BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan merupakan hal yang penting untuk mengamankan suatu aset perusahaan, aset dari suatu sistem yang tidak tersedia atau tidak dipakai oleh yang berwenang dapat di pergunakan oleh oknum yang tidak bertanggung jawab untuk melakukan tindakan pencurian data, melakukan perubahan nilai pada file data, memodifikasi program sehingga tidak berjalan semestinya dan penyadapan terhadap data dalam suatu sistem.[1]

Monitoring keamanan jaringan diperlukan dengan tujuan memberikan peringatan adanya penyusupan terhadap sistem. Sehingga dampak negatif yang ditimbulkan dapat diminimalisir baik pada penyedia layanan maupun pada pengguna. Belum adanya system monitoring jaringan pada kantor PT. Sujama Jaya Makmur membuat permasalahan yang ada pada *server* layanan seperti FTP *server* menjadi lambat untuk ditangani. Terutama kaitannya dengan adanya serangan atau intrusi yang menyebabkan kerentanan pada bocornya data atau informasi yang ada. Sehingga akan menimbulkan masalah dikemudian hari yang dapat berakibat mengganggu atau menghambat kinerja dari layanan ekspedisi yang ada pada perusahaan tersebut. Oleh karena itu dibutuhkan system monitoring jaringan yang akan memberikan peringatan kepada administrator jaringan saat adanya tindakan pennyerangan atau penyusupan pada jaringan.

Sehingga administrator jaringan dapat dengan cepat mengambil tindakan yang diperlukan.

Upaya untuk meningkatkan keamanan jaringan komputer salah satunya adalah dengan firewall. Implementasi dari sistem firewall ini dapat berupa software ataupun hardware yang bersifat aktif dengan melakukan penyaringan paket data yang lewat berdasarkan pengaturan yang diinginkan. Cara lain adalah dengan mengimplementasikan Intrusion Detection System (IDS) pada sebuah jaringan komputer menggunakan *Routerboard Mikrotik*.

Mikrotik adalah perangkat jaringan komputer yang berupa *Hardware* dan *Software* yang memiliki banyak fitur, salah satunya dapat menjadi *Router*, sebagai alat *Filtering, Switching* dan banyak lagi fungsinya. Selain itu *Mikrotik* dapat juga berfungsi sebagai *firewall* bagi jaringan dan memberikan prioritas kepada administrator yang memiliki hak akses lebih tinggi. *Firewall filtering* tidak hanya digunakan untuk memblock serangan client agar tidak dapat mengakses resource tertentu, namun juga digunakan untuk melindungi jaringan local dari ancaman luar, misalnya virus atau serangan hacker. Biasanya serangan dari internet ini dilakukan dari banyak IP sehingga akan sulit bagi kita untuk melakukan perlindungan hanya dengan berdasarkan IP.

Sedikit berbeda dengan firewall, Intrusion Detection System (IDS) adalah sebuah system yang digunakan untuk melakukan deteksi adanya usaha-usaha penyusupan terhadap sebuah system dengan melakukan pengamatan trafik data secara real-time. sistem peringatan (*alert*) akan memberikan peringatan kepada

administrator jaringan dalam bentuk notifikasi singkat pada system yang sudah dipasangi IDS, jika terdeteksi adanya aktifitas serangan atau penyusupan. Selain itu aktifitas serangan atau penyusupan yang telah terdeteksi dapat dilihat dan dianalisa dengan lebih *detail* melalui pesan email yang dikirimkan kepada administrator. Serta tindakan pencegahan yang diperlukan pada *Intrusion Detection System* seperti blok serangan terhadap *IP address* yang bersangkutan dapat dilakukan dengan segera.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, maka permasalahan utama adalah "Bagaimana membangun *Intrusion Detection System* dan *Firewall* menggunakan Routerboard Mikrotik yang dapat mengirimkan informasi penyerangan kepada administrator?"

1.3 Batasan Masalah

Berdasarkan rumusan masalah diatas maka didapat batasan-batasan masalah yang digunakan untuk membatasi ruang masalah dalam melakukan penelitian. Batasan masalah yang digunakan adalah sebagai berikut:

1. Menerapkan *Intrusion Detection System* dan *firewall* menggunakan Mikrotik yang dilakukan di kantor PT.Sujama Jaya Makmur.
2. Analisis yang dilakukan hanya untuk memantau aktivitas jaringan *nirkabel* jika terjadi serangan.
3. System dibangun dengan jenis Network-based IDS (NIDS)
4. Tidak membahas analisis dari semua jenis serangan secara mendalam.

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud

Maksud dari penelitian ini adalah menganalisis dan merancang keamanan jaringan nirkabel dengan menerapkan *Intrusion Detection System* dan *Firewall* menggunakan *Routerboard Mikrotik*.

1.4.2 Tujuan

1. Membangun *Intrusion Detection System* dan *firewall* (IDS) menggunakan Routerboard Mikrotik.
2. Memonitoring keamanan, memahami kelebihan dan kekurangan *Intrusion Detection System* dan *firewall* (IDS) pada Wireless.
3. Dapat memahami teknik pembuatan dan perancangan jaringan sistem deteksi serangan.
4. Dapat mengirimkan informasi penyerangan berupa *ip address*, waktu, tanggal dan protokol yang dilakukan oleh penyerang.

1.5 Manfaat Penelitian

Dengan melakukan penelitian ini, maka diharapkan mendapatkan manfaat-manfaat sebagai berikut :

1. Bagi pengguna sistem merasa terbantu dalam mengawasi dan melindungi jaringan.
2. Dapat memonitoring *traffic* jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan.

1.6 Metode Penelitian

Metode yang dilakukan selama pembuatan skripsi meliputi:

1.6.1 Metode Pengumpulan Data

1.6.1.1 Metode Observasi

Metode pengumpulan data dengan cara pengamatan dan pencatatan secara sistematis terhadap objek yang diteliti. Dengan cara melakukan pengamatan langsung di kantor PT. Sujama Jaya Makmur tentang perancangan dan implementasi sistem sebelum diterapkan dan sesudah diterapkan sistem yang baru.

1.6.1.2 Metode Wawancara

Metode wawancara dilakukan untuk mendapat informasi tambahan. Wawancara dilakukan dengan pemilik maupun orang-orang yang sering menggunakan jaringan yang ada di PT.Sujama Jaya Makmur.

1.6.2 Metode Perancangan Sistem

Metode implementasi yang digunakan dalam penelitian ini adalah PPDIOO Network Lifecycle. Tahapan yang terdapat pada PPDIOO adalah Prepare, Plan, Design, Implement, Operate, dan Optimize.

1.7 Sistematika Penulisan

Sistematika penulisan yang meliputi beberapa bab ini bertujuan untuk mempermudah dalam penulisan laporan skripsi.

BAB I PENDAHULUAN

Bab pendahuluan ini terdiri dari latar belakan masalah, rumusan masalah, batasan masalah, maksud dan tujuan, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab landasan teori merupakan tinjauan pustaka, berisi dasar teori yang digunakan dari sumber dalam penelitian dan referensi yang menjadi landasan dasar dalam perancangan, analisis kebutuhan sampai implementasi dan pengujian system.

BAB III ANALISIS DAN PERANCANGAN

Berisi tentang analisis kebutuhan jaringan, pengambilan data yang diperlukan, kebutuhan hardware dan software, serta perancangan jaringan yang dilakukan dalam penelitian.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini merupakan tahapan implementasi dan pengujian yang merupakan tahap yang dilakukan dalam mengimplementasikan dari hasil penelitian, dan perancangan yang diidentifikasikan untuk mengimplementasikan dan menguji sistem yang telah dibuat.

BAB V PENUTUP

Bab ini berisi kesimpulan dari penelitian serta saran guna memperbaiki kelemahan dan kekurangan yang diperoleh dari perancangan *Intrusion Detection System* dan *firewall* menggunakan Routerboard Mikrotik.

DAFTAR PUSTAKA

Daftar pustaka berisi referensi-referensi yang digunakan dalam analisis dan perancangan *Intrusion Detection System* dan *firewall* menggunakan Routerboard Mikrotik.