Jurnal Riset Multidisiplin Edukasi
https://journal.hasbaedukasi.co.id/index.php/jurmie
Halaman : 201 - 219

Implementasi Wireguard VPN di Mikrotik Untuk Pengembangan Akses Jarak Jauh Dengan Metode NDLC Pada PT Excellent Infotama Kreasindo

Muhammad Nugi Abdiansyah[1], Imam Farisi[2]
Teknik Informatika; Universitas Bina Insani; Jl. Raya Siliwangi No.6, RT.001/RW.004, Sepanjang Jaya, Kec.Rawalumbu, Kota Bekasi, Jawa Barat 17114, (021) 82400924[1,2]
Email: imam@binainsani.ac.id

Informasi

Volume : 2
Nomor : 9
Bulan : September
Tahun : 2025
E-ISSN : 3062-9624

Abstract

The rapid advancement of information technology has driven the need for secure and efficient network access solutions, particularly for companies that require remote connectivity. One such solution that has emerged is the use of modern VPN protocols, such as WireGuard, which offers faster speeds and better security compared to traditional VPN protocols. PT Excellent Infotama Kreasindo, a company engaged in the field of computerization and information technology, requires stable remote access to support its business operations. The implementation of WireGuard VPN on MikroTik devices using the Network Development Life Cycle (NDLC) method was carried out to enhance the performance of secure and efficient remote access.

Keyword: *WireGuard, MikroTik, VPN, Remote Access, NDLC*

Abstrak

Kemajuan teknologi informasi yang pesat mendorong kebutuhan akan solusi akses jaringan yang aman dan efisien, terutama untuk perusahaan yang membutuhkan konektivitas jarak jauh. Salah satu solusi yang berkembang adalah penggunaan protokol VPN modern, seperti WireGuard, yang menawarkan kecepatan dan keamanan lebih baik dibandingkan dengan protokol VPN tradisional. PT Excellent Infotama Kreasindo, sebagai perusahaan yang bergerak di bidang komputerisasi dan teknologi informasi, membutuhkan akses jarak jauh yang stabil untuk mendukung operasional bisnisnya. Implementasi WireGuard VPN di perangkat MikroTik menggunakan metode Network Development Life Cycle (NDLC) dilakukan untuk meningkatkan kinerja akses jarak jauh yang aman dan efisien.

Kata Kunci: *WireGuard, MikroTik, VPN, Akses Jarak Jauh, NDLC*

A. PENDAHULUAN

Perkembangan teknologi informasi yang pesat mendorong perusahaan untuk menyediakan solusi akses jarak jauh yang aman dan fleksibel, guna mendukung mobilitas kerja yang semakin tinggi serta kebutuhan operasional yang tidak terbatas oleh lokasi. PT Excellent Infotama Kreasindo (EIK), sebagai penyedia layanan komputerisasi khususnya di bidang email service, menghadapi tantangan dalam mengelola infrastruktur jaringan internal yang tidak selalu dapat diakses secara langsung oleh tim teknis.

Saat ini, akses jarak jauh ke infrastruktur internal EIK masih bergantung pada layanan pihak ketiga seperti Anydesk, Zoho, dan TeamViewer. Meskipun solusi ini mempermudah akses remote, ketergantungan pada aplikasi eksternal menimbulkan potensi risiko keamanan dan kendala fleksibilitas dalam pengelolaan akses, serta menambah biaya operasional. Oleh karena itu, dibutuhkan solusi yang mampu memberikan kendali penuh bagi perusahaan tanpa bergantung pada layanan luar [1].

Virtual Private Network (VPN) merupakan salah satu solusi umum untuk menyediakan akses jarak jauh yang aman. Beberapa protokol VPN tradisional seperti PPTP, L2TP/IPSec, dan OpenVPN masih banyak digunakan, namun masing-masing memiliki keterbatasan. OpenVPN, misalnya, dikenal stabil dan aman namun cenderung memiliki kompleksitas konfigurasi dan penggunaan resource CPU yang tinggi, terutama saat digunakan dalam skala besar L2TP/IPSec juga menghadirkan tingkat keamanan yang baik namun konfigurasi yang kompleks dan performa yang terbatas pada perangkat modern membuatnya kurang optimal untuk kebutuhan fleksibilitas [2][3][4].

WireGuard hadir sebagai solusi VPN modern yang mengutamakan kesederhanaan, performa, dan keamanan. Dengan jumlah kode sekitar 4.000 baris, jauh lebih sedikit dibanding OpenVPN dan IPSec yang mencapai ratusan ribu baris, WireGuard lebih mudah diaudit dan memiliki attack surface yang lebih kecil [5]. Secara performa, WireGuard mampu menghasilkan throughput yang lebih tinggi dengan konsumsi CPU lebih rendah dibandingkan IPSec, baik dalam konfigurasi single tunnel maupun bonding. Selain itu, WireGuard mendukung forward secrecy dan menggunakan algoritma kriptografi modern seperti Curve25519 dan ChaCha20-Poly1305 yang lebih efisien untuk perangkat mobile dan server multi-core [6][7].

Dengan mempertimbangkan kebutuhan EIK untuk menyediakan akses jarak jauh yang aman, mudah digunakan, dan dapat dikendalikan sepenuhnya, implementasi WireGuard VPN pada perangkat Mikrotik dinilai sebagai solusi yang tepat. Solusi ini diharapkan mampu meningkatkan produktivitas kerja tim teknis, menjaga keamanan data perusahaan, serta

mendukung operasional yang lebih fleksibel di tengah tantangan keamanan siber yang semakin kompleks [8][9].

Penelitian ini akan menerapkan metode Network Development Life Cycle (NDLC) dalam proses perancangan hingga implementasi, sehingga solusi yang dihasilkan tidak hanya sesuai kebutuhan teknis, tetapi juga mendukung kelangsungan operasional bisnis perusahaan.

B. METODE PENELITIAN

Metode penelitian merupakan metode ilmiah yang di gunakan pada saat melakukan penelitian.

Teknik Pengumpulan Data

Dalam melakukan suatu penelitian, ada beberapa teknik yang digunakan dalam pengumpulan data, diantaranya:

Observasi

Observasi dalam komputer jaringan melibatkan pengamatan langsung terhadap sistem akses jarak jauh di kantor milik EIK. Ini mencakup pemantauan kinerja perangkat keras, perangkat lunak, dan interaksi antar komponen jaringan. Dengan melakukan observasi, dapat diidentifikasi potensi masalah, pola penggunaan, dan karakteristik sistem secara real-time.

Wawancara

Wawancara dalam konteks sistem akses jarak jauh, penulis mengumpulkan data secara langsung dengan narasumber yang diwawancarai yaitu administrator jaringan dan teknisi EIK, wawancara dilakukan di alamat Ruko Premier Serenity Blok J No. 12 Jl. KH Agus Salim No 40 E Bekasi Jaya Bekasi Timur, Bekasi 17112 Jawa Barat, Indonesia selama tanggal 01 November 2024 s.d. 31 Januari 2025. Tujuan wawancara adalah untuk memahami kebutuhan teknisi dan mengumpulkan informasi tentang masalah yang mungkin terjadi dalam pengelolaan jaringan di EIK.

Studi Pustaka

Studi pustaka melibatkan pencarian dan analisis literatur terkait sistem akses jarak jauh. Ini mencakup artikel jurnal, dokumentasi resmi mengenai Mikrotik dan buku untuk memahami konsep, teori, dan praktik terkait wireguard di mikrotik untuk sistem jarak jauh. Studi pustaka membantu menyusun dasar pengetahuan yang kuat untuk perancangan, implementasi, dan pemeliharaan jaringan.

Model Pengembangan

Pada penelitian yang dilakukan oleh penulis, metode yang digunakan adalah NDLC (Network Design and Implementation Cycle) merupakan suatu metode terstruktur yang digunakan dalam proses pengembangan jaringan komputer. Pendekatan ini melibatkan tahapan-tahapan yang harus dijalankan secara berurutan, mulai dari perancangan, pembangunan, penerapan, hingga pemeliharaan jaringan agar tetap efisien dan handal [10].

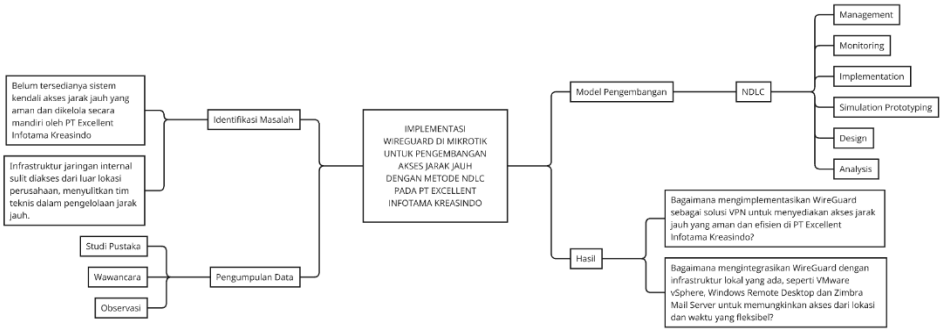
Sumber: Yulianto & Aprilyani, (2020)

Gambar 1. Network Development Life Cycle

Pada gambar metode NDLC tersebut dapat disimpulkan bahwa penulisan laporan ini melakukan tahapan analysis sampai dengan management.

Kerangka Pemikiran

Dalam memudahkan penelitian ini, maka diperlukannya susunan kerangka pemikiran secara terperinci, kerangka pemikiran ini merupakan Langkah-langkah yang akan dilakukan dalam menyelesaikan masalah yang akan dibahas. Adapun kerangka kerja penelitian yang digunakan dapat dilihat pada Gambar 2.



Sumber: Hasil Penelitian (2025)

Gambar 2. Kerangka Pemikiran

Identifikasi Masalah

Mengidentifikasi masalah-masalah apa saja yang terjadi di jaringan berjalan pada EIK

Pengumpulan Data

Pada tahap ini peneliti melakukan pengumpulan data dengan cara observasi jaringan yang sedang berjalan, wawancara langsung dengan administrator jaringan dan teknisi dan studi pustaka sebagai informasi dan referensi.

Model Pengembangan

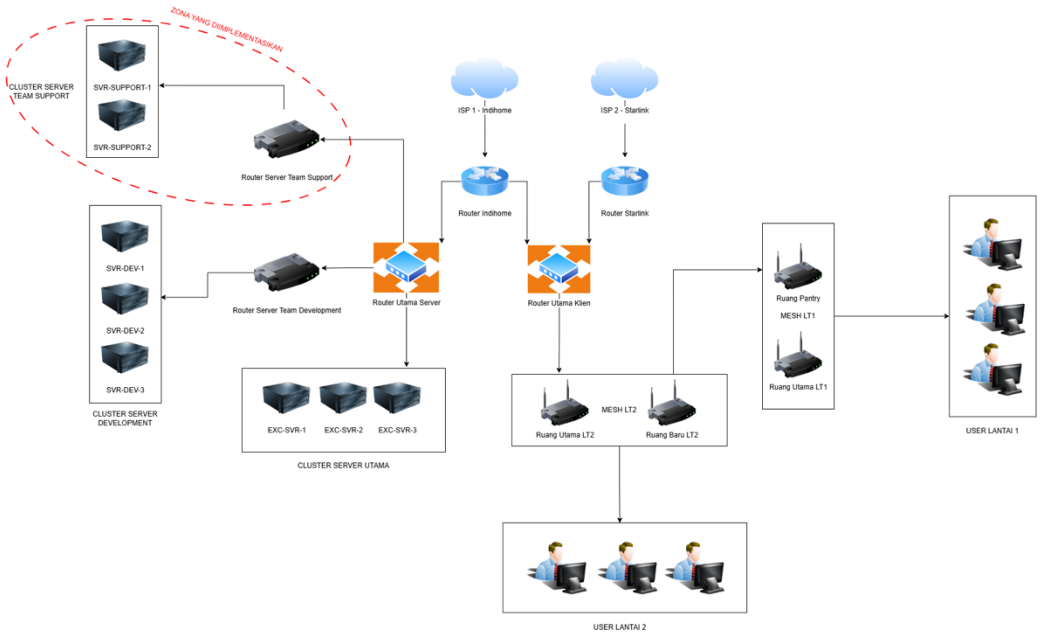
Model pengembangan yang digunakan adalah NDLC dimana metode ini bertujuan mempunyai fase, tahapan, langkah atau mekanisme proses desain ulang jaringan komputer dengan baik dan benar.

Hasil Penelitian

Protocol Wireguard bisa berjalan dengan baik dimana pengguna pada EIK dapat terkoneksi ke jaringan internal dari manapun namun dilengkapi dengan keamanan yang terjaga dengan adanya pembatasan akses menggunakan jaringan IP Publik VPN EIK.

C. HASIL DAN PEMBAHASAN

Berikut ini adalah topologi yang ada pada EIK berdasarkan hasil analisis yang dilakukan secara langsung dikantor milik EIK:

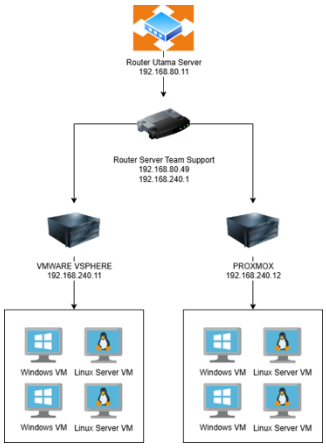


Sumber: Hasil Penelitian (2025)

Gambar 3. Topologi Jaringan EIK

Gambar diatas merupakan Topologi Jaringan yang ada pada EIK dimana ISP yang digunakan untuk user menggunakan 2 ISP yaitu Indihome dan Starlink sementara untuk cluster server menggunakan 1 ISP saja yaitu Indihome. Antara Jaringan user maupun Jaringan cluster server dapat terkoneksi satu dengan yang lainnya menggunakan Static Routing pada Router

Utama Klien dan Router Utama Server. Kemudian untuk Router Utama Server terbagi menjadi 3 cluster server yaitu cluster server utama yang langsung dibawah Router Utama Server, cluster development server menggunakan Router Server Team Development dan cluster server team support menggunakan Router Server Team Support. Dalam penelitian ini yang akan dibahas adalah cluster server team support yang menggunakan Router Server Team Support dengan aplikasi yang ada didalamnya.



Sumber: Hasil Penelitian (2025)

Gambar 4. Topologi Server Cluster Team Support

Pada gambar diatas, adalah gambaran alur topologi cluster server team support secara spesifik, dimana terdapat server VMware vSphere dan server Proxmox. Dalam server masing masing terdapat Virtual Machine (VM) yang terdiri dari OS Windows maupun Linux.

Permasalahan Sistem Jaringan

Berdasarkan hasil analisis yang dilakukan terhadap topologi jaringan milik EIK, dapat disimpulkan bahwa terdapat permasalahan yaitu:

1 Belum tersedianya sistem kendali akses jarak jauh yang aman dan dikelola secara mandiri oleh perusahaan.
2 Infrastruktur jaringan internal sulit diakses dari luar lokasi perusahaan, menyulitkan tim teknis dalam pengelolaan jarak jauh.

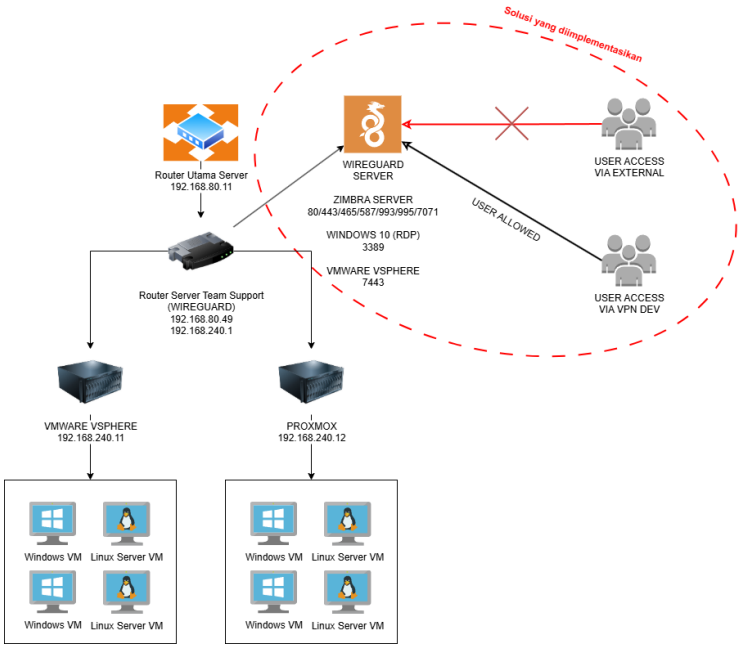
Alternatif Pemecahan Masalah

Adapun solusi alternatif dari permasalahan berikut ialah membuat perencanaan jaringan baru dengan menggunakan protocol Wireguard, yang nantinya dapat diimplementasikan untuk dilakukan pengembangan.

Rencana Jaringan Usulan

Setelah diketahui permasalahan serta kekurangan yang ada pada jaringan internal EIK, maka diusulkan rancangan jaringan baru yang diharapkan dapat menjadi solusi untuk

perbaikan dan pengembangan jaringan existing. Dalam Topologi Jaringan terdapat penambahan jalur jaringan baru ke Wireguard Server (VPS Linode) yang nantinya akan dijadikan sebagai akses pusat user yang berada diluar jaringan internal untuk tetap dapat akses seperti jaringan internal.



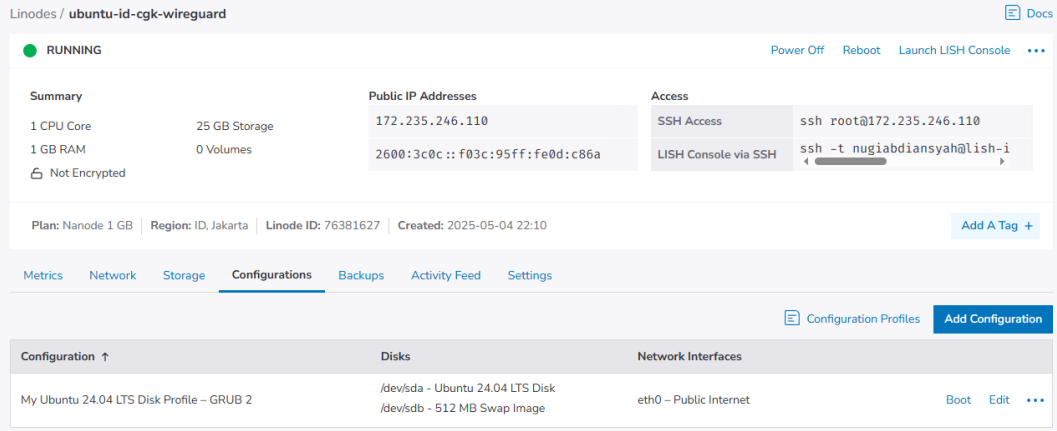
Sumber: Hasil Penelitian (2025)

Gambar 5. Topologi Jaringan Usulan

Pada Topologi Jaringan Usulan diatas, user yang berada di external diharapkan dapat mengakses jaringan lokal dengan menggunakan spesifik port pada VMware vSphere dengan spesifik port HTTPS yaitu 443 namun port forwarding secara khusus ke port 7443, kemudian Zimbra Mail Server dengan spesifik port HTTP/S yaitu port 80 / port 443, port SMTP/S yaitu port 465 (SSL) / port 587 (TLS), port POP3S/IMAPS yaitu port 993 (POP3S) / port 995 (IMAPS) dan port Zimbra Admin yaitu port 7071 serta port Remote Desktop Protocol (RDP) yaitu port 3389.

User external dapat mengakses jaringan lokal menggunakan IP VPN DEV Excellent, apabila user tidak menggunakan IP VPN DEV Excellent maka user juga tidak akan bisa mengakses jaringan lokal. Hal ini dipertimbangkan sebagai faktor keamanan pada sistem.

Hasil Implementasi Jaringan

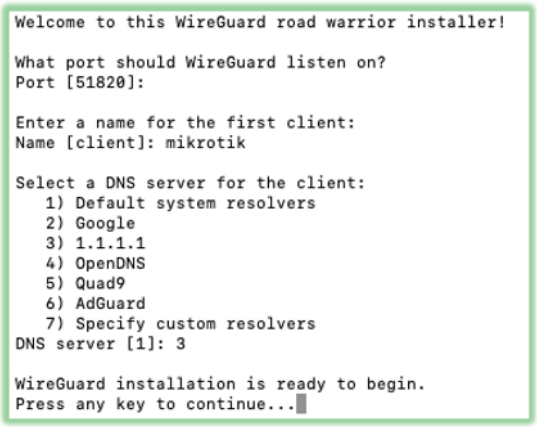


Sumber: Hasil Penelitian (2025)

Gambar 6. Spesifikasi Linode

Pada Gambar diatas adalah VPS Linode yang digunakan untuk Wireguard Server dengan spesifikasi 1 CPU Core, 1 GB RAM 25 GB Storage dan Sistem Operasi Ubuntu 24.04 LTS. Server diatas yang nantinya akan dijadikan sebagai pusat akses yang dapat terhubung dari manapun dan kapanpun.

Untuk implementasi hal pertama yang dilakukan adalah melakukan koneksi ke server terkait menggunakan SSH pada Terminal. Selanjutnya adalah melakukan instalasi Wireguard menggunakan script otomatis Nyr-Wireguard yang tersedia di Github.



Sumber: Hasil Penelitian (2025)

Gambar 7. Script Instalasi Wireguard

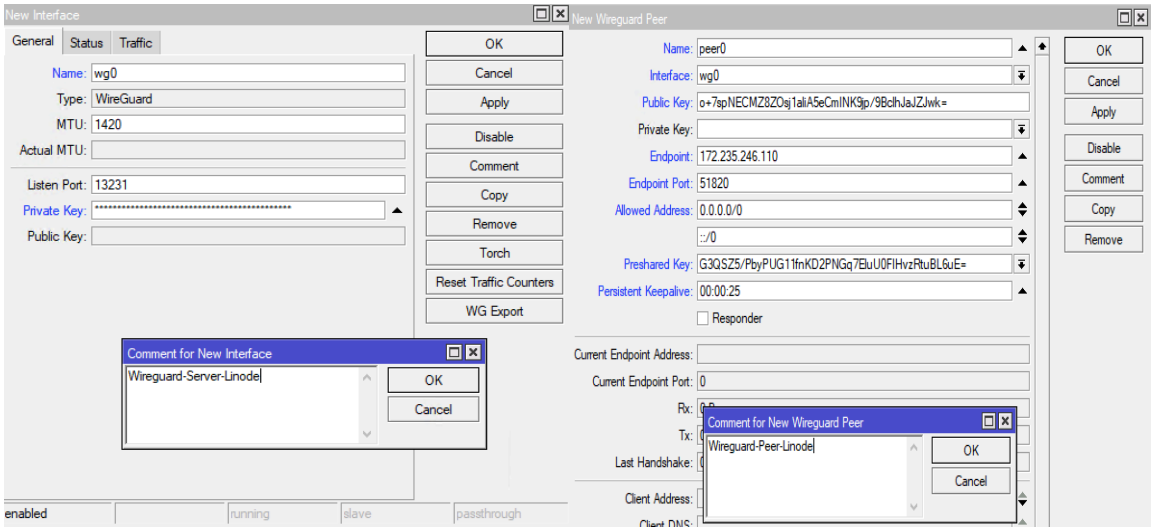
Pada Gambar diatas konfigurasi awal untuk Wireguard Server dengan port default yaitu 51820, nama klien mikrotik dan DNS menggunakan 1.1.1.1 (Cloudflare).

Sumber: Hasil Penelitian (2025)

Gambar 8. Hasil Konfigurasi Wireguard

Pada Gambar diatas adalah hasil dari implementasi Wireguard Server yang nantinya konfigurasi diatas akan digunakan sebagai mode integrasi dengan Mikrotik. Pada konfigurasi WireGuard sisi klien, terdapat dua bagian utama yaitu Interface dan Peer. Bagian Interface berisi konfigurasi untuk antarmuka WireGuard itu sendiri di perangkat klien. Di dalamnya terdapat Address, yang menunjukkan alamat IP lokal yang akan digunakan oleh antarmuka WireGuard, seperti misalnya 10.7.0.2/24. Kemudian ada DNS, yang mengatur server DNS yang akan digunakan selama koneksi WireGuard aktif, sehingga trafik DNS akan diarahkan melalui VPN, misalnya ke 1.1.1.1. Terakhir, terdapat PrivateKey, yaitu kunci privat milik klien yang digunakan untuk proses autentikasi dan enkripsi komunikasi; kunci ini bersifat rahasia dan hanya diketahui oleh klien.

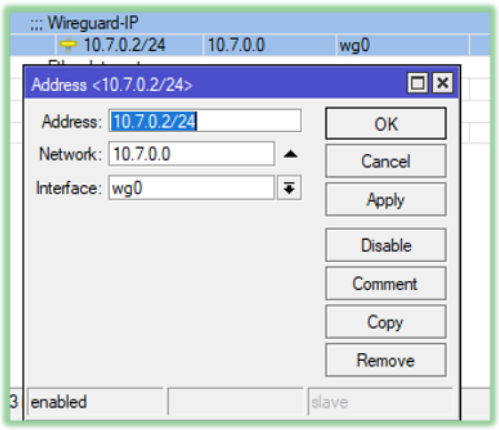
Bagian kedua adalah Peer, yang menggambarkan konfigurasi peer tujuan, dalam hal ini biasanya server WireGuard. PublicKey adalah kunci publik dari server yang digunakan klien untuk mengenkripsi data yang dikirim. Opsional, ada PresharedKey, yaitu kunci tambahan yang dipakai bersama-sama antara klien dan server untuk meningkatkan keamanan (pre-shared symmetric key). Parameter AllowedIPs menentukan rentang alamat IP yang bisa dikirim atau diterima melalui tunnel WireGuard; misalnya 0.0.0.0/0 jika semua trafik internet diarahkan melalui VPN. Selanjutnya, Endpoint menunjukkan alamat IP atau hostname dan port server WireGuard yang menjadi tujuan koneksi, contohnya 172.235.246.110:51820. Terakhir, PersistentKeepalive adalah pengaturan opsional yang berfungsi menjaga koneksi tetap hidup dengan mengirim paket keepalive secara berkala (biasanya setiap 25 detik), yang penting jika klien berada di balik NAT agar koneksi tidak tertutup oleh firewall atau router.



Sumber: Hasil Penelitian (2025)

Gambar 9. Konfigurasi Wireguard di Mikrotik

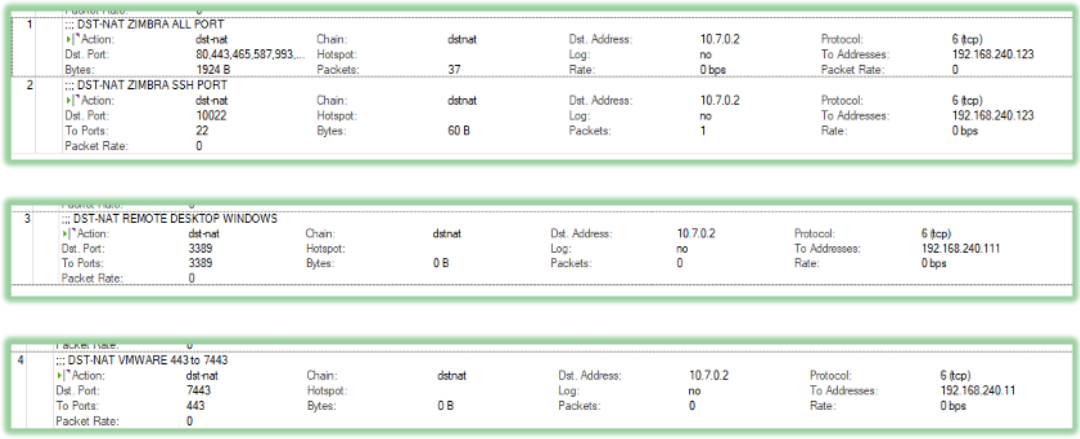
Pada Gambar diatas disisi Mikrotik haru dibuat terlebih dahulu Interface Wireguard sebagai gateway, dimana nilai yang dimasukkan Name wg0 dan Private Key yang sesuai dengan yang ada di Gambar 8. Agar mudah diidentifikasi tambahkan Comment for New Interface seperti Wireguard-Server-Linode. Pada Gambar diatas juga ditambahkan pula Wireguard Peers agar dapat terkoneksi antara VPS Linode dengan Mikrotik, kemudian sesuaikan nilai Name peer0, Interface wg0, Public Key Endpoint Endpoint Port Allowed Address Preshared Key Persistent Keepalive menggunakan nilai yang sama dengan yang ada pada Gambar 8. Agar mudah diidentifikasi tambahkan Comment for New Wireguard Peer dengan Wireguard-Peer-Linode.



Sumber: Hasil Penelitian (2025)

Gambar 10. Penambahan IP Wireguard di Mikrotik

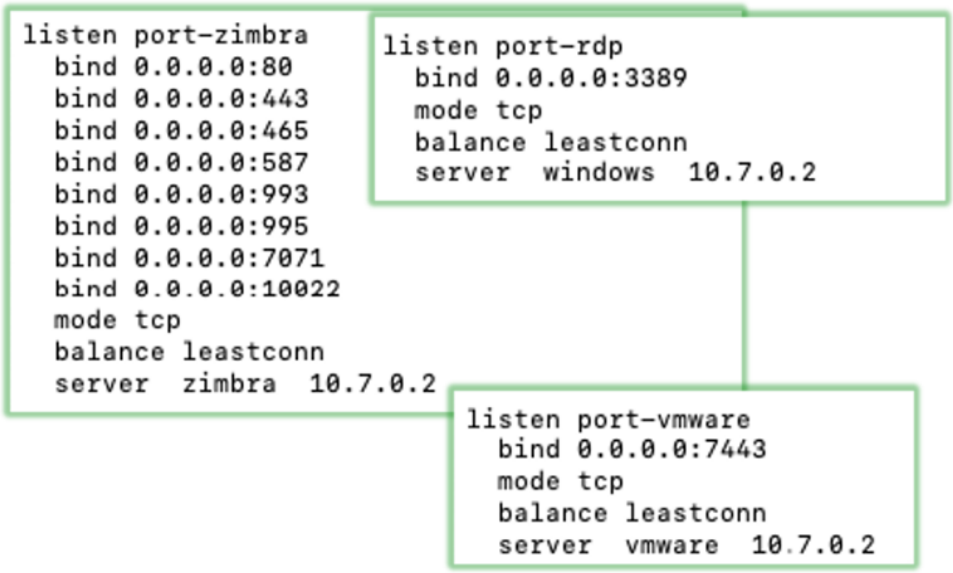
Pada Gambar ini pastikan untuk menambahkan IP Lokal Wireguard pada Mikrotik, nilai Address sesuai dengan yang ada pada Gambar 8 menggunakan Interface wg0.



Sumber: Hasil Penelitian (2025)

Gambar 11. Forwarding Akses di Mikrotik

Pada Gambar IV-13 dilakukan forwarding DST-NAT pada Mikrotik ke Zimbra Mail Server dengan port akses HTTP 80, HTTPS 443, SMTPS 465, SMTP-TLS 587, POP3S 993, IMAPS 995 dan Zimbra Admin 7070 serta port 22 yang ditranslasikan ke port 10022, Remote Desktop Windows dengan port akses 3389 yang sesuai dengan port akses default untuk Remote Desktop dan VMware dengan port akses 7433 yang sesuai dengan port akses default untuk VMware yaitu port 443.



Sumber: Hasil Penelitian (2025)

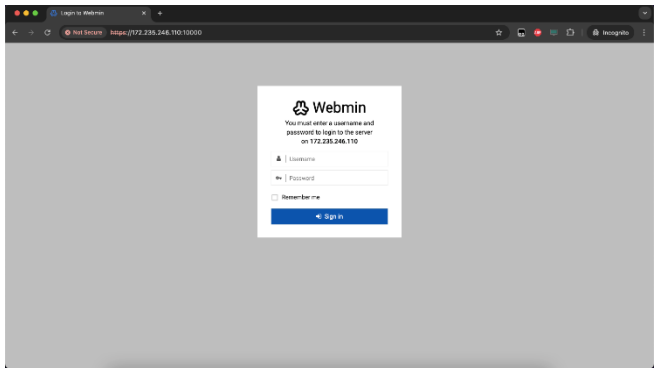
Gambar 12. Forwarding Akses di VPS Linode

Pada Gambar diatas dilakukan forwarding akses Zimbra menggunakan HAProxy agar dapat dengan mudah digunakan dengan port yang ditranslasikan yaitu HTTP 80, HTTP 443, SMTPS 465, SMTP-SSL 587, POP3S 993, IMAPS 995, Zimbra Admin 7071 dan SSH 10022 dari IP Lokal Mikrotik 10.7.0.2, Remote Desktop Windows via HAProxy agar dapat dengan mudah

digunakan dengan port yang ditranslasikan yaitu 3389 dari IP Lokal Wireguard 10.7.0.2 dan VMware vSphere via HAProxy agar dapat dengan mudah digunakan dengan port yang ditranslasikan yaitu 7443 dari IP Lokal Mikrotik 10.7.0.2.

Keamanan dan Limitasi Akses

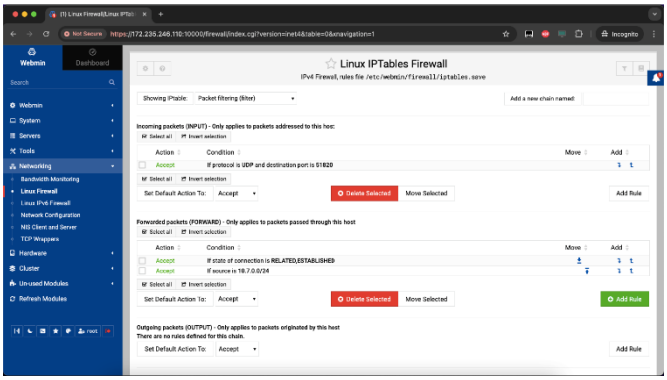
Untuk mempermudah akses keamanan dan melakukan limitasi akses, lakukan terlebih dahulu instalasi Webmin akses pada browser hingga muncul seperti ini:



Sumber: Hasil Penelitian (2025)

Gambar 13. Akses Webmin

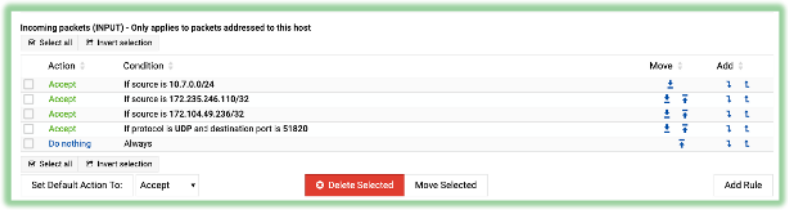
Pada Gambar diatas adalah tampilan Akses Webmin secara default biasanya diawali dengan https kemudian diikuti dengan IP Publik dan diakhiri dengan port 10000, dalam kasus peneliti jika diakses biasanya kurang lebih seperti ini https://172.235.246.110:10000



Sumber: Hasil Penelitian (2025)

Gambar 14. Setup Firewall (Sebelum)

Pada Gambar IV-22 diperlihatkan Linux IP Tables sebelum dilakukan penyesuaian dimana akses IP Publik masih bisa diakses oleh siapa saja asal tahu nama dan juga alamat IP Publik-nya. Sedangkan target yang diharapkan adalah akses hanya bisa dari IP VPN DEV Excellent yaitu 172.104.49.236.



Sumber: Hasil Penelitian (2025)

Gambar 15. Setup Firewall (Sesudah)

Pada Gambar IV-23 dilakukan penyesuaian IPTables dimana port yang ada di Wireguard Server hanya bisa diakses dari salah satu dari 3 segment IP ini yaitu 10.7.0.0/24 (Segment Wireguard), 172.235.246.110 (IP Publik Diri Sendiri) dan 172.104.49.236 (IP VPN Dev). Adapun pada konfigurasi ini belum dilakukan secara permanen karena untuk dilakukan uji coba nantinya dengan menyesuaikan rule paling bawah menjadi DROP.

DNS Publik

Untuk mempermudah akses, dilakukan penambahan DNS Publik pada nama wireguard.excelent.co.id agar mengarah ke IP Publik server Wireguard yaitu IP 172.235.246.110 agar mudah dikenali. Nantinya untuk pemanggilan server tidak perlu menggunakan IP Publik kembali namun sudah bisa menggunakan nama di internet yaitu wireguard.excellent.co.id dan dilakukan juga penambahan nama zimbra-demo.excellent.co.id pada IP Publik yang sama yaitu 172.235.246.110. Nantinya agar nama zimbra-demo.excellent.co.id dapat diakses oleh publik jadi tidak perlu menggunakan IP Publik seperti yang sebelumnya.

Sumber: Hasil Penelitian (2025)

Gambar 16. Penambahan DNS Publik

Hasil Pengujian Alfa

Tahap pengujian dilakukan untuk memastikan bahwa hasil implementasi sesuai dengan rancangan. Pengujian Alfa dilakukan dengan disisi perangkat jaringan dengan tujuan verifikasi fungsionalitas dasar, keamanan, dan performa dalam lingkungan simulasi khususnya pada teknisi. Dalam kasus ini pengujian dilakukan pada Router Mikrotik, Wireguard Server dan Teknisi yang bisa koneksi langsung ke Wireguard server. Berikut adalah tabel scenario dan pengujian alfa:

Tabel 1. Skenario Pengujian Alfa

No	Kasus Uji	Skenario Pengujian	Hasil Yang Diharapkan	Hasil Pengujian
1	Uji Konektivitas WireGuard	Ping 10.7.0.1 (VPS) dan 10.7.0.2 (MikroTik)	Latensi harus <50ms	Berhasil
		Mendapatkan IP Address dengan segment 10.7.0.0/24	Ping Segment IP 10.7.0.0/24	Berhasil
		Gunakan ping -n 100	Packet Loss <1%	Berhasil
2	Uji Port Forwarding	Akses RDP (3389) via WireGuard	Berhasil konek ke RDP dari teknisi	Berhasil
		Akses VMware (7443) via Wireguard	Berhasil konek ke VMware dari teknisi	Berhasil
		Akses Zimbra Mail Server (443) via Wireguard	Berhasil konek ke Zimbra Mail Server dari teknisi	Berhasil
3	Uji Keamanan Dasar	Coba akses pakai private key invalid di config teknisi	Pesan error gagal terkoneksi	Berhasil
		Coba akses pakai ip invalid di config teknisi	Pesan error gagal terkoneksi	Berhasil
		Coba akses port 3389 dari IP non-whitelist	Ditolak (timeout)	Berhasil

Sumber: Hasil Penelitian (2025)

Berdasarkan tabel pengujian alfa yang telah dilakukan terhadap teknisi, dapat disimpulkan bahwa seluruh parameter pengujian berjalan sesuai dengan target dan ekspektasi awal. Pengujian mencakup verifikasi konektivitas, validasi autentikasi, serta pengujian akses layanan internal melalui jalur VPN WireGuard. Berikut adalah poin-poin utama hasil pengujiannya:

Konektivitas Dasar WireGuard Berjalan Baik

Klien berhasil memperoleh alamat IP tunnel pada segmen 10.7.0.0/24, sesuai dengan konfigurasi yang telah ditetapkan. Pengujian konektivitas melalui perintah ping menunjukkan latency yang rendah dan stabil di bawah 50 ms, serta tidak ditemukan packet loss dalam pengujian normal.

Akses Layanan Internal Berhasil

Klien berhasil mengakses beberapa layanan internal melalui WireGuard, seperti Remote Desktop Protocol (RDP), VMware ESXi, dan Zimbra Mail Server, yang diakses melalui port forwarding Mikrotik. Hal ini menunjukkan bahwa konfigurasi port forwarding dan VPN routing berjalan dengan baik.

Mekanisme Keamanan WireGuard Berfungsi Optimal

Pengujian menggunakan private key yang tidak valid dan alamat IP yang tidak sesuai berhasil diblokir oleh sistem. Meskipun tampak tunnel terbentuk secara visual, namun tidak ada transfer data yang berhasil dilakukan dan koneksi ke server WireGuard gagal. Hal ini membuktikan bahwa WireGuard tidak hanya mengandalkan key exchange, tetapi juga validasi IP address sesuai konfigurasi server.

Firewall dan Filtering Mikrotik Berjalan Sesuai Harapan

Akses ke layanan RDP dari IP yang tidak terdaftar dalam whitelist Mikrotik berhasil ditolak. Hal ini menunjukkan bahwa mekanisme pengamanan pada level Mikrotik untuk memfilter koneksi berdasarkan IP sumber sudah berjalan dengan baik.

Secara keseluruhan, pengujian alfa membuktikan bahwa infrastruktur WireGuard VPN yang dibangun sudah berfungsi sesuai dengan desain, baik dari sisi konektivitas, keamanan, maupun akses ke layanan internal. Seluruh hasil pengujian sesuai dengan parameter yang telah ditentukan, sehingga implementasi WireGuard pada tahap alfa dinyatakan berhasil dan siap dilanjutkan ke tahap berikutnya, yaitu pengujian beta atau implementasi produksi secara terbatas.

Hasil Pengujian Beta

Pengujian dengan metode beta adalah evaluasi keandalan dan usability dalam kondisi real pengguna (Karyawan/Work From Anywhere). Berikut adalah tabel skenario dan pengujian beta:

Tabel 2. Skenario Pengujian Beta

No	Kasus Uji	Skenario Pengujian	Hasil Yang Diharapkan	Hasil Pengujian
1	Uji Konektivitas WireGuard	DNS Publik wireguard.excellent.co.id dikenali di Internet	Nama wireguard.excellent.co.id dikenali dimanapun	Berhasil
		DNS Publik zimbra-demo.excellent.co.id dikenali di Internet	Saat melakukan nslookup zimbra-demo.excellent.co.id dari manapun dapat mengenali	Berhasil

		Cek packet lost pada saat melakukan ping ke Wireguard Server	Packet loss <1% (gunakan ping -n 100)	Berhasil
		Akses Webmin Menggunakan Nama wireguard.excellent.co.id	Terkoneksi ke halaman login Webmin pada Browser	Berhasil
2	Uji Port Forwarding	Akses RDP (3389) via VPN Dev Excellent	Berhasil konek ke RDP dari pengguna	Berhasil
		Akses VMware (7443) via VPN Dev Excellent	Berhasil konek ke VMware dari pengguna	Berhasil
		Akses Zimbra Mail Server (443) via VPN Dev Excellent	Berhasil konek ke Zimbra Mail Server dari pengguna	Berhasil
3	Uji Keamanan Dasar	Coba akses port 3389 dari IP non-whitelist	Ditolak (timeout)	Berhasil
		Coba akses port 7443 dari IP non-whitelist	Ditolak (timeout)	Berhasil
		Coba akses port 443 dari IP non-whitelist	Ditolak (timeout)	Berhasil

Sumber: Hasil Penelitian (2025)

Berdasarkan tabel pengujian beta yang telah dilakukan terhadap pengguna, dapat disimpulkan bahwa implementasi VPN WireGuard beserta konfigurasi DNS, firewall, dan layanan internal berjalan sesuai dengan rencana serta target yang telah ditetapkan. Pengujian beta ini menitikberatkan pada validasi akses layanan melalui VPN dan pembatasan akses dari luar, yang bertujuan untuk memastikan keamanan serta ketersediaan layanan. Adapun kesimpulan utamanya sebagai berikut:

Resolusi DNS Berjalan Baik

Domain publik seperti wireguard.excellent.co.id dan zimbra-demo.excellent.co.id telah berhasil dikenali dari internet global melalui DNS resolver publik seperti Cloudflare (1.1.1.1). Ini memastikan bahwa nama domain dapat diakses secara global sesuai konfigurasi DNS.

Konektivitas Server Aman dan Stabil

Pengujian ping ke WireGuard Server dari internet menunjukkan konektivitas yang baik dan stabil dengan latency rendah dan tanpa packet loss, memastikan server siap menerima koneksi VPN dari berbagai lokasi.

Akses Layanan Internal Berhasil melalui VPN

Akses ke beberapa layanan internal seperti Webmin, VMware ESXi, dan Zimbra Mail Server berhasil dilakukan melalui VPN Dev Excellent menggunakan nama domain publik dan port yang sesuai. Hal ini membuktikan bahwa konfigurasi VPN, routing, serta port forwarding sudah berfungsi dengan baik.

Keamanan Firewall Berjalan Optimal

Seluruh upaya akses langsung ke layanan internal (RDP, VMware, Zimbra) dari IP non-whitelist atau tanpa VPN berhasil ditolak (timeout). Hal ini membuktikan bahwa firewall atau filter pada Mikrotik maupun server berhasil memblokir koneksi yang tidak sah sesuai skenario keamanan yang dirancang.

Akses Berbasis Whitelist Terbukti Efektif

Mekanisme whitelist yang diterapkan, baik di sisi Mikrotik maupun server, efektif membatasi akses ke port-port layanan tertentu, memastikan hanya perangkat yang sudah terautentikasi melalui VPN yang bisa mengakses layanan internal.

Kesimpulan akhir dari pengujian beta membuktikan bahwa seluruh komponen sistem mulai dari DNS, VPN WireGuard, firewall, hingga layanan internal telah terintegrasi dan berjalan dengan baik sesuai target pengujian. Sistem sudah siap untuk diterapkan lebih luas ke tahap produksi dengan tingkat keamanan dan ketersediaan layanan yang memadai.

Wawancara dengan Pengguna

Pada tahap ini dilakukan sesi wawancara dengan pengguna, pertanyaan-pertanyaan yang diajukan berdasarkan dari aspek kebergunaan dan pengujian yang telah dilakukan untuk mendapatkan feedback dari implementasi yang sudah dilakukan. Berikut adalah hasil wawancara yang dilakukan:

Tabel 3. Wawancara dengan Pengguna

Narasumber	Pertanyaan	Jawaban	Tanggal
Bpk. Ahmad Imanudin	Apakah solusi implementasi pada Mikrotik dengan Wireguard untuk akses jarak jauh pada PT Excellent Infotama Kreasindo membantu kinerja pengguna?	Menurut saya sangat membantu untuk Tim/Pengguna jadi bisa memanfaatkan infrastruktur yang ada di PT Excellent Infotama Kreasindo di manapun dan kapanpun	08 Mei 2025
Bpk. Ahmad Imanudin	Apakah dengan implementasi Wireguard yang dilakukan sisi keamanannya tetap terjaga dengan pembatasan yang dilakukan?	Kami punya VPN Dev Excellent untuk mengakses kebutuhan cloud, jadi bila bisa digunakan untuk mengakses jaringan infrastruktur lokal akan sangat baik. Skema pembatasannya pun berjalan sesuai dengan apa yang diharapkan.	08 Mei 2025
Bpk. Ahmad Imanudin	Apakah ada saran terkait implementasi Wireguard yang dilakukan?	Baiknya dilakukan juga sharing knowledge terkait apa yang dilakukan, bisa berupa blueprint, training atau sesi singkat pembahasan terkait hal ini.	08 Mei 2025

Sumber: Hasil Penelitian (2025)

D. KESIMPULAN

Berdasarkan hasil penelitian dan implementasi yang telah dilakukan di PT Excellent Infotama Kreasindo, penulis dapat menarik beberapa kesimpulan sebagai berikut:

1. Implementasi protokol WireGuard pada jaringan LAN PT Excellent Infotama Kreasindo yang terintegrasi dengan perangkat Mikrotik berhasil berjalan dengan baik. Hasil implementasi ini diuji pada pengguna/tim teknisi yang membutuhkan akses ke infrastruktur lokal, di mana mereka dapat terhubung secara aman dari mana saja dan kapan saja melalui VPN. Hal ini telah dibuktikan dalam pengujian beta, di mana layanan-layanan penting seperti Remote Desktop, VMware ESXi, dan Zimbra Mail Server berhasil diakses dengan stabil dan aman melalui jalur VPN.
2. Penerapan keamanan berbasis WireGuard dilengkapi dengan pengaturan autentikasi dan filtering akses yang ketat, sehingga hanya perangkat yang terhubung melalui VPN Dev Excellent dan telah tervalidasi yang dapat mengakses infrastruktur internal. Mekanisme ini diuji pada pengujian alfa, yang menunjukkan bahwa klien dengan private key yang salah atau konfigurasi IP yang tidak sesuai akan gagal membentuk koneksi yang valid. Selain itu, layanan internal tidak dapat diakses dari IP yang tidak terdaftar (non-whitelist), memastikan bahwa hanya pengguna yang berhak yang dapat mengakses jaringan internal.
3. Secara keseluruhan, implementasi WireGuard dan konfigurasi pendukungnya (DNS, firewall, port forwarding) terbukti mampu membangun jaringan yang aman, stabil, dan sesuai kebutuhan bisnis. Hal ini tercermin dari keberhasilan semua pengujian alfa (pengujian fungsionalitas dasar dan keamanan koneksi) serta pengujian beta (pengujian akses nyata terhadap layanan-layanan produksi dengan skenario pengguna sebenarnya).

E. DAFTAR PUSTAKA

[1] H. Awal, “Implementasi Intrusion Detection Prevention System Sebagai Sistem Keamanan Jaringan Komputer Kejaksaan Negeri Pariaman Menggunkan Snort Dan Iptables Berbasis Linux,” J. Sains Inform. Terap., vol. 2, no. 1, pp. 38–44, 2023, doi: 10.62357/jsit.v2i1.184.

[2] S. Kirmizi and T. Demirdelen, “Performance Evaluation of WireGuard and IPSec Protocols in Various Network Configurations,” OKU J. Inst. Sci. Technol. 8(3) 1353-1369, 2025, vol. 8, no. 3, pp. 1353–1369, 2025.

[3] 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,” J. Inf. Syst. Informatics,

vol. 6, no. 2, pp. 949–958, Jun. 2024, doi: 10.51519/journalisi.v6i2.746.

[4] N. Hayati, Syafriadi, and Jumarniati, "Implementasi Virtual Private Network (VPN) Menggunakan Mikrotik untuk Remote Access Jaringan di SMKN 1 Luwu Timur," J. Inf. dan Teknol., vol. 1, no. 1, pp. 23–27, 2024.

[5] J. A. Donenfeld, "WireGuard: Next Generation Kernel Network Tunnel," 24th Annu. Netw. Distrib. Syst. Secur. Symp. NDSS 2017, pp. 1–20, 2021, doi: 10.14722/ndss.2017.23160.

[6] A. Master and C. Garman, "A WireGuard Exploration," CERIAS Tech. Reports, 2021, [Online]. Available: https://docs.lib.purdue.edu/ceriastr/1

[7] B. Arifwidodo, "Mekanisme Keamanan Jaringan Menggunakan Protokol Wireguard Pada Jaringan Privat," J. Informatics Commun. Technol., vol. 5, no. 2, pp. 78–86, 2023, [Online]. Available: https://ejournal.akademitelkom.ac.id/j_ict/index.php/j_ict/article/view/211

[8] D. Novianto, Y. S. Japriadi, and L. Tommy, "Implementasi Keamanan Akses Terhadap Website Menggunakan Wireguard VPN Di Routerboard Mikrotik," J. Ilm. Inform. Glob., vol. 13, no. 2, pp. 139–145, Aug. 2022, doi: 10.36982/jiig.v13i2.2308.

[9] Ubaidi and N. Puspa Dewi, "Analisis dan Implementasi VPN pada VPS untuk Peningkatan Aksesibilitas Jaringan di Lingkungan Perguruan Tinggi," J. Inf. dan Teknol., vol. 5, no. 3, pp. 131–140, 2023, doi: 10.60083/jidt.v5i3.409.

[10] R. Yulianto and F. Aprilyani, "Sistem Keamanan Jaringan Komputer Menggunakan Metode NDLC Dengan Linux Zentyal Pada Instansi KEMENKO Maritim," Tek. Inform. STMIK Antar Bangsa, vol. 6, no. 2, pp. 79–86, 2020.