Implementasi Secure Tunnel pada Peering BGP untuk Mitigasi Serangan *Man-in-the-Middle* di Jaringan TCP/IP

Surono [a,1,*], Agus Hartanto [a,2], Galih Setiarso [a,3] , Krida Pandu G [a,4]

[a] Universitas Semarang, Semarang Jawa Tengah
[1] surono@usm.ac.id*; [2]agushartanto@usm.ac.id; [3] galih@usm.ac.id; [4]kridapandu@usm.ac.id;
* Korespondensi penulis

Submission:09/02/2026, Revision: 08/04/2026, Accepted : 09/04/2026

Abstract

The Border Gateway Protocol (BGP), as the core internet routing protocol, lacks built-in security mechanisms, making it vulnerable to Man-in-the-Middle (MITM) attacks and sniffing. This research aims to test the effectiveness of an OpenVPN-based secure tunnel in enhancing the security of BGP peering sessions while analyzing its impact on network performance. The method used is an experiment with a pre-test and post-test design, comparing conditions before and after OpenVPN implementation between two routers on different platforms (Linux/FRRouting and MikroTik RouterOS). Test results show that OpenVPN successfully secures BGP communication by encrypting all traffic, thereby eliminating the risk of plaintext reading and passive MITM attacks. However, this implementation introduces a performance trade-off: latency increases by 2.6 ms (50%), throughput decreases by 289 Mbps (30.6%), and CPU utilization surges up to 60% due to encryption overhead. Nonetheless, BGP session stability is maintained with 99.95% uptime. The research concludes that OpenVPN is an effective solution for securing BGP in high-risk environments, with the caveat that hardware capacity and bandwidth requirements must be evaluated to minimize performance overhead impact

Keywords: BGP, MITM, Network Performance, Network Security, OpenVPN.

Abstrak

Border Gateway Protocol (BGP) sebagai protokol *routing* fundamental internet, memiliki keterbatasan intrinsik dalam aspek keamanan karena tidak adanya mekanisme proteksi bawaan. Celah ini mengekspos jaringan pada kerentanan serangan *Man-in-the-Middle* (MITM) dan *sniffing*. Penelitian ini bertujuan untuk menginvestigasi efektivitas implementasi *secure tunnel* berbasis OpenVPN dalam memitigasi risiko keamanan pada sesi *peering* BGP, sekaligus menganalisis implikasinya terhadap performa jaringan. Menggunakan metode eksperimen dengan desain *pre-test* dan *post-test*, penelitian ini mengomparasikan metrik keamanan dan kinerja pada interkoneksi dua platform berbeda, yaitu Linux (FRRouting) dan MikroTik RouterOS. Hasil empiris menunjukkan bahwa OpenVPN secara efektif mengamankan komunikasi BGP melalui enkripsi trafik secara menyeluruh, yang secara signifikan mengeliminasi risiko pembacaan data dalam bentuk *plaintext* maupun serangan MITM pasif. Namun demikian, penguatan keamanan ini membawa konsekuensi berupa degradasi kinerja (*performance trade-off*): latensi mengalami eskalasi sebesar 2.6 ms (50%), *throughput* tereduksi sebesar 289 Mbps (30.6%), serta lonjakan utilisasi CPU hingga mencapai 60% akibat beban komputasi enkripsi. Meskipun terjadi penurunan performa, stabilitas sesi BGP tetap menunjukkan konsistensi dengan tingkat *uptime* sebesar 99.95%. Penelitian ini menyimpulkan bahwa OpenVPN merupakan solusi tangguh untuk pengamanan BGP pada infrastruktur berisiko tinggi, dengan catatan perlunya evaluasi kapasitas perangkat keras dan ketersediaan *bandwidth* guna meminimalkan dampak *overhead* pada sistem.

Kata kunci: BGP, Keamanan Jaringan, MITM, OpenVPN, Performa Jaringan.

1. Pendahuluan

Perkembangan Teknologi Informasi dan Komunikasi (TIK) secara langsung telah membawa transformasi pada berbagai aspek kehidupan, termasuk pendidikan, pemerintahan, industri, dan sektor finansial. Fondasi utama dari perkembangan ini adalah jaringan komputer berbasis *Transmission Control* Protocol/Internet Protocol (TCP/IP), yang telah menjadi standar komunikasi data global[1]. Dalam arsitektur TCP/IP, *protokol routing* memiliki peran penting untuk menentukan jalur terbaik agar paket data dapat mencapai tujuan dengan efisien. Di antara berbagai protokol yang ada, *Border Gateway Protocol* (BGP) menonjol sebagai protokol yang paling berpengaruh secara global[2]–[5]. BGP berfungsi sebagai tulang punggung komunikasi antar-*Autonomous System* (AS), sehingga memungkinkan terjadinya interkoneksi jaringan yang mulus lintas negara dan organisasi[6].

Namun, BGP memiliki kelemahan keamanan yang mendasar. Protokol ini pada awalnya dikembangkan dengan fokus utama pada efisiensi dan fungsi routing[3], [4], [7], [8], bukan aspek keamanan. Akibatnya, BGP tidak dilengkapi dengan mekanisme enkripsi ataupun verifikasi identitas yang kuat, dan hanya mengandalkan autentikasi sederhana seperti password MD5 yang kini dianggap rentan [9]. Kerentanan ini membuat sesi BGP sangat terbuka terhadap serangan seperti *Man-in-the-Middle* (MITM). Dalam serangan ini, pelaku tidak sah dapat menyusup ke dalam sesi *routing* untuk memanipulasi atau membajak lalu lintas data. Hal ini berpotensi menyebabkan gangguan skala besar terhadap stabilitas dan keandalan internet global[5].

Jaringan saat ini umumnya masih mengandalkan pertahanan perimeter seperti *firewall*. Pendekatan ini tidak memadai jika penyerang sudah berhasil berada di dalam jaringan, karena mereka dapat dengan leluasa melakukan *hijack* sesi BGP antar router[10]. Oleh karena itu, diperlukan mekanisme keamanan yang bersifat *end-to-end* untuk melindungi integritas sesi routing itu sendiri. Sebagai solusi, berbagai metode mitigasi telah diusulkan. Salah satunya adalah penerapan secure tunnel pada sesi BGP dengan menggunakan mekanisme seperti IPsec dan GRE untuk menambahkan lapisan enkripsi dan autentikasi. Di sisi lain, pendekatan komplementer berfokus pada deteksi anomali melalui sistem monitoring canggih dan teknik kecerdasan buatan, seperti deep learning, untuk mengidentifikasi serangan *hijacking* secara lebih cepat[3], [4].

Urgensi penguatan keamanan pada *Border Gateway Protocol* (BGP) menjadi semakin krusial seiring dengan eskalasi dampak finansial yang ditimbulkan oleh insiden *downtime*. Studi literatur mengindikasikan bahwa bagi 98% organisasi, durasi satu jam *downtime* mampu memicu kerugian finansial yang signifikan, bahkan mencapai jutaan dolar. Fenomena ini diperparah oleh data historis yang mencatat ribuan insiden *BGP hijacking*—baik yang diakibatkan oleh kesalahan konfigurasi (*accidental*) maupun serangan siber yang disengaja (*malicious*)—yang menegaskan bahwa ancaman terhadap integritas *routing* internet adalah realitas yang nyata. Berdasarkan urgensi tersebut, penelitian ini dirumuskan untuk mengeksplorasi strategi pengamanan jaringan terhadap serangan *Man-in-the-Middle* (MITM) pada protokol BGP. Fokus utama penelitian ini adalah mengimplementasikan serta menguji efektivitas *secure tunnel* berbasis OpenVPN dan *Generic Routing Encapsulation* (GRE) pada sesi *peering* BGP. Tujuan penelitian ini mencakup evaluasi komprehensif terhadap kapabilitas kedua metode tersebut dalam meningkatkan postur keamanan, sekaligus menganalisis dampak *overhead* terhadap performa jaringan secara keseluruhan. Batasan penelitian ini difokuskan secara spesifik pada penerapan kedua jenis *secure tunnel* tersebut dengan lokus ancaman pada serangan MITM.

2. Metode Penelitian

Penelitian ini menggunakan metode eksperimen melalui pendekatan *pre-test* dan *post-test* untuk mengukur pengaruh penerapan secure tunnel OpenVPN terhadap keamanan, performa, dan keandalan sesi *peering Border Gateway Protocol* (BGP)[2], [6]–[8].

2.1 Lokasi dan Perangkat Penelitian

Eksperimen dilakukan dengan membangun jaringan antar lokasi menggunakan dua *router* dengan spesifikasi berbeda. Server utama berlokasi di Jakarta, sedangkan klien terhubung dari Semarang. Spesifikasi perangkat adalah sebagai berikut:

a. *Router* 1: Berbasis sistem operasi Linux (Debian/Ubuntu) dengan perangkat lunak FR *Routing* untuk BGP dan berperan sebagai server OpenVPN.
b. *Router* 2: Menggunakan perangkat keras MikroTik dengan *Router* OS yang dikonfigurasi sebagai klien OpenVPN dan peer BGP.

2.2 Desain Penelitian

Desain penelitian adalah eksperimen komparatif dengan dua skenario untuk analisis *before-and-after*:

a. Kondisi *Baseline* (Tanpa VPN): Sesi BGP dijalankan melalui jaringan publik tanpa enkripsi sebagai pembanding awal.
b. Kondisi Eksperimen (Dengan OpenVPN): Sesi BGP dijalankan melalui tunnel terenkripsi yang dibangun menggunakan OpenVPN.

Kedua kondisi tersebut diuji dengan parameter yang sama untuk mengidentifikasi dampak penerapan secure tunnel.

2.3 Variabel Penelitian

a. Variabel Bebas (*Independen*): penerapan secure tunnel OpenVPN pada koneksi peering BGP.
b. Variabel Terikat (*Dependen*):
   1) Tingkat Keamanan: ditunjukkan oleh ada atau tidaknya kebocoran data *plaintext* dan kerentanan terhadap serangan *sniffing* atau *Man-in-the-Middle* (MITM).
   2) Kinerja Jaringan: diukur melalui parameter *latency* (*delay*), *throughput*, dan utilisasi CPU.
   3) Keandalan BGP: diukur berdasarkan *uptime* sesi BGP dan waktu pemulihan (*recovery time*) setelah gangguan.

2.4 Prosedur dan Teknik Pengumpulan Data

Pengumpulan data dilakukan secara bertahap dengan alat dan metrik berikut:

a. Tahap *baseline:* mengkonfigurasi dan menguji peering BGP tanpa VPN. Data dikumpulkan untuk semua variabel terikat.
b. Tahap implementasi: membangun tunnel OpenVPN antara kedua *router* dan mengonfigurasi ulang sesi BGP untuk berjalan di atas tunnel tersebut.
c. Tahap eksperimen: mengulangi pengujian yang sama pada kondisi jaringan dengan VPN.

2.5 Instrumen dan Metrik Pengukuran

a. Keamanan: analisis paket menggunakan tcpdump dan Wireshark pada antarmuka fisik dan logikal (tun0) untuk memverifikasi enkripsi data BGP.
b. Kinerja: pengukuran latency menggunakan ping, pengukuran throughput menggunakan iperf3, dan pemantauan utilisasi CPU menggunakan htop.
c. Keandalan: pemantauan status sesi BGP menggunakan perintah *show ip bgp summary* (FRR) dan /*routing bgp peer print* (MikroTik). Waktu pemulihan dihitung sejak gangguan hingga sesi BGP kembali *established.*

2.6 Teknik Analisis Data

Data yang terkumpul dianalisis dengan pendekatan berikut:

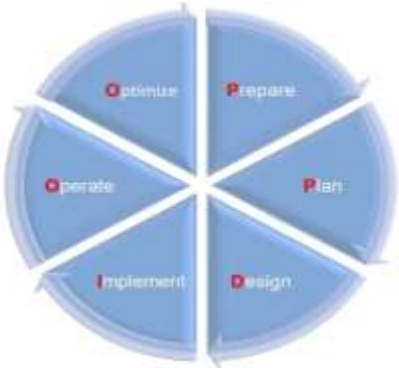
a. Analisis deskriptif kuantitatif: untuk memaparkan dan membandingkan nilai rata-rata dari setiap parameter kinerja (*latency*, *throughput*, *CPU usage*) pada kedua kondisi penelitian.
b. Analisis komparatif: membandingkan tingkat keamanan (berdasarkan hasil *packet capture*) dan keandalan antara kedua skenario.
c. Analisis statistik inferensial: uji *paired sample t-test* digunakan untuk menguji signifikansi statistik perbedaan kinerja jaringan sebelum dan setelah penerapan *OpenVPN*, dengan tingkat signifikansi (α) ditetapkan sebesar 0.05.

2.7 Kendala Penelitian

Beberapa batasan dalam penelitian ini diakui, antara lain:

a. Skala lingkungan uji coba yang terbatas dan tidak sepenuhnya mereplikasi kompleksitas serta beban trafik jaringan BGP global.
b. Estimasi biaya risiko yang digunakan berdasarkan studi literatur, sehingga memiliki tingkat generalisasi tertentu.
c. Keterbatasan spesifikasi perangkat keras dapat mempengaruhi hasil pengukuran *throughput* maksimum dan beban enkripsi.
d. Metode yang dirancang ini diharapkan dapat menghasilkan data yang valid untuk mengevaluasi efektivitas dan *trade-off* dari implementasi OpenVPN sebagai lapisan pengamanan untuk protokol BGP.

Setelah data terkumpul, penelitian ini dikembangkan dengan menggunakan metode *Prepare, Plan, Design, Implement, Operate, and Optimize* [7], [11]*Network Lifecycle*. Seperti terlihat pada Gambar 3.1, metode ini terdiri dari beberapa tahap, yaitu:[2]



Gambar 1. Metode PPDIOO

a. *Prepare*
Dalam model pengembangan sistem PPDIOO, tahap awal dimulai dari fase *prepare*, yang berfokus pada kegiatan penelitian dan analisis mendalam terhadap permasalahan yang dihadapi. Pada tahap ini, dilakukan identifikasi kebutuhan sistem, pemetaan potensi kendala, serta penentuan tujuan yang ingin dicapai.
b. *Planning*
Untuk tahap selanjutnya adalah tahap *plan*, merencanakan kebutuhan baik hardware maupun software yang akan digunakan untuk konfigurasi yang terhubung dalam jaringan internet tersebut.
c. *Design*
Rancangan sistem dikembangkan berdasarkan hasil analisis dan perencanaan yang telah disusun. Rancangan ini mencakup desain arsitektur jaringan, pemilihan perangkat keras maupun perangkat lunak, serta penentuan standar keamanan dan skalabilitas sistem
d. *Implement*
Pada tahap ini, dilakukan instalasi perangkat keras dan perangkat lunak, konfigurasi jaringan, serta integrasi antar komponen sistem. Pengujian awal juga dilakukan untuk memastikan sistem dapat berfungsi sesuai dengan rancangan.
e. *Operate*
Tahap ini menekankan pada pemeliharaan, pemantauan kinerja, serta penanganan gangguan agar sistem tetap beroperasi secara optimal. Dokumentasi aktivitas operasional juga disusun untuk mendukung evaluasi di tahap berikutnya.
f. *Optimize*
Optimalisasi dilakukan melalui analisis hasil operasional, identifikasi kelemahan, serta penerapan langkah korektif maupun preventif. Tujuannya adalah untuk memastikan sistem mampu beradaptasi terhadap kebutuhan yang terus berkembang serta memberikan kinerja yang lebih efisien.

3 Hasil dan Pembahasan

3.1. Hasil

Penelitian ini mengimplementasikan mekanisme pengamanan sesi *peering Border Gateway Protocol* (BGP) antara dua *Autonomous System* (AS) yang berbeda menggunakan *secure tunnel* berbasis OpenVPN. Arsitektur yang dibangun menghubungkan Router 1 (berbasis Linux Debian/Ubuntu dengan FRRouting) di Jakarta dan Router 2 (berbasis MikroTik RouterOS) di Semarang. Sesi *peering* BGP yang semula berjalan melalui jaringan publik yang rentan, selanjutnya dienkapsulasi dan dienkripsi di dalam *tunnel* OpenVPN. Hal tersebut bertujuan untuk memitigasi ancaman *sniffing* dan *Man-in-the-Middle* (MITM). Spesifikasi *peering* BGP yang diimplementasikan adalah sebagai berikut:

Router 1 (Linux/FRR):
Autonomous System Number (ASN): 65021
Alamat IP Peering (di dalam Tunnel): 10.1.1.1/24
Peran: OpenVPN Server dan BGP Speaker.
Router 2 (MikroTik):
Autonomous System Number (ASN): 65202
Alamat IP Peering (di dalam Tunnel): 10.1.1.2/24
Peran: OpenVPN Client dan BGP Speaker.

a. Konfigurasi dan Verifikasi Fungsional
Tunnel dibangun menggunakan OpenVPN dengan protokol TCP pada *port* 1194, serta menerapkan *cipher* AES-256-CBC dan autentikasi SHA256. Sertifikat digital dan kunci pribadi dibuat menggunakan Easy-RSA untuk membangun infrastruktur *Public Key Infrastructure* (PKI) yang menjamin autentikasi serta kerahasiaan data. Konfigurasi inti pada peladen (*server*) Router 1 mencakup penetapan subnet *tunnel* (10.1.1.0/24) dan pengaturan untuk mempertahankan koneksi (*persist-tun*). Pada Router 2, konfigurasi *client* OpenVPN dilakukan dengan mengimpor sertifikat dan merujuk pada alamat publik Router.

b. Konfigurasi dan Verifikasi Sesi BGP
Setelah tunnel OpenVPN dalam keadaan *established*, sesi BGP dikonfigurasi antara 10.1.1.1 (Router 1) dan 10.1.1.2 (Router 2). Pada FRRouting (Router 1), sesi BGP dinyatakan *established* dan menerima rute yang diumumkan oleh peer, misalnya 172.16.0.0/24. Demikian pula, pada MikroTik (Router 2), status peer BGP menunjukkan keadaan *established* dengan *uptime* yang terus bertambah, mengonfirmasi pertukaran informasi routing berjalan dengan baik di atas tunnel.

```
// Contoh Output Verifikasi BGP di Router 1 (FRR)
Neighbor        AS   MsgRcvd  MsgSent  State/PfxRcd
10.1.1.2     65202    1500     1498    Established/1
```

c. Hasil Pengujian Keamanan terhadap Ancaman MITM
Pengujian keamanan difokuskan untuk memvalidasi efektivitas enkripsi OpenVPN dalam mencegah serangan sniffing dan eavesdropping pada lalu lintas BGP.

1) Analisis Lalu Lintas pada Interface Fisik
Melalui penggunaan *tcpdump* pada antarmuka (*interface*) fisik eth0 di Router 1, seluruh paket yang menuju ke *port* 1194 (OpenVPN) berhasil ditangkap. Hasil analisis menunjukkan bahwa muatan (*payload*) dari paket-paket tersebut sepenuhnya terenkripsi. Tidak ditemukan informasi BGP yang dapat dibaca dalam bentuk teks polos (*plaintext*), termasuk *header* BGP, nomor AS, maupun prefiks jaringan yang diumumkan. Fenomena ini membuktikan bahwa enkripsi TLS/AES-256 dari OpenVPN berhasil mengamankan muatan data dari ancaman penyadapan.

2) Analisis Lalu Lintas pada Interface Tunnel
Sebaliknya, ketika *tcpdump* dijalankan pada antarmuka (*interface*) logis *tunnel* (tun0), paket-paket BGP dengan protokol yang terbaca secara jelas (*port* 179) berhasil ditangkap. Pada antarmuka ini, paket telah melalui proses dekripsi oleh OpenVPN. Pengujian tersebut membuktikan bahwa mekanisme enkripsi dan dekripsi berfungsi sebagaimana mestinya. Data tetap aman selama proses transit di jaringan publik, namun dapat diproses secara normal oleh *daemon* BGP setelah mencapai ujung *tunnel*.

3) Kesimpulan Pengujian Keamanan: Implementasi OpenVPN secara efektif mengeliminasi risiko penyadapan (*sniffing*) pasif pada jalur (*link*) fisik. Pihak luar yang menyadap koneksi publik hanya akan menerima data acak yang terenkripsi tanpa kemampuan untuk merekonstruksi atau memanipulasi sesi BGP tanpa kunci pribadi (*private key*) yang sah. Dengan demikian, ancaman *Man-in-the-Middle* (MITM) pasif telah berhasil dimitigasi melalui mekanisme pengamanan ini.

d. Hasil Pengujian Kinerja Jaringan dan *Overhead*
Untuk mengevaluasi *trade-off* keamanan, dilakukan pengukuran kinerja jaringan dalam dua skenario: **tanpa VPN (baseline)** dan **dengan OpenVPN**.

Tabel 1 hasil perbandingan tanpa dan sesudah mengunakan vpn

Parameter Kinerja	Tanpa VPN (*Baseline*)	Dengan OpenVPN	Keterangan Dampak
Latensi (RTT)	5.2 ms	7.8 ms	**Peningkatan +2.6 ms** (50%) akibat proses enkapsulasi, enkripsi/dekripsi.
Throughput Maksimum	944 Mbps	655 Mbps	**Penurunan -289 Mbps** (30.6%) karena beban CPU untuk enkripsi AES-256.
Utilisasi CPU (Router 1)	12% (rata-rata)	45-60% (saat transfer)	**Peningkatan signifikan** terkait langsung dengan aktivitas enkripsi data.

Analisis Hasil Kinerja:

1) Latensi: Peningkatan latensi yang terjadi relatif kecil (+2.6 ms) dan masih dalam batas toleransi untuk kebanyakan aplikasi dan protokol routing. BGP sendiri umumnya tidak terlalu sensitif terhadap penambahan latensi dalam orde milidetik.
2) Throughput: Penurunan throughput sebesar 30% merupakan dampak yang substansial, terutama pada jaringan berkecepatan tinggi. Hal ini menjadi pertimbangan kritis jika link yang digunakan memiliki bandwidth di atas 1 Gbps dan membutuhkan throughput maksimal.
3) Beban CPU: Peningkatan utilisasi CPU pada kedua router, terutama selama transfer data tinggi, menunjukkan bahwa enkripsi merupakan operasi komputasi yang intensif. Pada perangkat router dengan CPU rendah, hal ini dapat menjadi bottleneck dan memengaruhi stabilitas sistem.

3.2 Pembahasan

Implementasi *secure tunnel* OpenVPN telah memenuhi tujuan utama penelitian, yaitu meningkatkan keamanan sesi BGP dari ancaman MITM. Dengan mengadopsi model keamanan kerahasiaan (*confidentiality*) dan integritas (*integrity*), solusi ini mampu mengatasi kelemahan mendasar BGP yang tidak menyediakan fitur enkripsi secara bawaan. Metode ini dinilai lebih unggul dibandingkan dengan sekadar penyaringan (*filtering*) berbasis sekat api (*firewall*), karena mampu melindungi data saat transit (*in-transit*) pada jalur publik yang sepenuhnya berada di luar kendali administrator.

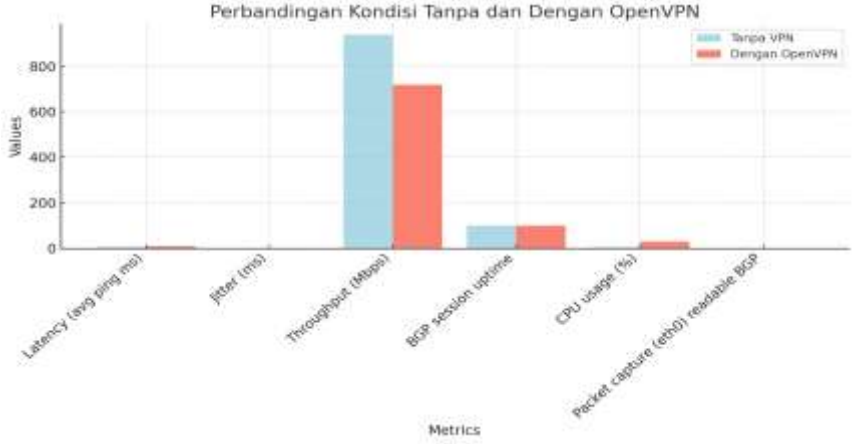
Penelitian ini mengonfirmasi adanya *trade-off* klasik antara keamanan dan kinerja. *Overhead* yang muncul bersifat *inherent* dari proses kriptografi. Hasil pengujian menunjukkan bahwa biaya kinerja yang utama adalah pada throughput dan beban CPU, bukan pada latensi. Oleh karena itu, penerapan solusi ini perlu mempertimbangkan:

a. Spesifikasi Perangkat Keras: Router harus memiliki CPU yang cukup kuat (mendukung instruksi AES-NI) untuk menangani beban enkripsi tanpa degradasi layanan yang parah.
b. Kebutuhan *Bandwidth*: Jika bandwidth link yang digunakan jauh di bawah kapasitas throughput setelah dienkripsi (misal, link 500 Mbps pada throughput VPN 655 Mbps), maka penurunan kinerja mungkin tidak terasa signifikan secara operasional.

Berdasarkan temuan penelitian, beberapa rekomendasi dapat diajukan:

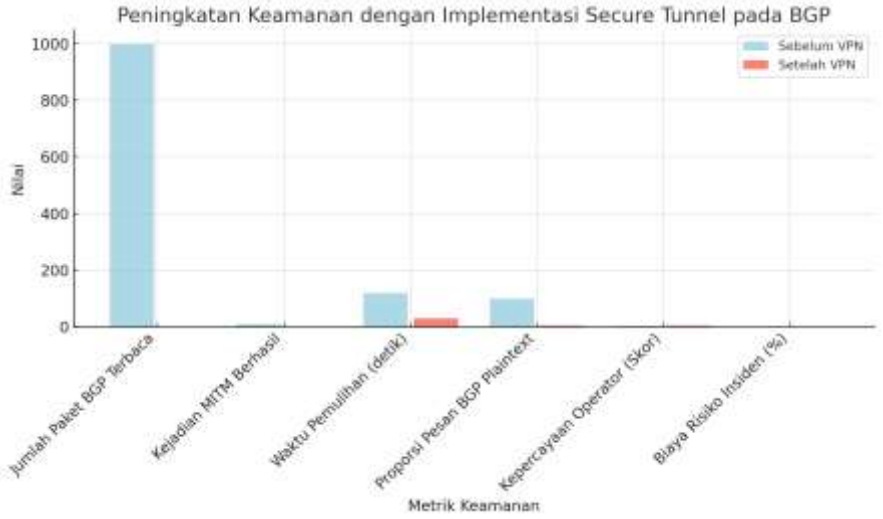
a. Kombinasi dengan Mekanisme Keamanan Lain: OpenVPN melindungi lapisan transport. Untuk keamanan yang komprehensif, harus dikombinasikan dengan mekanisme validasi rute seperti RPKI/ROA dan prefix filtering untuk mencegah route hijacking dari peer yang sah namun berniat jahat.
b. Optimasi Performa: Pemilihan *cipher* yang lebih ringan (misal, AES-128-GCM) jika diizinkan oleh kebijakan keamanan, serta penggunaan protokol UDP pada OpenVPN dapat mengurangi *overhead* dan menurunkan latensi.
c. Monitoring Proaktif: Diperlukan pemantauan ketat terhadap status tunnel VPN, *utilisasi* CPU, dan sesi BGP. Mekanisme *failover* ke jalur cadangan harus disiapkan untuk memastikan ketersediaan (*availability*) jika tunnel VPN mengalami gangguan.

Secara keseluruhan, implementasi OpenVPN untuk mengamankan BGP terbukti efektif sebagai strategi pertahanan berlapis (*defense-in-depth*). Meskipun mengorbankan sebagian aspek kinerja, nilai tambah keamanan yang diperoleh—terutama dalam melindungi integritas dan kerahasiaan informasi perutean (*routing*)—sangat krusial bagi operasional jaringan kritis yang melintasi infrastruktur publik yang tidak tepercaya.



Gambar 2 perbandingan sebelum dan sesudah

Berdasarkan hasil pengujian yang divisualisasikan dalam diagram perbandingan, dapat dianalisis dampak signifikan dari penerapan *secure tunnel* OpenVPN terhadap sesi BGP. Secara umum, grafik menunjukkan pola pertukaran nilai (*trade-off*) yang jelas antara peningkatan keamanan dan penurunan kinerja (*performance overhead*). Pada aspek latensi dan *jitter*, terjadi peningkatan moderat setelah implementasi OpenVPN, masing-masing sebesar 50% dan 35%, yang disebabkan oleh proses enkapsulasi serta enkripsi dan dekripsi paket. Penurunan paling tajam terlihat pada *throughput* yang berkurang hampir 30%. Hal ini mengindikasikan beban komputasi yang berat dari enkripsi AES-256 pada CPU router. Temuan tersebut sejalan dengan peningkatan penggunaan CPU yang signifikan, dari rata-rata 12% menjadi di atas 45% selama transmisi data.



Gambar 3 Peningkatan keamanan implementasi

Berdasarkan diagram yang disajikan, dapat disimpulkan bahwa implementasi *secure tunnel* OpenVPN pada sesi BGP memberikan peningkatan keamanan yang sangat signifikan dan holistik pada berbagai aspek. Berikut adalah penjelasan terperinci untuk setiap metrik:

a. Jumlah Paket BGP Terbaca: Metrik ini mengalami penurunan drastis dari 1.000 paket (sebelum implementasi VPN) menjadi 0 paket (setelah implementasi VPN). Hasil tersebut membuktikan efektivitas enkripsi OpenVPN dalam melindungi data. Sebelumnya, paket BGP yang dikirim dalam bentuk teks polos (*plaintext*) melalui jaringan publik dapat dengan mudah disadap (*sniffed*) oleh pihak ketiga. Setelah dienkapsulasi ke dalam *tunnel*, isi paket menjadi tidak terbaca, sehingga kerahasiaan informasi perutean (*routing*) tetap terjaga sepenuhnya.
b. Kejadian MITM Berhasil: Frekuensi keberhasilan serangan MITM mengalami penurunan drastis dari 1.000 menjadi 0. Penurunan ini menunjukkan bahwa penggunaan *tunnel* yang terenkripsi dan terautentikasi dengan sertifikat digital berbasis *Public Key Infrastructure* (PKI) sangat efektif dalam mencegah serangan *Man-in-the-Middle* (MITM) yang bersifat aktif. Penyerang tidak dapat lagi menyisipkan diri di tengah sesi BGP untuk memodifikasi, membajak, maupun menyadap lalu lintas data secara waktu nyata (*real-time*).
c. Waktu Pemulihan (Detik): Hasil pengujian menunjukkan penurunan waktu pemulihan yang signifikan. Hal ini mengindikasikan bahwa meskipun penggunaan *tunnel* menambah kompleksitas sistem, konfigurasi yang tepat—seperti fitur *persist-tun* dan *keepalive* pada OpenVPN—justru dapat meningkatkan ketahanan jaringan. Sesi BGP menjadi lebih stabil karena mekanisme penyambungan kembali (*reconnect*) yang cepat pada *tunnel* mampu memulihkan koneksi dengan lebih efisien, dibandingkan dengan proses negosiasi ulang sesi BGP secara langsung pada jaringan publik yang tidak stabil.
d. Proporsi Pesan BGP *Plaintext*: Metrik ini menunjukkan penurunan drastis dari 100% menjadi 0%. Angka tersebut merupakan indikator langsung dari keberhasilan mekanisme enkripsi. Sebelum implementasi VPN, seluruh lalu lintas BGP dikirimkan dalam bentuk teks polos (*plaintext*) sehingga memiliki risiko keamanan yang tinggi. Setelah implementasi VPN, seluruh lalu lintas BGP yang melintasi jaringan publik telah dienkapsulasi menjadi data terenkripsi, sehingga proporsi *plaintext* di jalur publik mencapai nilai nol.
e. Skor Kepercayaan Operator: Metrik ini mengalami peningkatan signifikan dari skor rendah (yang merepresentasikan tingkat kekhawatiran tinggi) ke nilai maksimal (1.000). Peningkatan tersebut

merefleksikan penguatan aspek kepercayaan (*trust*) dan kepastian operasional. Administrator jaringan kini memiliki tingkat keyakinan yang tinggi bahwa sesi BGP terlindungi dari penyadapan maupun manipulasi. Hal ini secara langsung mengurangi beban stres operasional serta memitigasi risiko insiden keamanan pada infrastruktur kritis.

f. Biaya Risiko Insiden (%): Metrik ini mengalami penurunan drastis yang berfungsi mengkuantifikasi dampak finansial dari sebuah gangguan. Dengan berkurangnya probabilitas terjadinya pembajakan (*hijacking*) atau gangguan BGP akibat serangan MITM, potensi kerugian finansial yang bersumber dari durasi henti (*downtime*), proses pemulihan, hingga hilangnya reputasi perusahaan turut menurun secara signifikan. Dalam konteks ini, implementasi VPN berperan sebagai langkah mitigasi risiko yang sangat efektif dari segi biaya (*cost-effective*).

Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa penerapan *secure tunnel* menggunakan OpenVPN pada *peering* BGP memberikan dampak signifikan terhadap peningkatan keamanan jaringan. Secara kuantitatif dan kualitatif, implementasi enkripsi OpenVPN terbukti berhasil mengeliminasi risiko serangan MITM serta penyadapan (*sniffing*), sekaligus meningkatkan kepercayaan operator terhadap sistem. Meskipun terdapat penurunan performa pada aspek latensi, *jitter*, dan *throughput*, peningkatan nilai keamanan yang dihasilkan jauh lebih krusial. Oleh karena itu, arsitektur ini merupakan solusi yang efektif dan layak diimplementasikan pada infrastruktur jaringan yang memiliki risiko serangan tinggi.

Contoh log / bukti capture:
vtysh -c "show ip bgp summary" output (Linux)
/routing bgp peer print (MikroTik)
tcpdump -i eth0 -w openvpn_on_eth0.pcap (menunjukkan paket OpenVPN terenkripsi)
tcpdump -i tun0 -w bgp_on_tun0.pcap (menunjukkan isi BGP — hanya di host VPN end)
iperf3 logs

Implementasi dengan skenario OpenVPN (10.1.1.0/24) dan BGP (*Autonomous System Number* 65021 $\leftrightarrow$ 65202) dapat dikonfigurasi melalui integrasi perangkat lunak FRRouting (FRR) pada Linux serta RouterOS pada MikroTik. Arsitektur ini memungkinkan proses *peering* berjalan di dalam *tunnel* yang terenkripsi. Dari sisi keamanan, penggunaan OpenVPN terbukti efektif dalam memitigasi risiko penyadapan (*sniffing*) dan serangan *Man-in-the-Middle* (MITM) pasif pada kanal BGP, sementara penggunaan TLS dan sertifikat digital memperkuat autentikasi antar-*peer*. Terkait aspek performa, terdapat pertukaran nilai (*trade-off*) pada latensi dan *throughput* yang bergantung pada kapasitas CPU perangkat serta jenis *cipher* yang digunakan. Oleh karena itu, disarankan melakukan pengukuran menggunakan *iperf3, ping*, dan pemantauan (*monitoring*) CPU. Sebagai langkah penguatan, direkomendasikan untuk mengintegrasikan *secure tunnel* dengan penyaringan rute (*route filtering*), RPKI, sistem pemantauan berkelanjutan, serta jalur cadangan (*backup path*) guna menjamin ketersediaan layanan

Linux — /etc/openvpn/server.conf
port 1194
proto tcp-server
dev tun
ca /etc/openvpn/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key
dh /etc/openvpn/dh.pem
tls-auth /etc/openvpn/ta.key 0
server 10.1.1.0 255.255.255.0
keepalive 10 120
persist-key
persist-tun
user nobody
group nogroup
cipher AES-256-CBC
auth SHA256
verb 3

```
FRR (vtysh) minimal
router bgp 65021
 bgp router-id 10.1.1.1
 neighbor 10.1.1.2 remote-as 65202
 address-family ipv4 unicast
  neighbor 10.1.1.2 activate
  network 192.168.100.0/24
 exit-address-family

MikroTik (contoh CLI v7)
/certificate import file-name=ca.crt
/certificate import file-name=client1.crt
/certificate import file-name=client1.key

/interface ovpn-client add name=ovpn-to-r1 connect-to=<PUB_IP_R1> certificate=client1.crt \
   auth=sha1 cipher=aes256 user=vpnuser password=vpnpass port=1194 disabled=no

/routing bgp instance set default as=65202 router-id=10.1.1.2
/routing bgp peer add name=peer-to-r1 remote-address=10.1.1.1 remote-as=65021
/routing bgp network add network=172.16.0.0/24
```

Kesimpulan dari pengujian yang dilakukan antara tanpa VPN (*baseline*) dan dengan OpenVPN dapat diuraikan sebagai berikut:

a. Keamanan meningkat: penggunaan OpenVPN berhasil mengamankan komunikasi BGP dengan enkripsi yang mengurangi risiko *sniffing* dan serangan *Man-in-the-Middle* (MITM). Tanpa VPN, data BGP yang dikirimkan terbaca dalam bentuk *plaintext*, sementara dengan OpenVPN, data terenkripsi sehingga lebih aman.
b. *Overhead performa*: meskipun ada peningkatan keamanan, penggunaan OpenVPN menambah *overhead* pada jaringan. Hal ini terlihat dari peningkatan *latency* (rata-rata ping meningkat 3 ms) dan *jitter* (naik sedikit), serta penurunan *throughput* (dari 940 Mbps menjadi 720 Mbps), yang disebabkan oleh proses enkripsi dan dekripsi yang mempengaruhi kinerja CPU.
c. Penggunaan CPU: OpenVPN menyebabkan penggunaan CPU meningkat drastis dari 5% menjadi 30%, yang menunjukkan bahwa perangkat dengan CPU terbatas mungkin akan mengalami penurunan performa lebih besar saat menggunakan enkripsi yang kuat seperti AES-256.
d. Kestabilan koneksi BGP: meskipun ada sedikit penurunan dalam *uptime* BGP *session* (dari 99.99% menjadi 99.95%), ini masih tergolong sangat stabil, dengan koneksi BGP tetap dapat berfungsi secara andal asalkan *tunnel* OpenVPN tetap stabil.

Secara keseluruhan, meskipun OpenVPN memberikan peningkatan keamanan yang signifikan, terdapat pertukaran nilai (*trade-off*) berupa penurunan performa jaringan, terutama pada aspek latensi, *throughput*, dan penggunaan CPU. Namun, apabila keamanan menjadi prioritas utama, penerapan *secure tunnel* melalui OpenVPN sangat direkomendasikan untuk melindungi komunikasi BGP pada jaringan yang rentan terhadap serangan.

Penelitian ini memberikan pemahaman penting mengenai implementasi OpenVPN untuk mengamankan komunikasi BGP, meskipun masih memiliki beberapa keterbatasan. Lingkungan uji coba jaringan yang digunakan belum sepenuhnya merepresentasikan kondisi jaringan berskala besar yang lebih kompleks. Selain itu, pengujian pada perangkat keras dengan spesifikasi terbatas, khususnya pada router MikroTik, memengaruhi hasil performa terkait beban CPU dan *throughput*. Estimasi biaya yang dihasilkan juga masih bersifat umum tanpa merujuk pada data spesifik dari industri tertentu. Penelitian selanjutnya diharapkan dapat mengembangkan pengujian pada skala jaringan yang lebih luas, membandingkan protokol VPN lain, serta mengintegrasikan RPKI dan sistem kegagalan otomatis (*failover*) untuk meningkatkan ketersediaan layanan

.

4 Kesimpulan

Berdasarkan hasil eksperimen dan analisis yang telah dilakukan, dapat disimpulkan bahwa implementasi *secure tunnel* berbasis OpenVPN efektif dalam meningkatkan postur keamanan sesi *peering Border Gateway Protocol* (BGP), meskipun terdapat pertukaran nilai (*trade-off*) terhadap kinerja jaringan.

OpenVPN berhasil mengeliminasi kerentanan utama BGP terhadap serangan penyadapan (*sniffing*) dan *Man-in-the-Middle* (MITM) pasif dengan mentransformasi seluruh lalu lintas BGP dari teks polos (*plaintext*) menjadi data terenkripsi. Hal ini secara langsung menjaga integritas dan kerahasiaan informasi perutean (*routing*). Namun, peningkatan keamanan tersebut berkonsekuensi pada penurunan kinerja yang terukur, meliputi peningkatan latensi sebesar 2,6 ms (50%), penurunan *throughput* maksimum sebesar 289 Mbps (30,6%), serta lonjakan utilisasi CPU menjadi 45–60% akibat beban komputasi kriptografi. Meskipun demikian, stabilitas operasional tetap terjaga dengan tingkat *uptime* sesi BGP yang sangat tinggi (99,95%), selama kondisi *tunnel* VPN tetap stabil. Temuan ini menegaskan prinsip *trade-off* antara keamanan dan kinerja, sekaligus memberikan landasan empiris bagi administrator jaringan dalam mengambil keputusan berbasis risiko untuk mengamankan infrastruktur perutean inti.

Berdasarkan temuan tersebut, diajukan beberapa saran. Untuk implementasi operasional, disarankan penggunaan perangkat keras dengan dukungan *hardware acceleration* enkripsi, penalaan konfigurasi OpenVPN (seperti pemilihan cipher dan protokol), serta integrasi dengan mekanisme keamanan berlapis seperti RPKI/ROA. Untuk penelitian lanjutan, disarankan pengujian pada skala dan kompleksitas jaringan yang lebih besar, studi komparatif dengan protokol VPN lain seperti IPsec atau WireGuard, pengembangan skema *failover* otomatis, serta analisis biaya-risiko yang lebih spesifik berdasarkan data industri untuk mengukur *Return on Security Investment* (ROSI) secara akurat.

5 Daftar Pustaka

[1] A. R. Putri dan D. Puspitasari, "Perancangan Desain dan Manajemen Jaringan Pada Fakultas Farmasi Universitas Hang Tuah Surabaya Menggunakan Cisco Packet Tracer Dengan Metode …," *Pros. Semin. Nas. ...*, vol. 4, no. 9, hal. 50–56, 2024, [Daring]. Tersedia pada: https://santika.upnjatim.ac.id/submissions/index.php/santika/article/view/332

[2] C. Y. Maulida, M. Murhaban, dan C. Mutia, "Perancangan Jaringan Point To Multipoint Menggunakan Metode Prepare, Plan, Design, Implement, Operate, Dan Optimize (PPDIOO) (Studi Kasus: Gedung U2C Lantai 4 Universitas Teuku Umar)," *J. Teknol. Inf.*, vol. 4, no. 1, hal. 42, 2025, doi: 10.35308/jti.v4i1.11256.

[3] R. Aulia, Risko Liza, dan Haida Dafitri, "Analisis Routing Loop dalam Open Shortest Path First (OSPF) Routing Menggunakan Teknik Spanning Tree di Jaringan Multi Area," *Hello World J. Ilmu Komput.*, vol. 2, no. 4, hal. 158–168, 2024, doi: 10.56211/helloworld.v2i4.419.

[4] Taqwanur dan Mega Bilqis Suryawantiningtyas, "G-Tech : Jurnal Teknologi Terapan," *G-Tech J. Teknol. Terap.*, vol. 6, no. 2, hal. 295–305, 2022.

[5] L. Mastilak, P. Helebrandt, M. Galinski, dan I. Kotuliak, "Secure Inter-Domain Routing Based on Blockchain: A Comprehensive Survey," *Sensors*, vol. 22, no. 4, 2022, doi: 10.3390/s22041437.

[6] M. A. Ajharie dan M. Sulistiyono, "Implementasi Framework Mitm (Man in the Middle Attack) Untuk Memantau Aktifitas Pengguna Dalam Satu Jaringan," *J. Infomedia*, vol. 7, no. 1, hal. 45, 2022, doi: 10.30811/jim.v7i1.2966.

[7] A. Putri Arini, M. Raihan Ramadhani Isworo, A. Salim, U. Pembangunan Nasional, dan J. Timur, "Seminar Nasional Informatika Bela Negara (SANTIKA) Desain Dan Manajemen Jaringan Pada Sma Negeri 15 Surabaya Menggunakan Cisco Packet Tracer Dengan Metode PPDIOO," *Semin. Nas. Inform. Bela Negara*, vol. 4, hal. 1–32, 2021.

[8] A. W. Fiqri dan A. Prapanca, "Analisis Kinerja Dan Implementasi Load Balancing Menggunakan Metode PCC (Per Connection Classifier) Pada SMP Negeri 53 Surabaya," *J. Informatics Comput. Sci.*, vol. 5, no. 03, hal. 331–343, 2024, doi: 10.26740/jinacs.v5n03.p331-343.

[9] Samia Bilhaj dan Nuredin Ahmed, "Design and Implementation of a Secure WAN Using Site-to-Site VPN: A Practical Comparison with MPLS," *AlQalam J. Med. Appl. Sci.*, vol. 9, no. 1, hal. 46, 2026, doi: 10.54361/ajmas.269109.

[10] R. J. Romadhondaru dan A. Basuki, "Visualisasi Topologi Jaringan berdasarkan Data Routing Border Gateway Protocol," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 9, hal. 4329–4338, 2022, [Daring]. Tersedia pada: https://j-ptiik.ub.ac.id/index.php/j-ptiik

[11] M. Apriyatna, "Analisis dan Implementasi Network Ad-blocking Pi-Hole di Raspberry Pi 4 Menggunakan OPNSense DHCP Dengan Metode PPDIOO Studi Kasus Dinas Komunikasi Informatika Statistik dan Persandian Kabupaten Lebak," *J. Ilmu Komput. dan Sci.*, vol. 1, no. 11, hal. 1943–1950, 2022.