*Journal of Information Technology and Computer Science (INTECOMS)*
Volume 7 Nomor 5, Tahun 2024
e-ISSN : 2614-1574
p-ISSN : 2621-3249

# OPTIMASI KEAMANAN JARINGAN VPN IPSEC TUNNEL FORTIGATE DENGAN AES

## *FORTIGATE IPSEC TUNNEL VPN NETWORK SECURITY OPTIMIZATION WITH AES*

**Gipari Pradina Abdillah[1], Danendra Satriyohadi Notonegoro[2], Hermawan Susanto[3], Dadang Iskandar Mulyana[4]**
[1,2,3,4]Sekolah Tinggi Ilmu Komputer, Cipta Karya Informatika, DKI Jakarta, Indonesia.
giparipradinaabdillah@yahoo.com[1], danendraraja80@gmail.com[2], wanzdhy@gmail.com[3], mahvin2012@gmail.com[4]

***ABSTRACT***

*VPN is a communication technology that uses a private network that can be connected to a public network. In this way, the same permissions and settings as if they were on a local network use a public network. This research uses AES encryption in IKEv2 IPSec Tunnel. AES (Advanced Encryption Standard) is an encryption algorithm commonly used in IPSec (Internet Protocol Security) to protect data transmission in tunnels. Therefore, to add the AES encryption layer, IPSec and IKEv2 encryption protocols are used. That's why this implementation in Fortigate allows users to create a secure optimization path between two different networks. All traffic passing through the optimization path is encrypted using IPSec. This implementation shows a high level of security. AES encryption, which is a strong security standard, works effectively in protecting communications over IPSec tunnels.*

***Keywords****: IPSec, VPN, Tunnel, AES, IKEv2, Fortigate.*

***ABSTRAK***

VPN merupakan teknologi komunikasi yang menggunakan jaringan pribadi yang dapat dihubungkan ke jaringan publik. Dengan cara ini maka izin dan pengaturan yang sama seolah-olah berada di jaringan lokal yang menggunakan jaringan publik. Penelitian ini menggunakan enkripsi AES pada IKEv2 IPSec Tunnel. AES (Advanced Encryption Standard) merupakan algoritma enkripsi yang biasa digunakan di IPSec (Internet Protocol Security) untuk melindungi transmisi data di terowongan. Oleh karena itu, untuk menambahkan lapisan enkripsi AES, digunakan protokol enkripsi IPSec dan IKEv2. Itu sebabnya penerapan di Fortigate ini memungkinkan pengguna membuat jalur pengoptimalan yang aman antara dua jaringan berbeda. Semua lalu lintas yang melewati jalur optimasi dienkripsi menggunakan AES. Implementasi ini menunjukkan tingkat keamanan yang tinggi. Enkripsi AES, yang merupakan standar keamanan yang kuat, berfungsi secara efektif dalam melindungi komunikasi melalui tunnel IPSec.

**Kata Kunci**: IPSec, VPN, Terowongan, AES, IKEv2, Fortigate.

## PENDAHULUAN

Dalam era di mana pertukaran informasi sangat penting dan kerahasiaan data menjadi prioritas utama, pengamanan komunikasi melalui jaringan menjadi suatu keharusan. Keamanan informasi dapat dijamin dengan menggunakan protokol keamanan yang handal. Salah satu protokol yang umum digunakan untuk mengamankan komunikasi jaringan adalah IPsec (Internet Protocol Security). IPsec menyediakan layanan keamanan pada tingkat lapisan jaringan, memungkinkan pengamanan end-to-end melalui enkripsi dan otentikasi. Dalam konteks implementasi IPsec, Advanced Encryption Standard (AES) menjadi pilihan utama untuk menyediakan enkripsi yang kuat dan efisien. AES telah diakui secara luas sebagai algoritma enkripsi yang aman dan dapat diandalkan dalam melindungi data sensitif. Pada jurnal ini, kami akan mengeksplorasi implementasi AES pada IPsec tunnel menggunakan perangkat Fortigate.

Fortigate, sebagai perangkat firewall dan keamanan jaringan yang terkemuka, menyediakan kemampuan integrasi IPsec untuk meningkatkan keamanan lalu lintas data melalui jaringan. Implementasi AES

pada IPsec tunnel Fortigate menjadi topik krusial untuk dipelajari, karena memberikan solusi yang kokoh dalam mengamankan komunikasi data.

Dalam jurnal ini, kami akan membahas langkah-langkah implementasi AES pada Fortigate, termasuk konfigurasi yang diperlukan, keuntungan dari penggunaan AES dalam konteks IPsec, dan evaluasi kinerja. Penelitian ini bertujuan untuk memberikan pemahaman yang mendalam tentang cara memanfaatkan keamanan yang diberikan oleh kombinasi AES dan IPsec pada perangkat Fortigate.

Melalui analisis implementasi ini, diharapkan dapat diidentifikasi potensi risiko keamanan yang mungkin muncul, serta memberikan rekomendasi untuk meningkatkan keamanan dan efisiensi dalam mengimplementasikan AES pada IPsec tunnel Fortigate. Kesimpulan dari penelitian ini diharapkan dapat memberikan panduan yang berharga bagi para profesional keamanan jaringan dan peneliti yang tertarik dalam meningkatkan keamanan komunikasi melalui jaringan menggunakan teknologi terkini.

[1] Virtual Private Network

VPN pada Fortigate merupakan suatu solusi keamanan jaringan yang memanfaatkan teknologi Virtual Private Network (VPN) untuk menyediakan saluran aman dan terenkripsi untuk komunikasi data melalui jaringan publik atau internet. Fortigate adalah perangkat firewall dan keamanan jaringan yang sering digunakan untuk mengimplementasikan solusi VPN yang kuat.

[2] Internet Protocol Security

IPsec Tunnel merupakan saluran aman yang dibuat melalui implementasi protokol keamanan IPsec (Internet Protocol Security). IPsec Tunnel digunakan untuk melindungi dan mengamankan lalu lintas data yang dikirimkan antara dua titik (atau lebih) dalam suatu jaringan, biasanya melalui internet atau jaringan publik lainnya. Tujuan utama dari IPSec Tunnel adalah untuk menyediakan enkripsi, otentikasi, dan integritas data, sehingga informasi yang dikirimkan melalui tunnel tersebut tetap aman dari ancaman keamanan.

[3] Advanced Encryption Standard

AES pada IPsec (Internet Protocol Security) merujuk pada penggunaan Advanced Encryption Standard (AES) sebagai algoritma enkripsi dalam implementasi IPsec untuk mengamankan komunikasi data melalui jaringan. IPsec menyediakan kerangka kerja keamanan di tingkat lapisan jaringan, dan AES dipilih sebagai salah satu algoritma kriptografi yang paling umum digunakan dalam konteks ini.

Penggunaan AES pada IPsec memberikan tingkat keamanan yang tinggi dan efisien, dan kombinasi ini sering digunakan dalam berbagai skenario, termasuk Site-to-Site VPN, Remote Access VPN, dan proteksi lalu lintas data yang sensitif melalui jaringan yang tidak terpercaya.

[4] Internet Key Exchange version 2

IKEv2, singkatan dari Internet Key Exchange version 2, merupakan sebuah protokol yang digunakan untuk mengatur pembentukan kunci keamanan dalam jaringan komputer. Protokol ini termasuk dalam keluarga protokol Internet Security Association and Key Management Protocol (ISAKMP) dan sering digunakan dalam implementasi Virtual Private Network (VPN).

IKEv2 bertanggung jawab untuk menegosiasikan, mendukung, dan memperbarui parameter keamanan antara dua entitas (biasanya antara klien dan server VPN). Proses ini melibatkan pertukaran kunci, penyelesaian keamanan, dan pembentukan asosiasi keamanan. IKEv2 memiliki beberapa keunggulan, termasuk kemampuan untuk merespons perubahan IP, mendukung mobilitas, dan

memiliki prosedur penanganan kesalahan yang lebih baik.

[5] Fortigate Firewall

FortiGate Firewall adalah solusi keamanan jaringan terkemuka yang diproduksi oleh Fortinet, sebuah perusahaan yang dikenal dalam industri keamanan informasi. FortiGate berperan sebagai firewall andal yang melindungi jaringan dari berbagai ancaman yang dapat merugikan. Dengan kemampuannya untuk menyaring dan mengontrol lalu lintas jaringan, FortiGate memastikan bahwa hanya lalu lintas yang sah dan diotorisasi yang diizinkan untuk melewati, memberikan lapisan pertahanan yang efektif terhadap serangan dari luar.

Selain fungsi dasar sebagai firewall, FortiGate juga menyediakan fitur-fitur keamanan tambahan yang signifikan. Ini termasuk kemampuan untuk membuat saluran VPN yang aman, memungkinkan komunikasi terenkripsi antara lokasi atau pengguna yang berbeda. FortiGate juga dilengkapi dengan sistem pencegahan intrusi (IPS) yang canggih, mendeteksi dan merespons secara otomatis terhadap ancaman jaringan potensial.

FortiGate Firewall tidak hanya menyediakan perlindungan terhadap serangan dari luar, tetapi juga membantu dalam memerangi ancaman internal seperti malware dan virus. Dengan fitur antivirus dan antimalware yang kuat, perangkat ini secara proaktif melacak dan menghapus ancaman keamanan yang mungkin muncul di jaringan.

Selain itu, kemampuan FortiGate untuk mengelola lalu lintas web, mengontrol aplikasi, dan membentuk lalu lintas jaringan memberikan administrator kontrol penuh terhadap lingkungan jaringan. Hal ini memungkinkan implementasi kebijakan keamanan yang ketat dan efisien.

Dengan fitur-fitur andal seperti logging dan monitoring, FortiGate memfasilitasi tindak lanjut dan analisis yang efektif terhadap aktivitas jaringan. Keseluruhan, FortiGate Firewall merupakan solusi komprehensif yang menyatukan keamanan, manajemen, dan kinerja dalam satu platform yang andal.

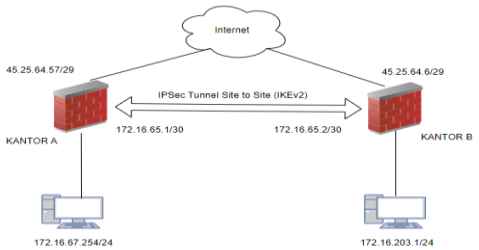
## METODE

Desain Penelitian :

Penelitian ini menggunakan pendekatan eksperimental untuk implementasi Enkripsi AES pada IKEv2 IPSec Tunnel Fortigate

Perancangan :

Perancangan metode penelitian dilakukan dengan langkah-langkah sebagai berikut. Observasi dilakukan untuk memperoleh data, yang dicari dengan referensi dan studi literatur berupa buku, jurnal, penelitian, karya ilmiah, artikel tentang perangkat Fortigate yang digunakan, seperti Internet Protocol Security (IPSec) dan Advanced Encryption Standard (AES), Internet Key Exchange version 2.

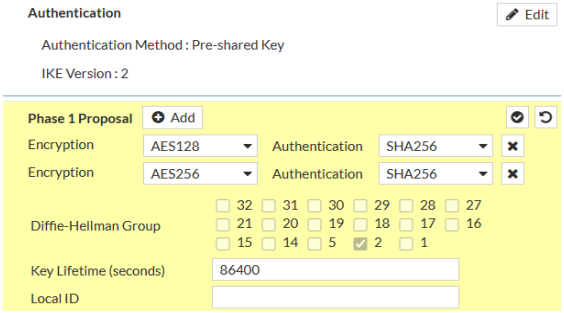



**Gambar 1. Topologi Network IPSec tunnel**

Rancangan topologi pada Gambar 1 menjelaskan terdapat 2 Fortigate 101E terhubung ke jaringan

publik (internet), PC Kantor A dan PC Kantor B terhubung ke perangkat Fortigate sebagai jaringan LAN. Kemudian di Fortigate 101E Kantor A dan Fortigate 101E Kantor B yang membentuk suatu Tunnel IPSec VPN site to site dengan enkripsi AES di IKEv2 dan memiliki network tunnel yaitu 172.16.65.1/30. PC A melakukan ping dan telnet ke PC B. Kemudian pada Fortigate 101E A akan dilakukan capture packet yang melintas melalui tunnel dengan menggunakan fitur yang tersedia dari Fortigate.

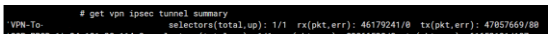
Implementasi :
Implementasi enkripsi pada Fortigate 101E A dan Fortigate 101E B menggunakan enkripsi AES128 dan AES256 dengan autentikasi SHA256.




**Gambar 2. Enkripsi AES pada IKEv2 IPSec tunnel**

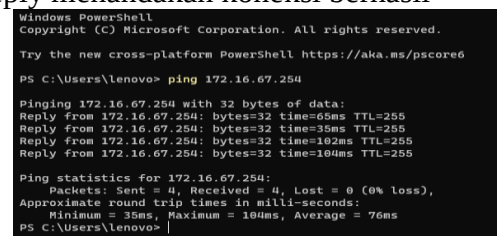
## HASIL DAN PEMBAHASAN

Tahap Pengujian IPSec VPN
Gambar 3 menampilkan verifikasi VPN Tunnel sudah berjalan dengan status "UP". Menggunakan command "get vpn ipsec tunnel summary" untuk menampilkan status interface VPN



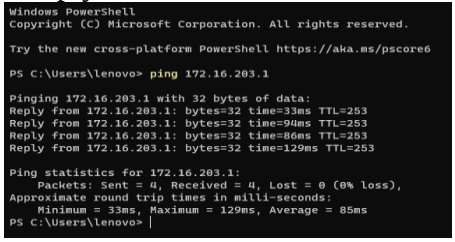

**Gambar 3. Status IPSec tunnel**

Tahap Pengujian Koneksi antara PC
Gambar 4 menunjukan hasil test koneksi dengan protokol ping (ICMP) dari PC kantor A ke PC Kantor B dengan status reply menandakan koneksi berhasil



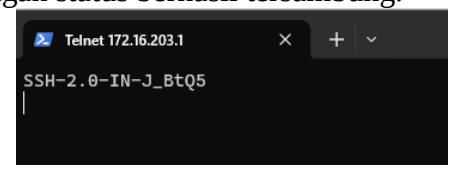

**Gambar 4. Tes koneksi ping dari PC Kantor A ke PC Kantor B**

Sebaliknya Gambar 5 menunjukan hasil test koneksi dengan protokol ping (ICMP) dari PC kantor B ke PC Kantor A dengan status reply menandakan koneksi berhasil




**Gambar 5. Tes koneksi ping dari PC Kantor B ke PC kantor A**

Sedangkan Gambar 6 menunjukan hasil test dari PC kantor A ke PC kantor B dengan menggunakan telnet port 22 dengan status berhasil tersambung.

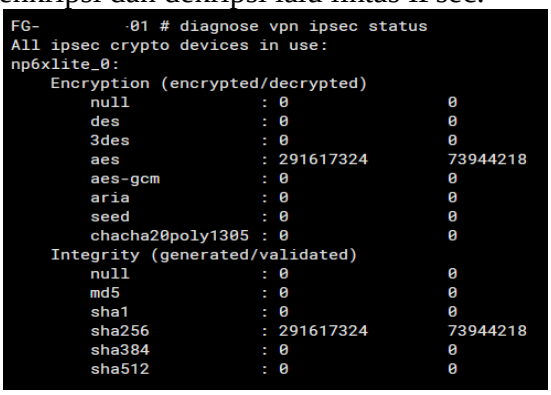



**Gambar 6. Tes telnet dari PC Kantor A ke PC Kantor B**

Tahap Pengujian Enkripsi AES pada IKEv2 IPSec tunnel

Gambar 4 menampilkan hasil output dari perintah diagnose vpn ipsec status pada perangkat FortiGate. Perintah ini digunakan untuk menampilkan status semua perangkat kriptografi IPsec yang digunakan oleh perangkat.

np6xlite_0: Perangkat ini menggunakan algoritma enkripsi AES-256 dan integritas SHA-256 dan jumlah paket yang telah dienkripsi dan didekripsi oleh perangkat np6xlite_0 adalah 291.617.324 dan 73.944.218, masing-masing. Hal ini menunjukkan bahwa perangkat ini sedang digunakan untuk melakukan enkripsi dan dekripsi lalu lintas IPsec.




**Gambar 4. Hasil output Enkripsi AES pada IPSec tunnel**

## SIMPULAN

Berdasarkan hasil pengujian enkripsi AES pada IKEv2 IPsec tunnel di Fortigate, dapat disimpulkan bahwa implementasi ini menunjukkan tingkat keamanan yang tinggi. Enkripsi AES, yang merupakan standar keamanan yang kuat, berfungsi

secara efektif dalam melindungi komunikasi melalui tunnel IPSec. Pengujian juga menunjukkan bahwa kinerja sistem tetap memadai meskipun menggunakan enkripsi AES, menandakan kemampuan Fortigate untuk menjaga throughput dan latensi dalam batas yang dapat diterima. Kompatibilitas dengan standar industri, seperti IKEv2 dan IPSec, terlihat terpenuhi, menunjukkan bahwa solusi ini dapat berintegrasi dengan baik dengan perangkat lunak dan perangkat keras lain yang mendukung standar yang sama. Meskipun hasilnya positif, rekomendasi untuk pemeliharaan rutin dan pembaruan konfigurasi dapat memberikan tambahan lapisan keamanan atau kinerja yang optimal. Secara keseluruhan, implementasi enkripsi AES pada IKEv2 IPsec tunnel di Fortigate dapat dianggap sebagai solusi yang efektif dan andal dalam mendukung keamanan komunikasi jaringan

## DAFTAR PUSTAKA

[1] Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.

[2] Dang, Q., & Chen, C. (2003). IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks. Prentice Hall PTR.

[3] Ferguson, P., & Schneier, B. (2003). Practical Cryptography. Wiley.

[4] Fortinet. (2022). Fortigate Security Fabric. Retrieved from https://www.fortinet.com/products/next-generation-firewall/security-fabric

[5] National Institute of Standards and Technology. (2001). FIPS PUB 197: Advanced Encryption Standard (AES). Retrieved from

[6] Ikhwanul Kurnia Rahman; Dadang Iskandar Mulyana; Yuma Akbar, (2023) “Optimasi IPSec Site to Site VPN Mikrotik menggunakan Algoritme Enkripsi Blowfish”