“BIMASAKTI”
Jurnal Riset Mahasiswa Bidang Teknologi Informasi

Volume 8 Nomer 1
P ISSN : 2355-4401 – E ISSN 3109-1652
Available online at https://ejournal.unikama.ac.id/index.php/JFTI

PEMILIHAN PROTOKOL VIRTUAL PRIVATE NETWORK MENGGUNAKAN MIKROTIK UNTUK KEBUTUHAN AKSES JARAK JAUH PADA SMK NEGERI 11 MALANG

Rizka Laela Saputri Ramadhanti[1)], Akhmad Zaini[2)], Danang Aditya Nugraha[3)]

Universitas PGRI Kanjuruhan Malang[1,2,3)]
rrizkalaelasaputri@gmail.com

Abstrak

SMK Negeri 11 Malang merupakan sekolah yang memanfaatkan teknologi dan informasi. Administrator memiliki tugas untuk memantau dan memahami kondisi jaringan sekolah. Permasalahan ketika administrator berada diluar jaringan lokal atau jaringan publik. Administrator membutuhkan akses jarak jauh untuk mengakses server ataupun aplikasi dengan aman tanpa adanya kebocoran data. VPN memberikan keamanan dengan mengenkripsi lalu lintas internet. PPTP, L2TP, OpenVPN merupakan pilihan protokol VPN yang dapat digunakan untuk menghubungkan antar jaringan yang berbeda. Pada penelitian ini dilakukan pengujian antar protokol tersebut untuk mengetahui manakah yang memiliki performa terbaik dan kemampuan menjaga kerahasiaan data dan informasi yang tersimpan di dalamnya.

Kata Kunci : VPN, PPTP, L2TP, OpenVPN

Abstract

State Vocational School 11 Malang is a school that uses technology and information. Administrators have the duty to monitor and understand the condition of the school network. The problem when the administrator is outside the local network or public network. The administrator needs remote access to access the server or application safely without data leakage. VPN provides security by encrypting internet traffic. PPTP, L2TP, OpenVPN are VPN protocol options that can be used to connect between different networks. In this research, testing was carried out between these protocols to find out which one has the best performance and the ability to maintain the confidentiality of the data and information stored in it.

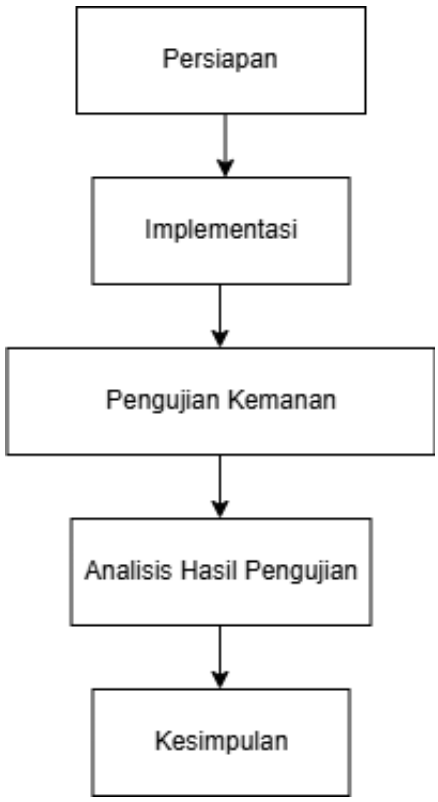
Keywords **:** *VPN, PPTP, L2TP, OpenVPN*

1. PENDAHULUAN

SMK Negeri 11 Malang merupakan SMK PK (Pusat Keunggulan) yang mengoptimalkan kualitas dan kinerja dengan memanfaatkan teknologi dan informasi. Administrator harus siap dalam menghadapi tantangan yang ada seperti permintaan perubahan data mendadak, update dan upgrade sistem informasi dan menjamin kemanan data tersebut. Seorang Administrator memiliki tugas untuk mengawasi lalu lintas data dengan mengakses router ataupun accespoint untuk mengetahui kondisi jaringan sekolah. Tunneling adalah dasar dari VPN untuk membuat suatu jaringan private melalui jaringan internet. Ada berbagai macam teknologi Tunnel yang tersedia. Teknologi tunnel yang didukung oleh mikrotik yaitu PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), OpenVPN. VPN memberikan keamanan dengan mengenkripsi lalu lintas internet, sehingga data pengguna aman dari akses penyadapan. Untuk itu, pengunaan VPN pada mikrotik bisa digunakan untuk akses jarak jauh pada SMK Negeri 11 Malang. Dari banyaknya VPN yang disediakan oleh mikrotik masing-masing VPN memiliki perbedaan, untuk itu diperlukannya pemilihan protokol VPN yang sesuai dengan kebutuhan sekolah.

2. METODE / ALGORITMA

Pada penelitian ini, desain penelitian dibuat untuk menjelaskan dari proses awal penelitian hingga hasil penelitian sesuai dengan Gambar 1.



Gambar.1 Metode Penelitian

Tahapan dalam penelitian dijelaskan seperti berikut ini:

1. Persiapan
   Pada tahap ini peneliti mempersiapkan instrumen penelitian dengan membuat skenario pengujian yang akan dilakukan.
2. Implementasi
   Pada tahapan ini peneliti mengimplementasikan rancangan VPN seperti melakukan konfigurasi mikrotik untuk penggunaan VPN server dengan menggunakan IP publik, melakukan konfigurasi VPN klient pada laptop yang digunakan oleh administrator.
3. Pengujian Keamanan
   Pada tahapan ini dilakukan pengujian VPN yang akan digunakan. Pengujian yang dilakukan yaitu memastikan keamanan yang diberikan oleh setiap VPN.
4. Analisis Hasil Pengujian
   Pada tahapan ini dilakukan analisis dari hasil pengujian VPN yang sudah dilakukan.
5. Kesimpulan
   Pada tahapan ini, peneliti akan menyusun kesimpulan dari hasil penelitian dan saran yang didapat dari pemilihan VPN.

3. HASIL DAN PEMBAHASAN

Dilakukan pengujian dengan memantau dan mengalisis trafik jaringan apakah komunikasi anatar klien dan server terenkripsi dengan benar. Pada VPN PPTP terlihat username adalah pptp dan perangkat yang digunakan adalah MSRAS-0-DESKTOP P-GBI8RPC, alamat IP yang digunakan adalah alamat IP klien, jumlah paket yang terkirim selama komunikasi adalah 448 dan panjang enkripsi yang digunakan adalah 48. Pada VPN L2TP tidak terlihat username dan

perangkat yang digunakan dan alamat IP yang digunakan adalah alamat IP klien, jumlah paket yang terkirim selama komunikasi adalah 472 dan panjang enkripsi yang digunakan adalah 172. Pada OpenVPN tidak terlihat username dan perangkat yang digunakan dan alamat IP yang digunakan adalah alamat IP Server VPN, jumlah paket yang terkirim selama komunikasi adalah 224 dan panjang enkripsi yang digunakan adalah 117.
Pengujian Integritas dilakukan ckecksum MD5 pada pada file VPN.txt pada sisi klien yang menggunakan sistem operasi windows dan server menggunakan sistem operasi Debian untuk mengetahui hash dan dipeloleh nilai yang sama. VPN PPTP, L2TP, dan OpenVPN dapat terkoneksi dengan Penyedia Layanan Internet dari dari Iconnet, Telkomsel Orbit dan IM3 Ooredoo.
Hasil pengujian waktu respon VPN pada hari efektif, VPN PPTP adalah VPN dengan waktu respon tercepat dengan waktu yang diperoleh 00,85 detik dengan Penyedia Layanan Internet Iconnet. VPN L2TP memiliki waktu respon mulai dari 03,38 – 03,82 detik. Open VPN membutuhkan waktu respon yang cukup lama yaitu 04,98 detik pada penyedia layanan IM3 Ooredoo. Dari hasil pengujian waktu respon VPN pada hari libur, VPN PPTP adalah VPN dengan waktu respon tercepat dengan waktu yang diperoleh 00,43 detik dengan Penyedia Layanan Internet Iconnet. VPN L2TP memiliki waktu respon pada Penyedia Layanan Internet Iconnet 01,32 detik dan IM3 Ooredoo 03,37 detik dan Telkomsel Orbit 05,30 detik. Open VPN membutuhkan waktu respon yang cukup lama yaitu 06,29 detik pada penyedia layanan IM3 Ooredoo.

4. KESIMPULAN

Berdasarkan pada hasil penelitian diperoleh kesimpulan bahwa VPN PPTP, L2TP dan OpenVPN memiliki integritas yang baik dan dapat diakses oleh beberapa Penyedia Layanan Internet yang berbeda, waktu respon tercepat dimiliki oleh VPN PPTP dan terlama oleh OpenVPN, jumlah paket data yang terkirim selama proses komunikasi yang berjalan dengan Compressed data pada VPN PPTP sebanyak 448, pada VPN L2TP dengan ESP (SPI=0x00f64f2f) sebanyak 472, dan Open VPN dengan P_DATA_V1 sebanyak 224. Dari segi enkripsi VPN PPTP memiliki kelemahan karena masih ada data yang bisa terbaca oleh sniffer yaitu username, alamat IP klien dan perangkat yang terhubung dengan VPN, untuk VPN L2TP hanya Alamat IP klien yang terbaca oleh sniffer, sedangkan OpenVPN terenkripsi dengan baik. Protokol VPN yang sesuai dengan kebutuhan sekolah dari sisi kemananan adalah OpenVPN.
Saran memuat berbagai usulan atau pendapat yang sebaiknya dikaitkan oleh penelitian sejenis. Saran dibuat berdasarkan kelemahan, pengalaman, kesulitan, kesalahan, temuan baru yang belum diteliti dan berbagai kemungkinan arah penelitian selanjutnya

5. REFERENSI

[1] Affandi, M. (2022). Implementasi Virtual Private Network (Vpn) Open vpn Dengan Keamanan Sertifikat SSL pada Network Attached Storage (Nas) Freenas. Jurnal Impresi Indonesia, 1(12), 1329–1341.
[2] G. Pañeda, X., Melendi, D., Corcoba, V., G. Pañeda, A., García, R., & García, D. (2024). Forensic Analysis of File Exfiltrations Using AnyDesk, TeamViewer and Chrome Remote Desktop. Electronics (Switzerland), 13(8).
[3] Haeruddin, H., & Kelvin, K. (2022). Analisa Penggunaan VPN L2TP dan SSTP di Masa Pandemi Covid-19. Jurnal Ilmu Komputer Dan Bisnis, 13(1), 105–114.
[4] Kurniawan, A. (2023). Analisis Performansi Remote Acces VPN Menggunakan PPTP dan L2TP Untuk Kebutuhan Work From Home (WFH) bagi Karyawan PT Dunia Makmur Jaya. Jurnal Pendidikan Tambusai, 7(2), 7378–7389.

[5] Kustian, M. A. (2023). Analisis Forensik Penggunaan Fungsi Hash Dalam Menentukan Keaslian Video, Metadata Image Dan Magic Number File. Jurnal Sains, Nalar, Dan Aplikasi Teknologi Informasi, 2(2), 10–16.
[6] Luthfansa, Z. M., & Rosiani, U. D. (2021). Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet. Journal of Information Engineering and Educational Technology, 5(1), 34–39.
[7] Pratama, H., & Puspitasari, N. F. (2021). Penerapan Protokol L2TP/IPSec dan Port Forwarding untuk Remote Mikrotik pada Jaringan Dynamic IP. Creative Information Technology Journal, 7(1), 51.
[8] Putra, U., Yptk, I., & Email, C. (2022). Protocol and Ipsec Methods As Network. Implementation Of Vpn Server Using L2tp Protocol And Ipsec Methods As Network Security, 16, 754–760.
[9] Riansah, M. F. (2024). Perancangan Dan Implentasi Jaringan VPN Dengan Metode L2TP/SSTP Pada PT. Palapa Media Indonesia. OKTAL : Jurnal Ilmu Komputer Dan Science, 3(3), 581–588.
[10] Syifa, S. (2022). Implementasi Checksum Dengan Menggunakan Algoritma Fletcher Untuk Mendeteksi Keaslian Sertifikat Rumah. Jurnal Sains Dan Teknologi Informasi, 2(1), 1–6.
[11] Wicaksana, M. R. N. (2022) Private Network Layer 2 Tunneling Protocol (L2TP) Berbasis Mikrotik: Perancangan Virtual Private Network Layer 2 Tunneling Protocol (L2TP) Berbasis Mikrotik. Journal of Network and Computer Applications, 1(1), 38–47.