1. Pendahuluan

Latar Belakang

Keamanan jaringan merupakan salah satu aspek penting dalam teknologi, baik dalam industry bisnis, Pendidikan, dan beberapa aspek serupa lainnya. Keamanan jaringan berperan utama dalam mencegah serta mengatasi terjadinya serangan yang dilakukan oleh *attacker.* Pada lingkungan kampus terutama pada Fakultas Teknologi Informasi dan Bisnis (FTIB) yang terdapat banyak mahasiswa dan mahasiswi yang memiliki keberagaman pengetahuan tentunya merupakan salah satu faktor dapat terjadinya suatu serangan yang ditujukan pada server. Keberadaan server FTIB yang masih baru telah digunakan oleh sebagian mahasiswa dan mahasiswi untuk penelitian sehingga ketersediaan Server FTIB sangatlah penting. Dengan penggunaanya yang masih minim dalam satu tahun belakangan tentunya keamanan jaringan masih belum ada dan diterapkan pada lalu lintas server FTIB.

Berdasarkan sumber dari Badan Siber dan Sandi Negara yang dituangkan dalam sebuah dokumen yaitu lanskap keamanan siber Indonesia tahun 2023[1]. Dalam dokumen tersebut diprediksi adanya beberapa serangan siber salah satunya adalah serangan *Denial of Service* (DoS) atau *Distributed Denial of Service* (DDoS). Dengan adanya serangan tersebut tentunya akan sangat berpengaruh terhadap performa pada server FTIB.

Sebuah sistem *Network Access Control* berfungsi dalam memberikan akses control menuju server dan memberikan aturan/*policy* terkait pengguna sebagai bentuk preventif akan adanya suatu serangan menuju server. Penerapan sistem NAC beserta *firewall* dan IDS pada lalu lintas menuju server FTIB dapat mengecilkan kemungkinan serangan menuju server FTIB secara langsung.

Topik dan Batasannya

Pada penelitian ini masalah yang didapati adalah bagaimana memberikan keamanan pada lalu lintas serta keoptimalan *resource* pada server FTIB dengan pengujian berupa serangan DDoS. Dalam penerapan sistem NAC beserta *firewall* dan IDS apakah telah sesuai dengan kebutuhan dalam meningkatkan keamanan pada lalu lintas server FTIB.

Batasan dalam penelitian ini adalah sebagai berikut :

1. Implementasi sistem *Network Access Control* (NAC) dengan platform yang digunakan ialah FortiGate.
2. Implementasi dan uji coba dilakukan secara simulasi berdasarkan topologi nyata pada FTIB.
3. Sistem hanya dapat mendeteksi perangkat yang terhubung.

Tujuan

Pada penelitian ini memiliki tujuan sebagai upaya preventif dalam mengatasi serangan dengan mengidentifikasi pengaruh server terhadap serangan yang terjadi setelah diterapkannya sistem NAC dan pengujian terhadap aturan/*policy* yang diterapkan berdasarkan jaringan yang digunakan. Evaluasi teliti dilakukan dengan membandingkan pengaruh digunakannya sistem NAC dan tidak digunakannya sistem NAC pada lalu lintas server. Parameter yang digunakan untuk mendapatkan hasil evaluasi tersebut adalah jumlah serangan terkirim, jumlah serangan terdeteksi, dan *resource* server berupa kinerja CPU.

Tabel 1. Keterkaitan antara tujuan, pengujian dan kesimpulan

No	Tujuan	Pengujian	Kesimpulan
1	Pengujian NAC	Pengguna dalam mengakses jaringan yang ada pada topologi server FTIB.	Keberhasilan penerapan NAC.
2	Pengujian IDS	Total serangan yang terkirim, total serangan yang terdeteksi serta status CPU.	Keberhasilan dalam meminimalisir serangan.
3	Pengujian *Firewall*	Pengguna mengakses protokol pada port tertentu.	Keberhasilan dalam penerapan *rules.*

Organisasi Tulisan

Pada penelitian ini akan menjelaskan tentang studi terkait terhadap penelitian yang berkaitan dengan topik tugas akhir yang dipilih. Sistem yang dibangun berupa simulasi berdasarkan topologi nyata yang berada pada server FTIB. Evaluasi berisi mengenai hasil dari analisis pengujian berdasarkan sistem yang dibangun. Kesimpulan akan menjelaskan rangkuman secara garis besar pengujian pada penelitian ini.