BAB I PENDAHULUAN

I.1 Latar Belakang

Dalam era transformasi digital yang semakin pesat, keamanan jaringan menjadi salah satu elemen kritis yang harus diperhatikan oleh organisasi. Semakin banyak munculnya pekerja jarak jauh dan adopsi teknologi berbasis *cloud*. Hal ini mendorong peningkatan perangkat terminal dan pertukaran data, yang memberikan kemudahan tetapi juga memunculkan ancaman internal dalam jaringan. Misalnya, Tim FireEye melaporkan bahwa ancaman internal meningkat dari 6% pada 2011 menjadi 53% pada 2021, sehingga diperlukan pertahanan yang lebih kuat terhadap ancaman internal (Kang et al., 2023).

Model keamanan tradisional, yang didasarkan pada perimeter jaringan, memiliki keterbatasan dalam menghadapi ancaman modern. Dalam konteks ini, pendekatan ZTNA muncul sebagai solusi yang menitikberatkan pada prinsip "*never trust, always verify*". ZTNA memberikan akses berdasarkan verifikasi ketat, tanpa memandang lokasi fisik pengguna atau perangkat, sehingga menghilangkan kepercayaan *default* yang rentan terhadap eksploitasi. Selain itu, protokol keamanan seperti WireGuard juga mendapatkan perhatian karena efisiensinya dalam menyediakan koneksi VPN yang aman dan sederhana.

Penelitian ini berfokus pada implementasi dan *profiling* fungsi kontrol keamanan dan *performance* pada dua platform, yaitu FerrumGate (ZTNA) dan WireGuard (VPN). FerrumGate, sebagai solusi ZTNA, menawarkan kemampuan kontrol akses granular dan segmentasi mikro yang memastikan bahwa hanya pengguna atau perangkat yang telah diverifikasi yang dapat mengakses sumber daya tertentu. Sementara itu, WireGuard menyediakan enkripsi kuat dan performa tinggi untuk komunikasi yang aman.

Untuk mendukung penelitian ini, eksperimen dilakukan menggunakan simulasi serangan berbasis jaringan, yang mencakup teknik seperti *Brute Force Attack* dan *Port Scanning,* serta dilakukan pengukuran metrik *performance*. Hasil eksperimen akan digunakan untuk mengevaluasi efektivitas fungsi kontrol yang diterapkan pada kedua platform ini. Dengan demikian, penelitian ini diharapkan

dapat memberikan kontribusi dalam memahami perbandingan performa kedua teknologi dalam meningkatkan keamanan jaringan modern.

I.2 Perumusan Masalah

Berdasarkan uraian masalah yang telah dijelaskan pada latar belakang, permasalahan yang akan dikaji adalah sebagai berikut:

a. Bagaimana mekanisme kerja fungsi keamanan pada ZTNA dan VPN?
b. Bagaimana perbandingan efektivitas fungsi kontrol keamanan ZTNA dan VPN dalam mendeteksi dan menangani serangan pada jaringan?
c. Bagaimana perbandingan *performance* jaringan antara ZTNA dan VPN?

I.3 Tujuan Penelitian

Berdasarkan perumusan masalah yang telah disampaikan, tujuan penelitian ini adalah sebagai berikut:

a. Mengidentifikasi penerapan fungsi kontrol (IAAA) pada FerrumGate (ZTNA) dan WireGuard (VPN).
b. Melakukan *profiling* metrik kontrol keamanan pada kedua FerrumGate (ZTNA) dan WireGuard (VPN) dalam mendeteksi dan menangani ancaman siber melalui pengelolaan fungsi kontrol.
c. Melakukan analisis perbandingan *performance* jaringan FerrumGate (ZTNA) dan WireGuard (VPN).

I.4 Batasan Penelitian

Adapun batasan dalam penelitian ini adalah sebagai berikut:

a. Penelitian fokus pada fungsi kontrol dan *performance* dalam bentuk simulasi dan eksperimen.
b. Simulasi serangan terbatas pada kategori *Brute Force* dan *Port Scanning*, dan simulasi dengan kategori *performance* dengan masing-masing skenario diujikan secara terpisah.
c. Penelitian ini dilakukan menggunakan pendekatan eksperimen berbasis sistem *blackbox testing*, hanya menguji fungsionalitas fitur tanpa mengeksplorasi arsitektur perangkat lunak maupun arsitektur sistem.

I.5 Manfaat Penelitian

1. Secara Teoritis:
    a. Menambah wawasan tentang implementasi terkait fungsi kontrol utama, dan *performance* pada FerrumGate (ZTNA) dan WireGuard (VPN).
    b. Memberikan pemahaman tentang metrik penting dan *performance* untuk mengevaluasi efektivitas fungsi kontrol dan performa WireGuard (VPN) dan FerrumGate (ZTNA).
2. Secara Praktis:
    a. Meningkatkan pemahaman teknis mengenai implementasi, konfigurasi, dan pengoperasian platform WireGuard dan FerrumGate.
    b. Memberikan pengetahuan teknis yang dapat digunakan untuk membantu pengelolaan keamanan akses menggunakan ZTNA dan VPN.