SMATIKA : STIKI Informatika Jurnal
Vol. 15, No. 2, Desember 2025, pp. 292~301
ISSN: 2087-0256, e-ISSN: 2580-6939

Implementasi Wireguard Sebagai Koneksi Menggunakan Routing Mikrotik

Muhammad Ilham Ikhwandi[1*]
Azmuri Wahyu Azinar[2]
Sumarno[3]

[1,2,3]Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Muhammadiyah Sidoarjo
[1]211080200026@umsida.ac.id, [2]azmuri@umsida.ac.id, [3]sumarno@umsida.ac.id

***Penulis Korespondensi:**
Muhammad Ilham Ikhwandi
211080200026@umsida.ac.id

Abstrak

WireGuard merupakan protokol *VPN (Virtual Private Network)* yang modern, sederhana, dan cepat yang lebih mudah diterapkan dibandingkan protokol *Virtual Private Network* (*VPN*) lain seperti *Ipsec,OpenVPN* dan *WireGuard* menekankan konfigurasi yang mudah, kinerja tinggi, dan keamanan yang kuat dengan menggunakan algoritma enkripsi terbaru. penelitian ini peneliti menggunakan metode *SDLC (Sofware/System Development life cycle)* di mana metode tersebut cukup detail meliputi enam tahapan, yaitu: perencanaan (Planing), analisis (*analysis*), desain (*design*), implementasi (*implementation*), pengujian (*testing*), pemeliharaan (*maintenance*). *WireGuard VPN* memiliki kelebihan yaitu mudah dalam penerapan jaringan *VPN*. Serta, *Wireguard* yang memiliki enkripsi data yang ada pada kedua perangkat tersebut. Kemudian untuk *VPN WireGuard* terdapat sedikit celah dalam peretasan *cyber*.
Kata Kunci : Jaringan Pribadi Virtual (VPN); Perutean; WireGuard.

Abstract

WireGuard is a modern, simple, and fast VPN (Virtual Private Network) protocol that is easier to implement than other Virtual Private Network (VPN) protocols such as Ipsec, OpenVPN and WireGuard emphasizes easy configuration, high performance, and strong security using the latest encryption algorithms. In this study, researchers used the SDLC (Software/System Development life cycle) method where the method is quite detailed covering six stages, namely: planning, analysis, design, implementation, testing, maintenance. WireGuard VPN has the advantage of being easy to implement a VPN network. Also, Wireguard has data encryption on both devices. Then for WireGuard VPN there is a small gap in cyber hacking.

Keywords : Routing; Virtual Private Network (VPN); WireGuard.

1. Pendahuluan

Virtual Private Network (VPN) merupakan sebuah protokol jaringan yang digunakan untuk membuat koneksi lebih aman dan terenkripsi. Maknanya yaitu *VPN* mampu melindungi privasi dengan menyembunyikan alamat IP dan mengenkripsi data pengguna[1], [2]. Hal ini mencegah pihak ketiga, seperti penyedia layanan internet (*ISP*) atau peretas dalam memantau aktivitas *online* para pengguna. VPN juga membantu komunikasi yang memungkinkan para pengguna untuk bergabung ke dalam jaringan lokal untuk tetap terhubung ke jaringan publik[3]. Pada penggunaan *VPN* di Indonesia sangat diawasi oleh pemerintah untuk meminimalisir tindakan yang dapat merugikan negara. Menurut Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang mengatur tentang penyelenggaraan sistem dan transaksi elektronik, termasuk persyaratan keamanan dan perlindungan data. Meskipun tidak langsung membahas *VPN*, peraturan ini dapat dijadikan acuan dalam konteks penggunaan *VPN* untuk melindungi data pribadi. Penggunaan *VPN* di Indonesia diperbolehkan, tetapi harus dilakukan secara bijak dan tidak melanggar hukum. Pemerintah memiliki hak untuk melakukan pengawasan dan tindakan jika terdapat indikasi penyalahgunaan *VPN* terhadap aktivitas ilegal.

Virtual Private Network (VPN) juga membantu para penggunanya untuk mengontrol jaringan dari jarak yang jauh [4], Tetapi, masih memerlukan protokol lain yaitu Transmision *Control*

Protocol/Internet Protocol (TCP/IP) yang berfungsi sebagai pengalamatan jaringan yang nanti akan dikirim ke alamat yang lain. Adapun *Protocol Virtual Private Network (VPN)* juga dapat digunakan dalam mengakses jaringan jarak jauh yaitu seperti, *PPTP*, *Ovpn*, *L2TP*, *Ipsec* dan *WireGuard* yang sudah tersedia di perangkat salah satu brand jaringan yaitu Mikrotik.

Teknologi *Virtual Private Network* (VPN**)** telah diadopsi secara luas sebagai solusi untuk mengamankan komunikasi data melalui jaringan publik, sebagian besar penelitian dan implementasi yang ada masih berfokus pada protokol-protokol konvensional seperti PPTP**,** L2TP/IPSec**,** dan OpenVPN. Protokol-protokol ini memiliki berbagai keterbatasan, baik dari sisi performa, efisiensi enkripsi, maupun kompleksitas konfigurasi. Tantangan ini semakin relevan mengingat sejumlah sistem operasi modern, seperti Android dan iOS versi terbaru, secara resmi menghentikan dukungan terhadap protokol-protokol lama seperti PPTP dan L2TP, karena dinilai tidak mampu memenuhi standar[5].

WireGuard bekerja dengan membuat "terowongan" terenkripsi antara dua perangkat. Semua data yang dikirim melalui terowongan ini dienkripsi dan dilindungi dari penyadapan [6]. Protokol ini mendapatkan popularitas karena sifatnya yang ringan, cepat dan mudah dalam penggunaannya sehingga mudah dikonfigurasikan dibandingkan dengan protokol *VPN* tradisional seperti *Ipsec[7]*. *WireGuard* dapat digunakan untuk mengamankan koneksi antar perangkat dengan mengenkripsi paket data dan mengaktifkan rute aman antar jaringan yang berbeda. Singkatnya *WireGuard* menawarkan solusi *VPN* yang menarik bagi pengguna Mikrotik. Performa tinggi, keamanan kuat, dan kemudahan penggunaan menjadikan *WireGuard* merupakan pilihan sempurna untuk berbagai kebutuhan jaringan[8]. *Mikrotik RouterOs* mikrotik merupakan sistem operasi yang sangat fleksibel dan kuat yang banyak digunakan untuk mengelola jaringan.

WireGuard menggunakan pendekatan minimalis dalam routing , memberi setiap perangkat alamat *IP* unik di jaringan *VPN* yang digunakan untuk merutekan paket data[9]. *WireGuard* menggunakan *handshakes* cepat yang membantu menjaga stabilitas bahkan di jaringan yang tidak stabil[10]. Tidak seperti protokol *VPN* lainnya yang perlu menjaga koneksi secara terus-menerus, *WireGuard* menggunakan *handshakes* cepat yang membantu menjaga stabilitas bahkan di jaringan yang tidak stabil[11]. Salah satu kelebihan *WireGuard* adalah kemudahan dalam pengaturannya. Cukup instal aplikasi *WireGuard*, buat kunci, dan atur satu file konfigurasi sederhana.

Jaringan berskala besar yang melibatkan banyak router akan sangat sulit dikelola tanpa adanya manajemen protokol *routing* yang tepat[12]. *Routing* merupakan metode yang digunakan dalam berkomunikasi antar router dalam jaringan besar, yang sering disebut sebagai Sistem Otonom *(Autonomous System*). Tujuan utamanya adalah agar router mampu menentukan jalur terbaik untuk meneruskan paket data ke alamat tujuan[13]. Pada penelitian ini, peneliti akan mengimplementasikan protokol *VPN (WireGuard*) yang di kombinasikan dengan *Routing* statik agar bisa mengefisiensi jaringan *LAN (Local Area Network*) yang terkoneksi di jaringan publik menggunakan perangkat *Mikrotik* [14]. Adapun kendala yang dialami peneliti dalam perancangan alat penelitian ini yaitu, mahalnya harga dari setiap komponen yang diperlukan dalam perancangan alat ini, sulitnya mendapatkan *IP* Publik *V4* yang disebabkan mendekati limitnya dari pihak PT. Selanjutnya kendala lain yang dialami peneliti yaitu adanya hambatan dalam mengkoneksikan jaringan *VPN* di *android*, kendala tersebut menimbulkan keterlambatan untuk tersambung pada koneksi internet.

Adapun penelitian terdahulu yang peneliti jadikan acuan dan referensi dalam penyusunan jurnal penelitian ini, yaitu Menurut A. P. Pamungkas, Muhammad Reza Putra dan M. Hafizh telah melakukan penelitian pada tahun 2021 pada pertukaran informasi antara kantor satu dan yang lainnya, dari hasil penelitian tersebut yaitu masih diperlukannya teknologi yang mampu menjamin keamanan data yang dikirimkan[15]. *VPN* merupakan teknologi yang memungkinkan terciptanya jaringan privat dengan memanfaatkan jaringan publik, sehingga mampu membuat pertukaran data menjadi lebih aman, seperti yang diterapkan di Diskominfo Kabupaten Muko-Muko. Data yang saling

dipertukarkan oleh Diskominfo mencakup data teks untuk layanan *FTP*, *HTTP*, serta data absensi, yang merupakan data penting dan harus dijaga keamanannya. Pentingnya keamanan data dalam layanan *VoIP* yaitu untuk mencegah terjadinya kebocoran informasi sensitif, penelitian yang dilakukan Menurut I. K. Rahman dan L. N. Harnaningrum. Pada tahun 2024, sehingga diperlukan teknologi *VPN* yang mampu mencegah penyadapan[16]. Penelitian ini menguji panggilan *VoIP* pada jaringan tanpa *VPN*, dengan *VPN L2TP IPSec*, dan *WireGuard*. Selanjutnya, hasil dari penelitian ini menunjukkan bahwa *L2TP IPSec* dan WireGuard berhasil mengamankan komunikasi *VoIP* dari penyadapan. Pengujian menunjukkan rata-rata delay sebesar 19,9997 ms untuk *L2TP IPSec* dan delay yang sedikit lebih rendah, 19,9994 ms, untuk *WireGuard*. Berdasarkan uji pengembangan *VoIP* dalam berbagai skenario, disimpulkan bahwa sistem komunikasi *VoIP* tanpa pengamanan berisiko mengalami penyadapan percakapan dan intersepsi data suara melalui deteksi panggilan *VoIP* dan *RTP Player[17]*.

2. Metode Penelitian

Dalam penelitian ini peneliti menggunakan metode *SDLC (Sofware/System Development life cycle)* di mana metode tersebut cukup detail meliputi enam tahapan, yaitu: perencanaan (Planing), analisis (*analysis*), desain (*design*), implementasi (*implementation*), pengujian (*testing*), pemeliharaan (*maintenance*). Berikut penjelasan dari setiap tahapan.

a. Analisis (*analysis*)

Analisis (*analysis*) juga diperlukan karena jika *system* dengan skala besar, maka harus diukur untuk beban yang akan dilewatkan di perangkat keras agar *system* berjalan lancar dan dapat mengontrol, *upgrade* sekaligus untuk *maintenance* dan tidak harus mematikan *system* terlebih dahulu agar pengguna tidak terganggu saat menggunakan sistem. *RouterBoard*: Pastikan *Mikrotik* normal dan sudah bisa menggunakan *Router Os7. Winbox* : Untuk remote dan konfigurasi pada *RouterBoard*. *IP* Publik: Gunakan *IP* publik sebagai koneksi antara *RouterBoard* dengan ISP (*Internet Service Provider)*. Komputer: Sebagai konfigurasi pada *RouterBoard Mikrotik* melalui *software Winbox*. *OLT HSGQ 8 PON* : Sebagai *Swicth* untuk topologi jaringan *PON*

b. Rencana (*Planning*)

Perencanaan perancangan sistem pada alat dalam penelitian ini membutuhkan dua perangkat yaitu perangkat keras (*hardware*) dan perangkat lunak (*Sofware*). Setiap perangkat memiliki tipe dan versi yang harus sesuai guna menjalankan sistem yang sesuai dan tersusun baik. Berikut penjelasan setiap perangkat yang diperlukan dalam penyusunan sistem.

Tabel 1. *Daftar perangkat keras yang digunakan*

Perangkat Keras	Spesifikasi
Laptop	● *Processor* : *Intel Core* i5 Gen 4 ● Ram : 12Gb ● *Oprating Sistem* : *Windows* 10 ● Penyimpanan : SSD 256GB
Routerboard	● *Processor*: *Alpine* AL21400 1.4GHz *Quad Core* ● Ram: 1 GB ● Penyimpanan: 512MB ● Konektivitas: Ketersediaan IP *public* yang bisa digunakan sebagai koneksi di luar *local area network*

Perangkat Keras	Spesifikasi
OLT HSGQ 8 Pon	● DDR 512M ● FLASH 16M ● Vesion HSGQ-XE08ID_IR V2.0.2 REL ● Tipe perangkat Epon ● Layer 2 dan 3
Kabel *UTP*	● CAT 6

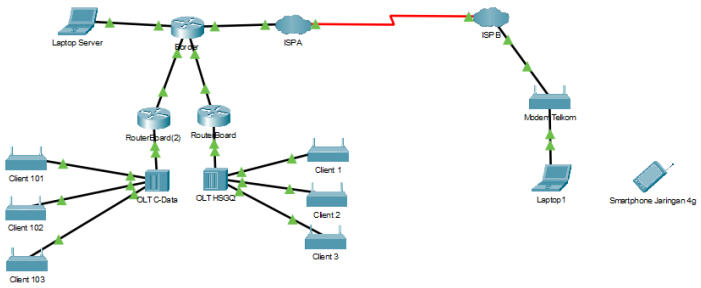
Menurut penulis, pemilihan perangkat keras dalam perancangan topologi jaringan merupakan aspek krusial yang tidak dapat diabaikan. Hal ini disebabkan oleh peran perangkat keras yang secara langsung memengaruhi stabilitas dan kinerja jaringan secara keseluruhan. Pemilihan perangkat dengan spesifikasi yang tidak sesuai dapat meningkatkan risiko terjadinya gangguan teknis seperti hang atau overload, terutama saat terjadi lonjakan trafik data[18]. Oleh karena itu, diperlukan pertimbangan yang matang dalam menyesuaikan kapasitas perangkat keras dengan kebutuhan operasional jaringan agar dapat menjamin performa yang optimal dan keberlangsungan layanan jaringan.

Tabel 2. *Daftar perangkat lunak yang digunakan*

Perangkat Lunak	Spesifikasi
Winbox	Versi: 4.0 Beta
ROS 7	*Mikrotik Router Oprating system* Versi 7
Wireguard	● Untuk *android v1.0.20231018* ● Untuk *WireGuard/0.5.3(Windows 10.0.19045; amd 64)*
Windows	*windows 10 pro 64bit(10.0,Build 19045*
Google Chrome	*Version 133.0.6943.142 (Official Build) (64-bit)*
Cisco Packet Tracer	*Version 8.2.1*
Wireshark	*Version 4.4.5*

Dalam rangka mendukung kelancaran proses penelitian ini, peneliti melakukan sejumlah persiapan perangkat lunak yang diperlukan. Persiapan tersebut mencakup pemilihan dan instalasi software yang relevan dan sesuai dengan kebutuhan teknis, guna memastikan bahwa seluruh tahapan penelitian dapat berjalan secara sistematis, efisien, dan sesuai dengan tujuan yang telah ditetapkan. Pemilihan software dilakukan berdasarkan kompatibilitas, stabilitas, serta kemampuan aplikasi dalam mendukung proses analisis dan pengujian yang akan dilakukan.

c. Desain (*Design*)



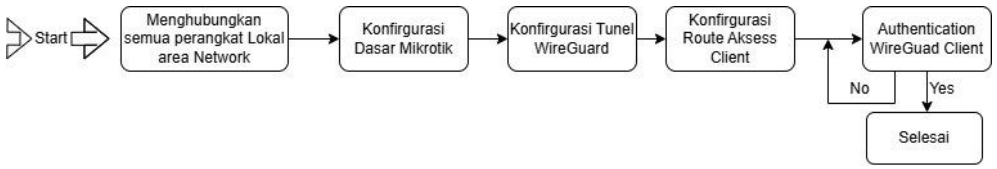
Gambar 1. *Instalasi Jaringan WireGuard Mikrotik*

Pada gambar 1, ditampilkan desain RouterBoard sebagai server. Semua perangkat dalam jaringan dihubungkan oleh RouterBoard. *RouterBoard* sebagai server kontrol, dan laptop digunakan untuk

mengkonfigurasi dan monitoring *RouterBoard*. *RouterBoard* di hubungkan menggunakan Fiber Optik yang langsung terhubung ke server *ISP* pusat yang nanti nya akan mendapatkan 1 *IP* publik dari *ISP*. Laptop dihubungkan ke *RouterBoard* melalui kabel *ethernet*, sehingga laptop dapat berkomunikasi dengan *RouterBoard* yang berfungsi sebagai server. *AccesPoint* juga di hubungkan menggunakan kabel *ethernet* sebagai server/*Klien* di bawah server utama (Border) yang akan di remote dari luar jaringan lokal.

d. Implementasi

Implementasi (*implementation*) merupakan implementasi konfigurasi *wireguard* dan *Routing* menggunakan *Mikrotik ROS* (*Router Oprating Sistem*) 7 dan menggunakan *IP* publik sebagai alat komunikasi jaringan lokal dan jaringan publik.



Gambar 2. *Penerapan konfigurasi Wireguard*

Berikut merupakan implementasi konfigurasi *WireGuard* dan *Routing* menggunakan *Mikrotik ROS* (*Router Oprating Sistem*) 7:

- Langkah pertama siapkan semua media yang di butuhkan.
- Langkah kedua konfigurasi dasar *Mikrotik* agar terhubung dengan Internet (*IP* Publik).
- Langkah ketiga konfigurasi *WireGuard* di *Mikrotik* dan membuat *user* untuk klien *WireGuard*.
- Langkah kempat konfigurasi *wireguad* klien (laptop / *handphone*) sebagai remote di jaringan publik.

Langkah kelima konfigurasikan *route* untuk memberi akses IP mana saja yang bisa diremote dari luar jaringan lokal.

e. Pengujian

Pada pengujian koneksi *WireGuard VPN*, Ada beberapa pengujian yang perlu dilakukan, diantaranya *MyIp*, Kontrol dan monitoring jaringan lokal dan *packet los* yang akan melihat perubahan alamat *IP* pada *user*. Ketiga faktor ini dapat memengaruhi seberapa bagus koneksi *VPN*[19]. Terutama pada akses jaringan lokal untuk menjaga kestabilan saat menggunakan *VPN* sebagai alat penghubung antara jaringan lokal dan jaringan publik.

Pada pengujian performa *WireGuard VPN*, tiga parameter utama yang perlu diuji adalah latensi (*delay*), *packet loss*, dan *jitter*. Ketiga faktor ini mempengaruhi kualitas koneksi *VPN*, terutama pada aplikasi *real-time* seperti *VoIP*, konferensi video, dan game[20].

Selanjutnya, setelah berhasil mengkonfigurasi WireGuard di server dan di pengguna, Langkah berikutnya adalah melakukan pengujian untuk memastikan kinerja dan optimalisasi perangkat. Beberapa aspek yang perlu diuji yaitu, Perubahan IP : Bertujuan untuk mengetahui apakah perangkat *user* sudah terkoneksi *VPN*. Remote Jaringan LAN (*Local area Network*) : pada penelitian ini digunakan sebagai alat mengontrol dan mengakses jaringan lokal dari jaringan publik. *Packet Loss*: Mengevaluasi apakah terdapat paket data yang hilang selama proses transmisi melalui *VPN*. Idealnya, tingkat kehilangan paket harus sangat rendah atau bahkan 0%.

f. Pemeliharaan

Pemeliharaan jaringan *VPN WireGuard* merupakan langkah penting untuk memastikan koneksi tetap aman, stabil, dan berkinerja optimal. Dengan pemeliharaan yang tepat, *VPN* dapat terus berfungsi

tanpa gangguan, melindungi data pengguna serta menjaga kecepatan dan kepenggunalan koneksi. Adapun tahapan yang harus diperhatikan dalam pemeliharaan ini yaitu:

a) Pemantauan kinerja dan performa, dimulai dengan pemantauan rutin terhadap konektivitas dan kinerja *VPN*. Administrator jaringan perlu memeriksa secara berkala terkait:
   - Ketersediaan layanan - Pastikan *WireGuard* tetap aktif dan dapat diakses oleh pengguna.
   - Penggunaan *Bandwidth* - Analisis lalu lintas jaringan untuk menghindari kemacetan.
   - Keamanan koneksi - Periksa log aktivitas dan deteksi potensi serangan atau akses mencurigakan.

b) Pembaruan Perangkat Lunak dan Konfigurasi, *WireGuard* merupakan protokol yang terus dikembangkan untuk meningkatkan keamanan dan efisiensi. Oleh karena itu, memperbarui perangkat lunak sangatlah penting.

c) Manajemen Pengguna dan Keamanan Akses

d) Pengujian Rutin dan Troubleshooting

3. Hasil

Pada tabel 3 menunjukkan perbedaan nilai latensi sebelum dan sesudah penggunaan VPN, terlihat pada peningkatan latensi yang relatif kecil. Kenaikan latensi ini merupakan hal yang wajar, mengingat rute lalu lintas data menjadi lebih kompleks dan memerlukan proses enkripsi serta pengiriman melalui terowongan VPN. Meskipun demikian, nilai latensi yang diperoleh masih sangat memadai untuk kebutuhan *remote access* dan pemantauan jaringan lokal dari luar jaringan utama.

Tabel 3. Hasil perbandingan

Detail	Ping To	Latensi	Packet Loss	Bandwidth
No VPN	8.8.8.8 / www.google.com	Minimum = 23ms, Maximum = 47ms, Average = 29ms	Packets: Sent = 20, Received = 20, Lost = 0 (0% loss)	Download = 9.75 Mbps Upload = 10.47 Mbps
VPN Wire Guard	8.8.8.8 / www.google.com	Minimum = 55ms, Maximum = 134ms, Average = 67ms	Packets: Sent = 20, Received = 20, Lost = 0 (0% loss),	Download= 17.28 Mbps Download = 11.58 Mbps
No VPN	192.168.100.1 / Local area Network	Packet Loss	Packets: Sent = 20, Received = 0, Lost = 20 (100% loss),	Download = 9.75 Mbps Upload= 10.47 Mbps
VPN Wire Guard	192.168.100.1 / Local area Network	Minimum = 29ms, Maximum = 84ms, Average = 39ms	Packets: Sent = 20, Received = 20, Lost = 0 (0% loss),	Download = 17.28 Mbps Upload = 11.58 Mbps

Peningkatan latensi yang cukup signifikan disebabkan oleh lokasi server MikroTik yang tidak berada di data center, melainkan melewati border ISP terlebih dahulu. Kondisi ini berdampak besar terhadap kinerja VPN karena jalur transmisi menjadi lebih panjang dan berpotensi mengalami gangguan pada tingkat jaringan ISP. Oleh karena itu, server VPN MikroTik ditempatkan di data center yang memiliki koneksi langsung dan infrastruktur jaringan yang lebih optimal, latensi yang terjadi diperkirakan akan jauh lebih rendah dan meningkatkan performa keseluruhan VPN.

4. Pembahasan

WireGuard menunjukkan keunggulan yang konsisten dalam berbagai aspek performa jaringan, terutama dalam stabilitas *jitter*, konsistensi latensi, dan efisiensi *bandwidth*. WireGuard mencatatkan nilai *jitter* rata-rata sebesar 0,1176 ms, lebih rendah dibandingkan L2TP/IPSec yang mencapai 0,1228 ms. Meskipun selisihnya relatif kecil, hal ini mencerminkan kestabilan transmisi data yang lebih baik, yang sangat krusial dalam aplikasi *real-time*.

a) Pengalamatan *IP*

Pada proses implemetasi ini, peneliti melakukan konfigurasi dasar pada *mikrotik* agar terhubung ke internet dan *IP Address* yang akan digunakan untuk pengalamatan di *VPN WireGuard*. Setiap jaringan mempunya alamat sendiri. Selanjutnya, peneliti akan mengatur jalur *route* yang berfungsi untuk mengenalkan jaringan satu ke jaringan yang lain , ada beberapa hal yang harus diperhatikan agar proses *routing* berjalan sesuai keinginan dan tidak menyebabkan eror.

b) *Peer To Windows*

Peneliti akan mengkonfigurasi *VPN WireGuard* sebagai alat komukasi antara server lokal dan publik dengan cara : Klik menu *Wireguard* >> lalu tambahkan >> Di bagian General >> Name : Tester Skripsi (Isi nama untuk *VPN*), *Type* : *WireGuard*, *Listen Port* : 13231 (*Default*) di bagian ini kita bisa rubah yang nanti nya akan di hubungkan ke perangkat lawan >> Klik *Apply* , lalu muncul *PrivateKey*, *Publickey* dan nilai *actual MTU* akan mucul otomatis , Untuk *Publickey* akan digunakan utuk *peer* yang ada di perangkat *user*.

Konfigurasi *Wireguard*

Selanjutnya, pindah ke bagian perangkat *windows 10* untuk menghubungkan ke *VPN WireGuard*. Buka aplikasi *WireaGuard* >> *Klik add Tunel* >> *add empety tunnel* >> *Copy* di bagian *publickey* di *windows* yang akan digunakan di perangkat mikrotik >> isi bagian *Peer Publickey* : (Sesuai *Publickey* di mikrotik), *AllowedIPs*: 0.0.0.0/0 untuk bisa meangakses semuanya, dibagian *End Poin* : Isikan Ip Publik beserta : *Listen Port* yang dibuat peniliti, *Persisten Keepalive*:10>> klik *save*.

c) Windows dan Peer Mikrotik to Windows

Kemudian, kembali pada perangkat mikrotik peneliti buat *peer* dari *windows* ke mikrotik. Klik *wireGuard* >> *Peers* >> Klik *add* >>Comment : Peer Komputer >> *Interface* diarahkan ke *VPN* yang dibuat dibagian *wireGuard(Tester Skripsi)* >> *Publickey* : (Isikan *PublicKey* dari perangkat *windows*) >> *allowed Address* : *IP* yang akan di gunakan perangkat *windows* sesuai yang di buat di *Address List* >> klik *Apply* dan klik Ok.

Pada tahap operasional, jaringan akan diuji dan dijalankan secara langsung mengimplementasikan konfigurasi yang telah dirancang. Penghubungan *VPN WireGuard* pengguna dengan *VPN WireGuard* server untuk memastikan koneksi jaringan dapat terjalin dengan baik. Apabila terdapat kekurangan pada sistem yang dibangun, dapat dilakukan perbaikan kinerja sistem menjadi lebih optimal. Pada tahap ini, pengujian dilakukan dengan mengaktifkan *VPN WireGuard* melalui menu "*Activate*" pada aplikasi *WireGuard*, kemudian dilakukan pengecekan apakah *VPN* sudah berhasil terhubung.

d) Activation VPN In Windows

Tahap selanjutnya yaitu *testing remote* jaringan *local* mikrotik dengan menggunakan koneksi publik pada perangkat *windows*. Setelah *Active* selanjutnya peneliti akan mencoba mengakses dari jauh salah satu modem pelanggan yang masih satu jaringan pada mikrotik

e) Sebelum tersambung ke *VPN*

Diketahui bahwa pada perangkat peneliti belum terkoneksi ke *VPN WireGuard* dengan alamat *IP* yang di dapat masih menggunakan *provider* PT.Telkom Indonesia. Selanjutnya jika perangkat *windows user* sudah tekoneksi *WireGuard VPN* yang *IP* pada perangkat sudah berubah mengikuti *provider* PT. Jinde Group yang peneliti gunakan, koneksi *IP* publik dari perusahaan tersebut digunakan untuk mendistribusikan *WireGuard VPN*. Meskipun koneksi dari perangkat masih sama menggunakan *provider* PT.Telkom Indonesia.

f) Kontrol dan akses jaringan lokal

Pada tahap ini peneliti menguji coba untuk mengakses sekaligus mengontrol jaringan *local* yang berada dibawah mikrotik yang menggunakan jaringan publik dengan *WireGuard VPN*, sebagai parameter untuk mengetahui apakah sistem jaringan yang dibuat sudah berjalan atau terjadi kendala.

g) Setelah tersambung ke *VPN*

Selanjutnya peneliti akan terus mengawasi dan mengecek kestabilan jaringan menggunakan *wireshark* dapat mengukur waktu perjalanan paket (*RTT – Round Trip Time*), sehingga kita dapat mengetahui seberapa banyak *packet los* data dikirim dan diterima melalui *VPN*.

h) *Peer to android*

Selanjutnya, proses dari *peer windows* akan melakukan *peer* pada *operating system android* dengan langkah-langkah yang sama. Selanjutnya, peneliti akan melakukan *peer* dari *android*

- Klik menu *Wireguard* >> lalu *add* >> Di bagian general >> *Name* : *Peer Android* (Isi nama untuk *VPN*), *Type* : *WireGuard*, *Listen Port* : 12345 (*Default*) di bagian ini kita bisa rubah yang akan dihubungkan ke perangkat lawan >> Klik *Apply* , lalu muncul *PrivateKey*, *Publickey* dan nilai

i) Konfiguari WireGuard to Android

- Buka aplikasi *WireGuard* >> Klik *add* >> Buat dari awal >> Antar muka>> Nama : *Peer Mikrotik* >> Kunci pribadi klik gambar arah dan kunci pribadi , kunci *public* akan terisi otomatis >> Alamat Di isikan alamat IP yang di dapat dari mikrotik >> Dns di isi 8.8.8.8. *Peer* >> kunci publik di isi *publickey* dari *mikrotik* >> *Keep presisten* 10>> *endpoin IP Public ISP* : *Listen Port* di mikrotik >> *IP* di Izinkan 0.0.0.0/0 >> klik *save*.
- Tahap selanjutnya peniliti perlu membuat *peer* baru di miikrotik untuk *peer* ke *android*. Klik *wireguard* >> *Peers* >> Klik *add* >> *Interface* diarahkan ke *VPN* yang dibuat untuk bagian *wireguard* (*Peer Android*)>> *Publickey* : (Isikan *PublicKey* dari perangkat *windows*) >> *allowed Address* : *IP* yang akan di gunakan perangkat *windows* sesuai yang di buat di *Address List* (10.10.10.12.4/24)>> klik *apply* dan Ok.
- Setelah konfigurasi dari perangkat *android* dan mikrotik dan sudah dipastikan terkoneksi dengan baik. Sehingga peneliti dapat melakukan pengujian dari koneksi *IP* yang didapat dari *provider* maupun monitoring pada perangkat yang terhubung langsung pada jaringan *local* mikrotik sebagai pusat kontrol.
- Koneksi *WireGuard VPN* sudah berhasil dan sudah bisa mengontrol jaringan *local* menggunakan *WireGuard VPN*. Selanjutnya, perangkat *android* mengunakan koneksi dari data seluler untuk mengontrol semua lokal jaringan yang di bawah mikrotik

5. Penutup

Berdasarkan hasil pengujian dan analisis yang telah dilakukan, peneliti menyimpulkan bahwa penggunaan VPN WireGuard memberikan dampak signifikan terhadap performa jaringan, khususnya dalam hal peningkatan throughput koneksi. Meskipun penggunaan WireGuard

menyebabkan peningkatan latensi rata-rata dari 29 ms menjadi 67 ms, hal ini diimbangi dengan peningkatan kecepatan unduh dan unggah secara keseluruhan. Selain itu, aplikasi WireGuard terbukti kompatibel dan berjalan stabil pada perangkat berbasis Android 13 maupun Windows 10. Implementasi mekanisme autentikasi yang terintegrasi dengan WireGuard juga menunjukkan efektivitas tinggi dalam mengakses jaringan lokal pada perangkat MikroTik. Namun demikian, perhatian terhadap konfigurasi IP Gateway sangat diperlukan, karena kesamaan alamat gateway antar perangkat dapat menimbulkan konflik koneksi yang berdampak pada terjadinya bottleneck. Dengan demikian, pemanfaatan WireGuard sebagai solusi VPN tidak hanya meningkatkan kualitas koneksi, tetapi juga menuntut perencanaan konfigurasi jaringan yang matang agar performa sistem tetap optimal.

6. Ucapan Terima Kasih

Dengan penuh rasa syukur, peneliti sampaikan terima kasih kepada semua pihak yang telah berkontribusi dalam penyusunan jurnal penelitian ini. Peneliti ucapkan terima kasih kepada Azmuri Wahyu Azinar, S.T,. M.Komp selaku dosen pembimbing yang sudah meluangkan waktunya untuk memberikan arahan dan bimbingan kepada peneliti, dukungan, dan masukan yang sangat berharga. Saya juga berterima kasih kepada Universitas Muhammadiyah Sidoarjo yang telah menyediakan fasilitas dan kesempatan untuk melakukan penelitian ini. Saya juga mengucapkan terima kasih kepada keluarga dan teman-teman yang selalu memberikan dorongan dan motivasi selama proses penyusunan jurnal penelitian ini.

7. Referensi

[1] J. A. Donenfeld and K. Milner, “Formal Verification of the WireGuard Protocol,” 2017. [Online]. Available: www.wireguard.com

[2] D. Lingga Hanayuda, “Implementasi Manajemen Bandwidth Menggunakan Mikrotik,” vol. 1, no. 1, 2022, [Online]. Available: https://jurnal.netplg.com/

[3] N. Nurdadyansyah and M. Hasibuan, “Konferensi Nasional Ilmu Komputer (KONIK) 2021 Perancangan Local Area Network Menggunakan NDLC Untuk Meningkatkan Layanan Sekolah”.

[4] L. Osswald, M. Haeberle, and M. Menth, “Performance Comparison of VPN Solutions.” [Online]. Available: https://www.wireguard.com/.

[5] V. Phang and E. Setyaningsih, “Perancangan Virtual Private Network Dengan Protokol PPTP Menggunakan MikroTik Untuk Kebutuhan Remote Access,” *Jurnal POLEKTRO: Jurnal Power Elektronik*, vol. 10, no. 2, p. 2021.

[6] D. Novianto, Y. S. Japriadi, and L. Tommy, “Implementasi Keamanan Akses Terhadap Website Menggunakan Wireguard VPN Di Routerboard Mikrotik,” *Jurnal Ilmiah Informatika Global*, vol. 13, no. 2, Aug. 2022, doi: 10.36982/jiig.v13i2.2308.

[7] J. G. A. Ginting, B. Arifwidodo, and E. Wahyudi, “Virtual Privat Network: Koneksi Keamanan Pada Aplikasi Berbasis Android,” *Journal of Telecommunication Electronics and Control Engineering (JTECE)*, vol. 7, no. 1, pp. 32–42, Jan. 2025, doi: 10.20895/jtece.v7i1.1632.

[8] B. Lipp, B. Blanchet, and K. Bhargavan, “A mechanised cryptographic proof of the WireGuard virtual private network protocol,” in *Proceedings - 4th IEEE European Symposium on Security and Privacy, EURO S and P 2019*, Institute of Electrical and Electronics Engineers Inc., Jun. 2019, pp. 231–246. doi: 10.1109/EuroSP.2019.00026.

[9] O. Kurniawan, A. Taufik, and F. Ariani, “Perancangan Routing OSPF Mikrotik pada PT. Arsen Kusuma Indonesia,” *Journal of Information System, Informatics and Computing*, vol. 8, no. 2, p. 354, Dec. 2024, doi: 10.52362/jisicom.v8i2.1682.

[10] S. Bajpai, “Wireguard Implementation on Security, Routing, Switching device,” *International Journal of Advances in Engineering and Management (IJAEM)*, vol. 5, no. 6, p. 424, 2023, doi: 10.35629/5252-0506424427.

[11] H. Jumakhan and A. Mirzaeinia, “Wireguard: An Efficient Solution for Securing IoT Device Connectivity,” Feb. 2024, [Online]. Available: http://arxiv.org/abs/2402.02093

[12] R. A. Sianturi, F. Larosa, A. Gea, and H. Artikel, "Analisis QoS Routing OSPF IP Versi 4 dan OSPF IP Versi 6 Pada Mikrotik OS," 2022. [Online]. Available: http://ojs.fikom-methodist.net/index.php/methotika

[13] Prayogi Wicaksana, F. Hadi, and Aulia Fitrul Hadi, "Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan," *Jurnal KomtekInfo*, pp. 169–175, Aug. 2021, doi: 10.35134/komtekinfo.v8i3.128.

[14] N. Novinaldi, R. Asmara, I. Ikhsan, and I. Ismael, "Pelatihan WDS (Wireless Distribution System) dan Routing Pada Router Mikrotik di SMK Negeri 1 Gunung Talang," *Jurnal Pustaka Mitra (Pusat Akses Kajian Mengabdi Terhadap Masyarakat)*, vol. 3, no. 6, pp. 263–267, Nov. 2023, doi: 10.55382/jurnalpustakamitra.v3i6.639.

[15] A. Putra, P. 1∗, M. R. Putra, and M. Hafizh, "Jurnal KomtekInfo Analisis Jaringan VPN Menggunakan PPTP dan L2TP Berbasis Mikrotik pada Diskominfo Kabupaten Muko Muko," 2021, doi: 10.37034/komtekinfo.v8i3.143.

[16] I. K. Rahman and L. N. Harnaningrum, "Analisa Quality of Service (QoS) Pada Jaringan L2TP IPSec Dan Wireguard VPN untuk mengamankan VoIP," *Jurnal RESISTOR (Rekayasa Sistem Komputer)*, vol. 7, no. 1, pp. 10–20, 2024, doi: 10.31598/jurnalresistor.v7i1.1553.

[17] D. Novianto, Y. S. Japriadi, L. Tommy, I. K. Rahman, L. N. Harnaningrum, and B. Arifwidodo, "Implementasi Keamanan Akses Terhadap Website Menggunakan Wireguard VPN Di Routerboard Mikrotik," *Jurnal Ilmiah Informatika Global*, vol. 5, no. 2, pp. 10–20, 2023, doi: 10.36982/jiig.v13i2.2308.

[18] F. Al Rasyid, I. Fitri, and A. Andrianingsih, "Augmented Reality Katalog Penjualan IT Hardware Pada PT. Unibless Menggunakan Algoritma MSER (Maximally Stable Extermal Regions)".

[19] 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.

[20] M. Lutfi Sulthon Auliyo Sulistiyono, A. Ilham Ramdhani, T. Informatika, S. Bani Saleh Bekasi, and M. Informatika, "RANCANG BANGUN JARINGAN MENGGUNAKAN ROUTING FILTER OSPF PADA MIKROTIK DENGAN METODE PPDIOO DI DATA CENTER SMK NEGERI 3 KOTA BEKASI," 2023.