# BAB I PENDAHULUAN

## I.1 Latar Belakang

Keamanan suatu jaringan menjadi hal yang sangat mutlak untuk diterapkan dengan memproteksi adanya ancaman serangan. Saat ini dengan berkembangnya sistem jaringan yang semakin pesat, perlu diketahui bahwa tidak ada sistem jaringan yang benar-benar aman untuk dapat mengamankan suatu sistem maupun data dari sebuah ancaman. Berdasarkan aspek keamanan informasi, suatu kerahasiaan data bahwa informasi di dalamnya tetap aman yang hanya dapat diakses oleh pihak tertentu saja, selain itu dapat menjamin integritas sumber daya yang dapat digunakan atau dimodifikasi oleh pihak tertentu, dan adanya ketersediaan informasi atau data yang dapat memudahkan pihak berwajib untuk dapat mengakses informasi tertentu pada saat dibutuhkan.

Salah satu serangan yaitu pada *Distributed Denial of Service* (DDoS) yang dapat mengakibatkan *server down, crash* hingga mati secara otomatis dan tidak dapat melayani permintaan dari pengguna. Ketersediaan layanan jaringan dengan pengamanan yang sangat ketat dan lambatnya dalam mengakses suatu informasi atau data, maka akan menyulitkan pihak yang berwenang dalam mengakses data atau informasi tersebut. Sehingga dari berbagai jenis serangan dapat dilakukan suatu tindakan dengan mengamankan jaringan menggunakan *firewall.*

*Firewall* merupakan bagian terpenting dalam keamanan jaringan yang berfungsi untuk memeriksa setiap paket yang masuk atau keluar dan memilah paket tersebut apakah dapat masuk ke dalam suatu jaringan. Penggunaan *firewall* tidak dapat menjamin sepenuhnya dalam mengamankan suatu perangkat, dikarenakan beberapa *firewall* terdapat fitur yang tidak selalu sama sesuai dengan tingkat efektifitasnya masing-masing.

Karakteristik *firewall* dapat menentukan jika terjadinya serangan DDoS pada suatu sistem. Salah satu jenis *firewall* yang banyak digunakan yaitu *next generation firewall* (NGFW) merupakan *firewall* yang memiliki kemampuan dalam mendeteksi dan memblokir terjadinya layanan IT yang terhenti, dengan memberikan proteksi perlindungan yang dapat menerapkan keamanan. Pada saat

melakukan konfigurasi *firewall* perlu dilakukannya pengujian keamanan dengan menetapkan kebijakan dan prosedur, yang dibutuhkan untuk melindungi sistem dari ancaman serangan. Dilakukan berdasarkan konsumsi sumber daya komputasi pada penggunaan CPU, *memory*, dan *session*.

Paloalto *firewall* merupakan salah satu NGFW yang dirancang untuk memberikan perlindungan keamanan yang terintegrasi dan konsisten ke seluruh jaringan pengguna. Virtualisasi Paloalto *firewall* dapat mengetahui atau mendeteksi adanya suatu serangan yang masuk ke dalam sistem penggunaan. Virtualisasi Paloalto *firewall* dapat mewujudkan salah satu aspek keamanan berdasarkan identifikasi suatu jaringan yang masuk ke dalam sistem dengan menentukan profil keamanan untuk melindungi terjadinya ancaman serangan.

Pada tugas akhir ini, melakukan *profiling* sistem dengan virtualisasi Paloalto *firewall* pada pendeteksian, pencegahan dan pemulihan berdasarkan pengukuran sumber daya komputasi. Terdiri dari dua skenario pengujian yaitu berdasarkan pengujian *service* HTTP *allow* dan berdasarkan pengujian *service* HTTP *block* dengan spesifikasi *memory* Paloalto pada RAM 5.5 GB dan spesifikasi RAM 8 GB. Melakukan pengukuran sumber daya komputasi mencakup penggunaan CPU, *memory*, dan *session* yang berfokus pada sebelum, saat, dan sesudah dilakukan serangan DDoS SYN *flood*.

## I.2 Perumusan Masalah

Berdasarkan uraian latar belakang, maka perumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana implementasi fungsi *firewall* untuk melindungi *asset* IT dan layanan IT?
2. Bagaimana cara menentukan suatu profil *firewall*?

## I.3 Tujuan Penelitian

Berdasarkan perumusan masalah, tujuan yang ingin dicapai pada penelitian ini adalah sebagai berikut:

1. Melakukan implementasi fungsi *firewall* pada saat melakukan *load testing*.

2. Mengetahui *profile* sistem pada *firewall* berdasarkan penggunaan sumber daya komputasi.

## I.4 Batasan Penelitian

Adapun batasan penelitian ini adalah sebagai berikut:

1. Penelitian berfokus pada fungsi *profiling* sistem virtualisasi Paloalto *firewall* dan tidak membahas mekanisme *internal software* yang digunak dan analisa paket.
2. Berfokus pada penggunaan dan pengukuran CPU, *memory* dan *session* dari *firewall* saat serangan DDoS.
3. Sistem yang digunakan pada skala laboratorium *simulation* dan *virtualized*

## I.5 Manfaat Penelitian

Adapun manfaat pada penulisan penelitian ini yaitu sebagai berikut:

1. Teoritis

   Secara teoritis pada penelitian ini diharapkan dapat menjadi kontribusi keilmuan yang berhubungan:

- Bagaimana mendapatkan gambaran cara untuk menangani serangan DDoS.
- Memberikan gambaran dalam penggunaan sumber daya komputasi pada virtualisasi Paloalto *firewall*.

2. Praktis

   Mendapatkan gambaran teknis untuk mengelola virtualisasi Paloalto *firewall* pada serangan DDoS SYN *flood*.

## I.6 Sistematika Penulisan

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

**Bab I** **Pendahuluan**

Pada Bab I ini berisi uraian mengenai latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, dan sistematika penulisan.

**Bab II Tinjauan Pustaka**

Pada Bab II ini berisi uraian pembahasan tentang *firewall*, *profiling*, sumber daya komputasi, DDoS, TCP *three-way handshake*, Paloalto *firewall*, *load testing*, penelitian terdahulu, serta penelitian saat ini.

**Bab III Metodologi Penelitian**

Pada Bab III ini berisi uraian mengenai pengembangan 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 IV ini berisi uraian mengenai perancangan *platform* percobaan berupa detail penggunaan *hardware* dan *software* berupa topologi percobaan. Skenario dalam implementasi dan pengujian yang mencakup pada fungsi serangan dan fungsi *firewall* mencakup hasil data penggunaan sumber daya komputasi pada *firewall*, *attacker*, dan *server*.

**Bab V Hasil Pengujian dan Analisis**

Pada Bab V ini berisi uraian hasil pengujian konsumsi penggunaan CPU, *memory*, dan *session* pada sebelum, saat dan sesudah serangan. Analisa berfokus pada *firewall* saja pada pola konsumsi sumber daya komputasi CPU, *memory* skenario yang telah ditentukan pada Bab IV.

**Bab VI Kesimpulan dan Saran**

Pada Bab VI ini menguraikan penjelasan kesimpulan yang berupa pola konsumsi sumber daya komputasi dan faktor dominan yang tertinggi penggunaan pada *firewall*, dan saran untuk penelitian selanjutnya dari relasi skenario pengujian.