BAB I PENDAHULUAN

I.1 Latar Belakang

Keamanan suatu jaringan komputer merupakan salah satu bagian sistem yang harus dilindungi untuk mengamankan data-data yang ada dan menghindari ancaman informasi pada server komputer. Keamanan informasi merupakan cara untuk melindungi informasi dari segala kemungkinan ancaman yang terjadi dan mendeteksi adanya suatu pencurian data atau informasi, seperti penyerangan *Denial of Service* (DOS). Jika perangkat komputer terkena serangan tersebut akan mengakibatkan *server down* dan bisa juga secara otomatis *server* tidak dapat beroperasi lagi. Dari berbagai serangan yang dialami sebuah server, dapat dilakukan tindakan pencegahan dengan melakukan identifikasi celah keamanan yang maksimal pada perangkat komputer, salah satunya dengan menggunakan *firewall.*

Firewall merupakan suatu sistem yang dapat menerapkan *access control policy* pada lalu lintas jaringan, yang dapat membantu melindungi dariserangan lalu lintas jaringan dan serangan lainnya serta dapat memfilter lalu lintas jaringan yang masuk pada jaringan. Implementasi *firewall* sangat penting diterapkan pada perangkat komputer untuk menghindari dari pencurian data-data yang ada di dalam perangkat yang sifatnya rahasia.

Implementasi *firewall* penting untuk diterapkan pada jaringan untuk menjaga dari ancaman serangan. Dasar kinerja yang dimiliki *firewall,* yaitu dapat mendeteksi *traffic* jaringan yang sah. Sehingga dapat diberikan akses ke dalam sistem dengan melewati *firewall* untuk dibatasi. Pembatasan akses yang masuk ke dalam jaringan lokal, kemudian melakukan pencegahan jaringan yang tidak terdaftar pada sistem. Pembatasan dilakukan dengan diaturnya *rules* atau *policy* pada konfigurasi *firewall*. Salah satu jenis *firewall* yang sering dibicarakan adalah *Next Generation Firewall* (NGFW). *Next Generation Firewall* merupakan *firewall* yang memiliki kemampuan dalam mendeteksi dan memblokir suatu serangan yang berbahaya. Kemampuan NGFW dengan memberikan proteksi dan perlindungan yang tinggi, serta dapat menerapkan keamanan yang terdapat pada tingkat *protocol, port*, dan aplikasi.

Ketersediaan sumber daya komputasi *firewall* seperti penggunaan CPU, *memory, bandwidth* dan *session* berdasarkan peningkatan kinerja suatu *firewall* dengan melakukan proses pemantauan pada sistem jaringan. Pada saat melakukan konfigurasi perlu dilakukannya pengujian keamanan pada suatu jaringan dengan menetapkan kebijakan yang dibutuhkan untuk melindungi sistem dari ancaman serangan.

Pada tugas akhir ini, menjalankan implementasi peran *firewall* dan melakukan *profiling* sistem *virtualized* Fortigate *firewall* guna mengetahui konsumsi penggunaan sumber daya komputasi pada fungsi deteksi, pencegahan, dan pemulihan terhadap serangan pada *firewall*. Pada *profiling* sistem *virtualized* Fortigate *firewall* terdapat dua skenario pengujian yaitu *service* HTTP *allow* dan *service* HTTP *block* dengan spesifikasi pada *firewall* Fortigate yaitu 1,5 GB *memory* dan 2 GB *memory*. Skenario pengujian dilakukan berdasarkan sumber daya komputasi pada sebelum serangan, saat serangan, dan setelah serangan terhadap *load testing*. Pada analisis, dilakukan perbandingan data hasil pengujian pada konsumsi penggunaan sumber daya komputasi pada *firewall*. Hasil analisis yang didapat bertujuan untuk mengetahui pola penggunaan sumber daya komputasi saat serangan.

I.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah yang menjadi bahan kajian pada penelitian ini, yaitu:

1. Bagaimana implementasi peran *firewall* dalam melindungi aset dan layanan IT?
2. Bagaimana cara mengenali profil suatu *firewall*?

I.3 Tujuan Penelitian

Berdasarkan rumusan masalah, tujuan yang akan dicapai pada penelitian ini yaitu:

1. Melakukan implementasi *firewall* yang diterapkan untuk memproteksi aset dan layanan IT dari serangan.
2. Mengetahui profil sistem *firewall* yang berfungsi berdasarkan

penggunaan sumber daya komputasi saat melakukan fungsi proteksi.

I.4 Batasan Penelitian

Batasan dari penelitian ini adalah sebagai berikut:

1. Berfokus pada fungsi pada *firewall* saat menjalani load testing berupa DDoS dan tidak membahas mekanisme *internal software* yang digunakan.
2. Berfokus pada penggunaan sumber daya komputasi pada *firewall* yaitu CPU, *memory, bandwidth* dan *session*.
3. Sistem yang digunakan *Based-on simulation* dan *virtualized*.

I.5 Manfaat Penelitian

Adapun manfaat yang diharapkan dari penulis adalah sebagai berikut:

1. Teoritis

Penelitian ini diharapkan dapat menjadi kontribusi pengetahuan pada fungsi *firewall* untuk memproteksi dari serangan. Memberikan gambaran profil *firewall* dalam penggunaan sumber daya komputasi.

2. Teknis

Penelitian ini diharapkan untuk mendapatkan gambaran penggunaan *virtualized* Fortigate. Mendapatkan gambaran implementasi teknis fungsi *firewall* untuk menangani serangan.

I.6 Sistematika Penulisan

Pada penelitian ini menggunakan sistematika penulisan yang dibagi menjadi beberapa bab, yang dapat mempermudah dalam penyusunan dalam pengerjaan Tugas Akhir ini. Adapun sistematika penulisan yaitu:

Bab I Pendahuluan

Pada bab ini berisi penjelasan tentang latar belakang, rumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian, serta sistematika penulisan.

Bab II Landasan Teori

Pada bab ini berisikan terkait *firewall,* serangan DDoS, sumber daya komputasi, *profiling*, TCP *Three-Way-Handshake*, virtualisasi, *load testing*.

Bab III Metodologi Penelitian

Pada bab ini dijelaskan penggambaran model konseptual penelitian dan sistematika penelitian yang berisi kerangka penelitian, dasar eksperimen, relasi skenario pengujian yang tersambung dengan data hasil eksperimen, dan sistematika penyusunan kesimpulan dan saran.

Bab IV Rancangan dan Skenario Pengujian

Pada bab ini menyajikan informasi mengenai keseluruhan perancangan *hardware* dan *software*. Skenario pengujian yang mencakup fungsi serangan, fungsi *firewall* dan data hasil pengujian mencakup data penggunaan sumber daya komputasi khususnya pada *firewall* dan data pada *attacker* dan *server* sebagai data pelengkap.

Bab V Analisis

Pada bab ini menjelaskan tentang hasil pengujian yang telah dilakukan yaitu hasil analisis sumber daya komputasi pada *firewall.* Analisa berfokus pada data hasil perbandingan *firewall* pada penggunaan sumber daya komputasi yang berupa data CPU, *memory, bandwidth,* dan *session.*

Bab VI Kesimpulan dan Saran

Pada bab ini menjelaskan kesimpulan yang berupa pola penggunaan dan nilai tertinggi dari metrik utama pada *firewall*. Saran dari penelitian yang berupa peluang lebih lanjut dari relasi skenario pengujian dan data percobaan.