

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi di Indonesia saat ini begitu pesat. Berdasarkan hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pengguna internet di Indonesia mencapai 215,63 juta orang pada periode 2022-2023 khususnya jaringan internet [1]. Seiring dengan kebutuhan masyarakat terhadap layanan yang memanfaatkan internet untuk mengakses berbagai informasi, tidak hanya itu internet juga bisa mengelola data informasi perusahaan, instansi, dan bisnis online lainnya.

Perkembangan teknologi informasi sayangnya tidak diikuti dengan perkembangan keamanan pada sistem itu sendiri dengan demikian cukup banyak sistem jaringan internet yang lemah dan harus ditingkatkan keamanannya. karena diluar sana banyak juga pihak-pihak yang tidak bertanggung jawab yang memanfaatkan informasi tertentu yang hanya menguntungkan pihak tersebut.

Ancaman terhadap keamanan jaringan menjadi semakin serius. Organisasi dan instansi di seluruh dunia kini menghadapi berbagai macam ancaman, mulai dari serangan DDoS, malware, phishing, hingga usaha pencurian data yang tidak sah. Pada penelitian ini Melawan ancaman-ancaman ini membutuhkan pendekatan yang kuat dan menyeluruh untuk keamanan jaringan, dimana serangan tersebut dapat mempengaruhi lalu lintas sebuah jaringan internet, bandwidth jaringan, waktu CPU, website dan lain-lain, overload dengan lalu lintas atau sangat lambat untuk pengguna [2]. Pengguna cloud tidak dapat mengakses sebuah layanan, penyerang juga akan mempengaruhi browser dengan memasukan kode berbahaya. Browser yang terinfeksi akan membuka banyak jendela tab browser sehingga pengguna yang sah tidak dapat mengakses web tersebut. Selain itu, penyerang akan membebani sistem cloud yang di targetkan dengan permintaan layanan yang banyak. Akibatnya sistem cloud akan berhenti merespons dan sumber daya akan keluar dari layanan internet. serangan tersebut sangatlah buruk. Hasilnya akan menjadi sebuah botnet, yang akan dilakukan oleh penyerang untuk melakukan serangan, awalnya serangan

HTTP DDoS dilakukan ketika banyaknya permintaan http yang sah dalam jumlah besar [3].

Seiring dengan berkembangnya ancaman ini, pentingnya optimalisasi keamanan jaringan yang efektif menjadi suatu hal yang penting bagi sebuah jaringan internet. Salah satu komponen yang digunakan dalam sistem keamanan jaringan adalah firewall. Sebagai dinding yang membatasi sebuah serangan melalui jaringan internet, firewall adalah sebuah fitur untuk mengontrol dan mengelola lalu lintas yang masuk dan keluar dari jaringan internet, serta mencegah akses dari pihak yang tidak bertanggung jawab [4].

Namun, mengandalkan firewall saja seringkali tidak cukup. Sistem deteksi intrusi (IDS) bertindak sebagai lapisan pertahanan kedua, memantau lalu lintas jaringan dan mendeteksi aktivitas mencurigakan yang mungkin melewati firewall. IDS memberikan visibilitas yang lebih mendalam terhadap potensi ancaman dan memungkinkan tim keamanan merespons lebih cepat [5].

PfSense adalah salah satu platform open source alias GPL GNU, yang dikembangkan untuk menyediakan semua layanan, untuk mengatasi ancaman serangan pada sebuah jaringan. instalasi dan konfigurasinya begitu sederhana dan biayanya terjangkau. sangat direkomendasikan untuk usaha kecil dan menengah karena menyediakan fitur layanan yang sangat luas. PfSense sebagai platform yang kuat fleksibel firewall dan routing, itu termasuk dari fitur yang biasanya digunakan di dalam pfSense memberikan keamanan yang potensial untuk distribusi dasar, dan juga pfSense sudah begitu populer, terbukti dalam instalasi yang tak terhitung jumlahnya mulai dari instansi kecil, menengah melindungi server jaringan dari ribuan perangkat [6].

Berdasarkan uraian diatas, penulis tertarik membangun suatu keamanan jaringan, yang dilakukan analisis terhadap keamanan jaringan dari jaringan tersebut, dimana pada kesempatan ini penulis akan membahas topik tentang ***“Optimalisasi Keamanan Jaringan Berbasis Firewall dan IDS Menggunakan PfSense”***

1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang, maka dirumuskan pokok permasalahan adalah:

1. Bagaimana mengkonfigurasi firewall dan IDS (Intrusion Detection Sistem) sehingga dapat memberikan perlindungan maksimal bagi jaringan.
2. Bagaimana cara menanggulangi ancaman keamanan jaringan (*Port Scanning*, *Denial of Service*, dan *Brute Force Login SSH*) menggunakan IDS?

1.3 Batasan Masalah

Batasan masalah yang dirumuskan dalam Analisis keamanan jaringan dengan firewall (IDS) menggunakan pfSense sebagai berikut :

1. Penelitian akan lebih terfokus pada ancaman-ancaman tertentu seperti serangan *Port Scanning*, *Denial of Service (DoS)*, dan *Brute Force Login SSH*.
2. Penelitian ini akan terfokus pada penggunaan firewall dan Sistem Deteksi Intrusi (IDS). Aspek-aspek keamanan lain seperti anti-virus, VPN, atau enkripsi data tidak akan menjadi fokus utama dalam penelitian ini.
3. Penelitian ini akan berkonsentrasi pada penggunaan PfSense sebagai solusi keamanan jaringan.
4. Penelitian akan membahas tentang prosedur instalasi dan konfigurasi dasar PfSense. Namun, penyesuaian konfigurasi khusus atau custom rules yang sangat teknis mungkin tidak akan dibahas dengan detail.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini diantaranya sebagai berikut:

1. Untuk memahami dan mengidentifikasi ancaman keamanan jaringan yang paling dominan, khususnya yang berkaitan dengan serangan *Port Scanning*, *Denial of Service (DoS)*, dan *Brute Force*.
2. Mengevaluasi efektivitas dan keterbatasan dari firewall dan IDS (*Intrusion Detection Sistem*) dalam melindungi jaringan dari ancaman external.

3. Mengetahui pengoptimalan dalam mengimplementasikan dan mengkonfigurasi PfSense, sehingga memberikan perlindungan yang maksimal pada jaringan.
4. Merekomendasikan pfSense berbasis FreeBSD sebagai platform keamanan jaringan *open-source* yang terjangkau dan efektif untuk digunakan dalam mengoptimalkan perlindungan jaringan.
5. Untuk memberikan kontribusi pada literatur keamanan jaringan di Indonesia dengan menyajikan temuan dan rekomendasi berdasarkan analisis dan pengujian terhadap PfSense.

1.5 Manfaat Penelitian

Penelitian ini memiliki manfaat yang signifikan dalam konteks keamanan jaringan di era digital saat ini, rumusan manfaat penelitian ini sebagai berikut :

1. Penelitian ini memberikan pemahaman mendalam tentang bagaimana firewall dan (IDS) beroperasi, serta potensi optimalisasi mereka melalui penggunaan PfSense. Ini penting, mengingat ancaman keamanan jaringan yang semakin meningkat dan kompleks.
2. Organisasi, khususnya usaha kecil dan menengah, akan mendapatkan rekomendasi konkret untuk memperkuat keamanan jaringan, dan juga mengurangi potensi *downtime* dan kerugian finansial.
3. Agar dapat meningkatkan kesadaran masyarakat tentang pentingnya keamanan jaringan dan memberikan solusi konkret untuk menghadapi ancaman di dunia maya.

1.6 Sistematika Penulisan

Sistematika penulisan yang akan digunakan dalam pembuatan laporan akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini akan membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan dalam laporan akhir ini.

BAB II TINJAUAN PUSTAKA

Bab ini akan membahas tentang landasan teori atau tinjauan pustaka yang mendasari pembahasan secara detail yaitu terdiri dari definisi-definisi yang berhubungan dengan ilmu dan permasalahan yang sedang diteliti.

BAB III METODE PENELITIAN

Bab ini akan membahas metode dan alur-alur apa yang digunakan dalam menyelesaikan studi ini, bab ini akan berisi objek penelitian, alur penelitian, dan alat bahan penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini akan membahas tahapan penelitian, mengidentifikasi dan melakukan penyelesaian masalah tersebut dengan mengaplikasikan perangkat dan pemodelan yang digunakan.

BAB V PENUTUP

Bab ini berisi kesimpulan dan saran yang akan dipaparkan setelah pengujian dilakukan, memberikan bukti-bukti yang diperoleh dari pengujian, dan akhirnya menarik kesimpulan, jika terdapat keterbatasan peneliti akan dipaparkan dalam saran untuk penelitian selanjutnya.