan cepat diimplementasikan, sementara VPN IPsec memerlukan konfigurasi yang lebih kompleks serta pemahaman teknis yang lebih mendalam.

Secara umum, kedua jenis VPN berhasil diuji dan menunjukkan kinerja yang sesuai dengan perannya masing-masing. Oleh karena itu, pemilihan jenis VPN sangat bergantung pada tujuan implementasi, skala jaringan, serta tingkat keamanan yang dibutuhkan oleh organisasi atau pengguna yang bersangkutan.

REFERENCES

- Anwar, R. (2020). *Keamanan Jaringan Komputer*. Yogyakarta: Andi Offset
- Ariyadi, T., & Syahrizal, M. A. (2021). Perbandingan kinerja Virtual Private Network antara VPN Tunnel dan Internet Protocols Security. *Jurnal Inovtek Polbeng - Seri Informatika*, 6(1), 52–57.
- Arsalan, M L. “Keamanan Jaringan Wireless Fidelity (Wi-Fi) Terhadap Serangan Packet Sniffing Faisal Fitri, (2022)“ANALISA KINERJA VPN DENGAN LAYER 2 TUNNELING PROTOCOL DAN IPSEC MENGGUNAKAN ROUTER MIKROTIK (STUDI KASUS RSU BUNDA MARGONDA)”.
- Kiswanto, D., Syahputra, H., & Panggabean, S. (2023). Training peningkatan kompetensi industri untuk sertifikasi profesi network engineer skema Network+ bersama PT. Nusanet dan PT. Wilearning Indonesia. *Jurnal Umum Pengabdian Masyarakat (JUPEMAS)*, 1(1), 43–49. <https://creativecommons.org/licenses/by-nc/4.0/>
- Menggunakan Firewall Rule (Studi Kasus: PT Akurat Sentra MediaA.” repository.uinjkt.ac.id, 2023.
- Permana, AHM, Widiyasono, N., & Rahmatulloh, A. (2020). Perbandingan algoritma pada teknologi Virtual Private Network (VPN) IPsec terhadap kecepatan transfer data. *SISTEMASI: Jurnal Sistem Informasi* , 9 (2), 259–273. <https://doi.org/10.>
- 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.
- Setiawan, A. (2021). “Analisis Keamanan Jaringan Virtual Private Network Menggunakan IPsec dan SSL”, *Jurnal Teknologi dan Sistem Komputer*, 9(2), 101–110.
- Setya, A., & Sudaryanto, A. (2021). Analisa konektivitas jaringan IPSEC dan OpenVPN pada jaringan berbasis IP dinamis. *INFOTRON: Jurnal Ilmiah Teknik Informatika, Elektronika dan Kontrol* , 1 (1), 1–5. <https://doi.org/10.xxx>
- Sudrajat, R. (2018). *Cisco Packet Tracer: Panduan Lengkap Praktikum Jaringan Komputer*. Bandung: Informatika.
- Torando, & Irwansyah. (2022). 2 . 1 VPN (Virtual Private Network) VPN adalah suatu mekanisme menyambungkan sebuah titik (atau biasa dengan node) pada sebuah jaringan computer dengan titik yang lain melalui mediasi sebuah jaringan yang lain , sebuah titik dapat berupa sebuah jaring. *Seminar Hasil Penelitian Vokasi (SEMHAVOK)*, 1–13.

Yuasta, A., Yulianto, FA, & Satrya, GB (2014). IPSec dan Berbasis SSL pada Jaringan IPv6. e-Prosiding Teknik , 1 (1), 634–637. <https://doi.org/10.>