

Implementasi Perancangan Virtual Private Network (VPN) dan Pembatasan Media Access Control Address pada PT Pegadaian Kantor Area Palembang

Kharisma Pangestu

Program Studi Teknik Informatika

Universitas Bina Darma

email : myusufs68@gmail.com

Jl. A. Yani No. 12, Palembang 30624, Indonesia

Abstract

The development of information technology and computer networks has become a primary requirement in supporting company operational activities. PT Pegadaian has an internal network that can only be accessed through a cable network and internal switches to maintain data security. However, the limited number of cable devices and employee work mobility are obstacles to operational efficiency. This study aims to implement a Virtual Private Network (VPN) over a Wireless Local Area Network (WLAN) by implementing Media Access Control (MAC) address restrictions and WPA2-PSK security. The method used is the Network Development Life Cycle (NDLC) which includes the stages of analysis, design, simulation, implementation, monitoring, and management. The results of the study show that all registered user devices successfully connected to the VPN network via WLAN. In addition, user restrictions through MAC address filtering have been proven to improve network security. Thus, the implementation of a WLAN-based VPN with MAC address and WPA2-PSK security has successfully increased the flexibility and security of internal network access at PT Pegadaian's Palembang Area Office.

Kata kunci: VPN; WLAN; access point; MAC address; NDLC.

Abstrak

Perkembangan teknologi informasi dan jaringan komputer telah menjadi kebutuhan utama dalam menunjang aktivitas operasional perusahaan. PT Pegadaian memiliki jaringan internal yang hanya dapat diakses melalui jaringan kabel dan switch internal guna menjaga keamanan data. Namun, keterbatasan jumlah perangkat kabel serta mobilitas kerja karyawan menjadi kendala dalam efisiensi operasional. Penelitian ini bertujuan untuk mengimplementasikan Virtual Private Network (VPN) melalui jaringan Wireless Local Area Network (WLAN) dengan menerapkan pembatasan Media Access Control (MAC) address dan pengamanan WPA2-PSK. Metode yang digunakan adalah Network Development Life Cycle (NDLC) yang meliputi tahap analisis, perancangan, simulasi, implementasi, pemantauan, dan manajemen. Hasil penelitian menunjukkan bahwa seluruh perangkat pengguna yang terdaftar berhasil terhubung ke jaringan VPN melalui WLAN. Selain itu, pembatasan pengguna melalui penyaringan MAC address terbukti meningkatkan keamanan jaringan. Dengan demikian, implementasi VPN berbasis WLAN dengan pengamanan MAC address dan WPA2-PSK berhasil meningkatkan fleksibilitas serta keamanan akses jaringan internal PT Pegadaian Kantor Area Palembang.

Kata kunci: VPN; WLAN; access point; MAC address; NDLC.

1. PENDAHULUAN

Internet merupakan jaringan berskala global yang menghubungkan jutaan perangkat komputasi di seluruh dunia dan telah menjadi infrastruktur utama dalam mendukung transformasi digital di berbagai sektor. Dalam lingkungan perusahaan, internet dan jaringan komputer internal digunakan untuk menunjang proses operasional, pertukaran data antarunit kerja, akses ke server, serta pengelolaan basis data perusahaan secara terpusat. Ketersediaan koneksi jaringan yang cepat, stabil, dan aman menjadi faktor kunci dalam meningkatkan produktivitas dan kualitas layanan organisasi (Kurniawan & Wibowo, 2020; Nugroho, 2021).

Sebagian besar perusahaan menerapkan jaringan internal khusus yang dilengkapi dengan sistem penyaringan (filtering) dan mekanisme keamanan tertentu agar tidak dapat diakses oleh pihak luar. Jaringan internal ini dirancang untuk menjaga kerahasiaan data serta menjamin integritas sistem informasi perusahaan (Putra & Sari, 2019). Namun, seiring meningkatnya mobilitas kerja dan kebutuhan fleksibilitas akses, penggunaan jaringan berbasis kabel (Local Area Network/LAN) mulai mengalami keterbatasan. Untuk mengatasi permasalahan tersebut, dibutuhkan jaringan nirkabel (Wireless Local Area Network/WLAN) atau hotspot yang mampu memberikan akses jaringan secara fleksibel tanpa bergantung pada instalasi kabel fisik (Firmansyah et al., 2021).

PT Pegadaian merupakan perusahaan milik negara yang bergerak pada tiga lini bisnis utama, yaitu pembiayaan, emas, dan aneka jasa. Salah satu unit operasionalnya adalah PT Pegadaian Kantor Area Palembang yang mengandalkan jaringan internal untuk mendukung aktivitas administrasi, transaksi pembiayaan, pengelolaan data nasabah, serta pelaporan ke kantor pusat secara daring. Jaringan internal PT Pegadaian yang dikenal sebagai jaringan Passion saat ini hanya dapat diakses melalui media kabel jaringan (LAN), sehingga akses jaringan menjadi terbatas pada titik-titik tertentu di lingkungan kantor (Sari & Hidayat, 2020).

Kondisi tersebut menimbulkan kendala ketika jumlah pengguna jaringan meningkat, sementara ketersediaan perangkat kabel terbatas akibat faktor perangkat keras maupun perangkat lunak. Selain itu, mobilitas pegawai yang tinggi menyebabkan kebutuhan akses jaringan dari berbagai lokasi dalam gedung kantor semakin meningkat. Keterbatasan akses jaringan ini berpotensi menghambat kelancaran pekerjaan, khususnya dalam proses akses sistem internal perusahaan yang bersifat real-time dan terintegrasi (Wibisono & Pratama, 2021).

Salah satu solusi untuk mengatasi permasalahan tersebut adalah dengan menerapkan Virtual Private Network (VPN) berbasis WLAN. VPN memungkinkan pengguna untuk mengakses jaringan internal perusahaan melalui jaringan publik secara aman dengan mekanisme enkripsi data (Safitri & Nugraha, 2019). Untuk meningkatkan keamanan jaringan nirkabel, diperlukan pula sistem pembatasan akses berbasis MAC address serta penggunaan metode enkripsi WPA2-PSK yang terbukti mampu melindungi data dari penyadapan dan akses tidak sah (Yusuf et al., 2020; Kurniadi & Ramadhan, 2021).

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk mengimplementasikan VPN berbasis WLAN pada PT Pegadaian Kantor Area Palembang dengan sistem keamanan tambahan berupa pembatasan MAC address dan enkripsi WPA2-PSK. Implementasi ini diharapkan dapat meningkatkan fleksibilitas, keamanan, serta efisiensi akses jaringan internal perusahaan sekaligus mendukung kelancaran aktivitas kerja di lingkungan PT Pegadaian Kantor Area Palembang.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode Network Development Life Cycle (NDLC) yang terdiri atas beberapa tahapan utama, yaitu analisis, perancangan, simulasi, implementasi, pemantauan, dan manajemen.

2.1 Tahap Analisis

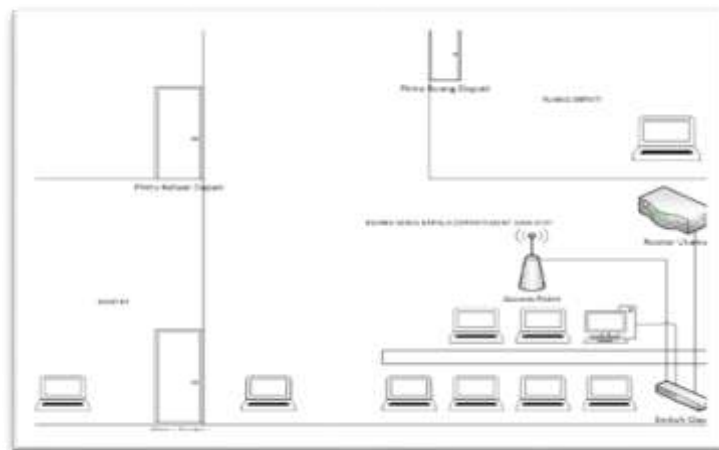
Analisis dilakukan pada infrastruktur jaringan PT Pegadaian Kantor Area Palembang. Hasil analisis menunjukkan bahwa jaringan internal masih mengandalkan kabel LAN dan konektor RJ45. Akses ke jaringan VPN hanya dapat dilakukan melalui jaringan kabel, sehingga mobilitas pengguna menjadi terbatas. Untuk mengatasi permasalahan tersebut, diperlukan penambahan access point sebagai media akses WLAN ke jaringan VPN.

Perangkat yang digunakan dalam penelitian ini meliputi:

1. Access point sebagai media utama akses WLAN.
2. Laptop sebagai perangkat konfigurasi dan klien.
3. Kabel LAN sebagai media penghubung jaringan.
4. Topologi jaringan lantai dua Kantor Area Palembang sebagai objek implementasi.

2.2 Tahap Perancangan

Pada tahap ini dilakukan penambahan access point ke dalam topologi jaringan yang telah ada. Perangkat tersebut dihubungkan langsung ke router utama jaringan internal PT Pegadaian. Selain itu, dirancang pula sistem penyaringan MAC address sebagai mekanisme pembatasan pengguna.



Gambar 1 Topologi Pada PT Pegadaian Area Palembang Lantai 2

2.3 Tahap Simulasi

Simulasi dilakukan dengan mengonfigurasi access point untuk menyebarkan jaringan WLAN yang terhubung langsung ke jaringan VPN PT Pegadaian. Tahapan konfigurasi meliputi penyambungan kabel LAN, pengaturan SSID, konfigurasi keamanan WPA2-PSK, serta penyaringan MAC address.

2.4 Tahap Implementasi

Implementasi dilakukan secara langsung pada jaringan lantai dua PT Pegadaian Kantor Area Palembang. Pengujian dilakukan melalui beberapa tahapan, yaitu: Uji konektivitas ke gateway VPN. Uji akses ke situs internal PT Pegadaian. Uji pemblokiran akses ke situs publik.

2.5 Tahap Pemantauan dan Manajemen

Pemantauan dilakukan untuk memastikan hanya perangkat yang terdaftar pada MAC address filtering yang dapat terhubung ke jaringan. Admin jaringan bertugas mengelola pendaftaran perangkat baru serta memelihara sistem keamanan jaringan.

3. HASIL DAN PEMBAHASAN

Hasil Uji Konektivitas VPN

Pengujian konektivitas dilakukan dengan melakukan ping ke alamat gateway VPN PT Pegadaian. Hasil pengujian menunjukkan bahwa koneksi berhasil terhubung dengan baik.

Hasil Uji Akses Sistem Internal

Pengujian akses ke situs internal PT Pegadaian melalui alamat <https://passion.pegadaian.co.id> menunjukkan bahwa pengguna berhasil mengakses sistem internal setelah terhubung ke jaringan VPN melalui WLAN.

Hasil Uji Akses Internet Publik

Pengujian akses ke situs publik seperti Google menunjukkan bahwa ketika pengguna terhubung ke jaringan VPN PT Pegadaian, akses ke internet umum dibatasi. Hal ini membuktikan bahwa pengguna benar-benar berada pada jaringan internal perusahaan.

Hasil Penerapan Penyaringan MAC Address

Pengujian terhadap perangkat yang tidak terdaftar menunjukkan bahwa perangkat tersebut tidak dapat terhubung ke jaringan WLAN. Dengan demikian, penyaringan MAC address terbukti efektif dalam membatasi akses pengguna hanya kepada perangkat yang telah memperoleh izin dari administrator.

Pembahasan

Implementasi jaringan VPN berbasis WLAN pada PT Pegadaian Kantor Area Palembang terbukti memberikan peningkatan yang signifikan terhadap fleksibilitas kerja karyawan. Sebelum penerapan sistem ini, akses ke jaringan internal perusahaan hanya dapat dilakukan melalui koneksi kabel (LAN), sehingga pengguna sangat bergantung pada ketersediaan port jaringan dan perangkat fisik. Dengan adanya VPN berbasis WLAN, karyawan kini dapat mengakses jaringan internal secara nirkabel dari berbagai titik dalam area kantor tanpa kehilangan fungsi keamanan. Hal ini berdampak langsung pada peningkatan mobilitas kerja dan efisiensi operasional sehari-hari.

Dari sisi keamanan jaringan, penerapan enkripsi WPA2-PSK dan pembatasan akses berbasis MAC address menunjukkan hasil yang sangat efektif. Penggunaan WPA2-PSK memastikan bahwa data yang dikirimkan melalui jaringan WLAN terenkripsi dengan baik sehingga tidak mudah disadap oleh pihak yang tidak berwenang. Sementara itu, filtering MAC address berfungsi sebagai lapisan keamanan tambahan yang memastikan hanya perangkat yang terdaftar saja yang dapat terhubung ke jaringan VPN. Kombinasi kedua metode ini menciptakan sistem keamanan berlapis yang mampu meminimalkan risiko penyusupan jaringan.

Hasil pengujian menunjukkan bahwa seluruh perangkat yang telah terdaftar dalam daftar MAC address berhasil terhubung ke jaringan VPN melalui WLAN tanpa mengalami hambatan berarti. Sebaliknya, perangkat yang tidak terdaftar secara otomatis ditolak aksesnya oleh sistem. Hal ini menunjukkan bahwa mekanisme autentikasi dan pembatasan perangkat berjalan sesuai dengan rancangan sistem yang telah ditetapkan. Keberhasilan ini membuktikan bahwa sistem mampu melakukan kontrol akses secara akurat dan konsisten.

Selain pembatasan perangkat, pembatasan akses terhadap internet publik juga berperan penting dalam menjaga stabilitas dan keamanan jaringan VPN. Dengan membatasi akses hanya pada layanan internal perusahaan, potensi gangguan dari lalu lintas internet eksternal dapat ditekan. Kebijakan ini sangat penting untuk memastikan bahwa bandwidth jaringan digunakan secara optimal untuk kepentingan operasional perusahaan dan tidak disalahgunakan untuk aktivitas non-produktif.

Dari sisi kinerja jaringan, penggunaan VPN berbasis WLAN tidak menunjukkan penurunan yang signifikan terhadap kecepatan akses layanan internal. Hal ini menandakan bahwa konfigurasi jaringan, enkripsi, serta manajemen trafik telah dirancang dengan baik. Sistem tetap mampu melayani kebutuhan akses data secara stabil meskipun melalui jalur nirkabel. Stabilitas ini sangat penting mengingat layanan internal PT Pegadaian mencakup sistem pembiayaan, pengelolaan data nasabah, dan transaksi operasional harian.

Secara keseluruhan, implementasi VPN berbasis WLAN di lingkungan PT Pegadaian Kantor Area Palembang tidak hanya meningkatkan fleksibilitas kerja, tetapi juga memperkuat aspek keamanan jaringan dan efisiensi akses sistem internal. Sistem ini memberikan solusi yang tepat terhadap keterbatasan jaringan berbasis kabel yang sebelumnya digunakan. Dengan keberhasilan implementasi ini, PT Pegadaian memiliki fondasi jaringan yang lebih modern, aman, dan adaptif terhadap perkembangan teknologi informasi serta kebutuhan operasional di masa mendatang.

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa: Jaringan VPN PT Pegadaian merupakan komponen vital dalam menunjang aktivitas operasional perusahaan. Implementasi WLAN pada jaringan VPN meningkatkan fleksibilitas dan mobilitas pengguna dalam mengakses jaringan internal. Penerapan penyaringan MAC address dan enkripsi WPA2-PSK terbukti mampu meningkatkan keamanan jaringan. Sistem yang dibangun mampu mempercepat akses jaringan bagi karyawan serta mengurangi ketergantungan terhadap kabel LAN.

Referensi

- Firmansyah, R., Purnama, S., & Astuti, D. (2021). Analisis Implementasi Jaringan Wireless pada Lingkungan Perusahaan. *Jurnal Teknologi Informasi*, 8(2), 115–123.
- Kurniawan, A., & Wibowo, T. (2020). *Manajemen Infrastruktur Jaringan Komputer*. Jakarta: Andi Publisher.
- Kurniadi, D., & Ramadhan, R. (2021). Keamanan Jaringan Berbasis WLAN Menggunakan WPA2-PSK. *Jurnal Sistem Informasi dan Jaringan*, 6(1), 44–52.
- Nugroho, A. (2021). *Transformasi Digital dalam Organisasi*. Bandung: Informatika.
- Putra, H., & Sari, M. (2019). Sistem Keamanan Jaringan Internal Perusahaan. *Jurnal Ilmu Komputer*, 7(3), 201–209.
- Safitri, N., & Nugraha, D. (2019). Implementasi VPN untuk Keamanan Akses Jaringan Perusahaan. *Jurnal Teknologi dan Sistem Komputer*, 5(2), 98–106.
- Sari, L., & Hidayat, A. (2020). Pemanfaatan Jaringan Internal dalam Sistem Informasi Pegadaian. *Jurnal Sistem Informasi*, 9(1), 67–75.
- Wibisono, R., & Pratama, Y. (2021). Analisis Kebutuhan Infrastruktur Jaringan pada Lingkungan Perkantoran. *Jurnal Teknik Komputer*, 4(2), 133–141.
- Yusuf, M., Prabowo, A., & Santoso, D. (2020). Pengamanan Jaringan Nirkabel Berbasis MAC Address Filtering. *Jurnal Keamanan Siber*, 3(1), 21–29.