BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan merupakan perhatian utama ketika hendak membangun sebuah infrastruktur jaringan, tujuan mengamankan jaringan adalah untuk mengantisipasi bentuk ancaman terhadap sistem komputer yang terhubung ke internet. Salah satu akibat dari ancaman tersebut, banyak jaringan dan sistem komputer terganggu bahkan mengalami kerusakan. Agar dapat menanggulangi hal tersebut bisa menggunakan *firewall* yang terintegrasi dengan router. *Firewall* merupakan sistem keamanan yang diterapkan dengan tujuan untuk melindungi, baik dengan menyaring (*filtering*), membatasi (*limit*) atau menolak (*block*) suatu atau semua hubungan suatu segmen pada jaringan lokal dengan jaringan publik yang bukan merupakan ruang lingkupnya melalui *packet* atau *traffic* yang melaluinya [1].

Router merupakan perangkat terluar yang menghubungkan jaringan *Local Area Network (LAN)* dengan internet, maka mengakibatkan lebih mudah diserang oleh seseorang yang tidak bertanggung jawab. Banyak sekali alat yang dapat digunakan untuk melakukan penyerangan pada router contohnya seperti *Hping3 (DoS), Hydra (Brute-Force), Srictp Exploitation (Winbox Exploitation)*. Serangan ini bertujuan untuk melumpuhkan dan mencoba menemukan kemungkinan password agar dapat login ke router Mikrotik [2].

Penerapan *port blocking* dan *port knocking* pada *firewall*, administrator dapat membuat rules yang sangat kompleks. *Port blocking* dan *port knocking* pada *firewall* bisa dimanfaatkan untuk mencegah atau menolak akses yang dapat mengancam jaringan atau server. *Port knocking* dapat digunakan untuk membuka akses ke port tertentu yang telah diblokir oleh *firewall*, pada device dengan cara mengirimkan paket tertentu. Fungsi dari keamanan jaringan metode *port blocking* untuk melakukan autentikasi sebelum mengakses server melalui sebuah aturan yang dikonfigurasi di *firewall* [3].

Virtual Private Network (VPN) disebut juga koneksi *private* dengan menggunakan internet sebagai perantara. Penggunaan *VPN* memberikan rasa aman bagi penggunanya karena hanya orang tertentu yang dapat mengaksesnya serta dapat juga dibuat terenkripsi [4].

Monitoring jaringan dapat membantu administrator mengelola suatu jaringan. Jika ada koneksi *down* maka akan langsung terlihat di sistem monitoring. Tak hanya itu, sistem monitoring jaringan juga mampu menganalisis dan memperlihatkan lalu lintas data di dalam jaringan sehingga memudahkan administrator memanajemen kualitas jaringan tersebut [5].

Berdasarkan penelitian sebelumnya, maka penulis mengusulkan metode yang digunakan adalah *Instrusion Detection System (IDS)* dan dibantu dengan *Port Blocking*. Metode ini sangat efektif digunakan untuk mendeteksi serangan dan melakukan pemblokiran. Sedangkan pada keamanan remote akses menggunakan *Virtual Private Network (VPN)*, cara ini lebih mudah digunakan dan aman dibanding *rule port knocking* yang harus mengetuk *ip address* dan *port* untuk dapat meremote ke router.

Jenis *VPN* yang digunakan adalah *L2TP VPN*, jenis vpn ini dapat digabungkan dengan *IPSec* untnuk menambah keamanannya serta dapat mengamankan router dari serangan *brute force*.

Untuk pengujiannya penulis mengusulkan menggunakan tool *nmap, hping3* dan *patator*, karena pada penelitian sebelumnya menggunakan *winbox exploit* dimana tool ini sudah usang dan tidak bisa digunakan pada router os versi terbaru.

Monitoring yang digunakan adalah *cacti* karena bersifat *open source*, proses instalasinya mudah, dan fitur dimilikinya banyak.

1.2 Rumusan Masalah

Berdasarkan dengan latar belakang yang telah diuraikan diatas, maka dapat dibuat rumusan masalah sebagai berikut :

1. Apakah penerapan firewall filter rules menggunakan metode *Intrusion Detection System (IDS)* dan *Port Blocking* di router Mikrotik RB941-2nD dapat mencegah serangan *ddos, port scanner,* dan *brute force* ?,
2. Apakah penerapan *Virtual Private Network (VPN)* sebagai *tunneling* dapat mencegah serangan *exploit (brute force attack)* ?,
3. Apakah penerapan *L2TP VPN* yang terenkripsi menggunakan *IPSec* dapat mengamankan jalur *tunneling* pada *Virtual Private Network (VPN)* ?,
4. Apakah penggunaan *Cacti* sebagai aplikasi monitoring efektif digunakan untuk memantau kondisi dari suatu jaringan ?.

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang sudah didapat, maka batasan masalah yang akan digunakan sebagai pembatas ruang lingkup untuk melakukan penelitian. Maka Batasan masalah yang akan dipakai dalam penelitian ini adalah sebagai berikut :

1. Sistem diimplementasikan menggunakan router Mikrotik RB941-2nD dan sistem operasi Linux Ubuntu.
2. Sistem dibangun dengan menggunakan *firewall filter rules* yang cukup kompleks.
3. *Virtual Private Network (VPN)* dirancang menggunakan *L2TP* yang terenkripsi menggunakan *IPSec*.
4. Penyerangan hanya di uji coba menggunakan *port scanner, ddos,* dan *brute force*.
5. Dalam melakukan penyerangan menggunakan sistem operasi Kali Linux menggunakan alat *nmap, hping3, patator*.
6. Penerapan monitoring server dibangun menggunakan *Cacti* yang berjalan diatas sistem operasi Linux Ubuntu.

1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut.

1. Dapat Mengetahui *firewall filter rules* menggunakan metode *Intrusion Detection System (IDS)* dan *Port Blocking* di router Mikrotik RB941-2nD dapat mengatasi serangan *port scanner*, *ddos*, dan *brute force* ke jaringan.
2. Dapat mengetahui penerapan *Virtual Private Network (VPN)* sebagai *tunneling* dapat mengamankan remote akses *(log-in)* ke router Mikrotik RB941-2nD dari serangan *brute force*.
3. Dapat mengetahui penerapan *L2TP VPN terenkripsi* menggunakan *IPSec* dapat mengamankan *Virtual Private Network (VPN)*.
4. Dapat mengetahui dengan menerapkan monitoring server menggunakan *Cacti* efektif digunakan jika terjadinya gangguan pada sistem dan jaringan.

1.5 Manfaat Penelitian

Dengan dilakukannya penelitian ini, maka diharapkan mendapatkan manfaat sebagai berikut :

1. Manfaat dari penelitian yaitu menghasilkan keamanan pada jaringan dari hal yang membahayakan infrastruktur jaringan, karena penggunaan *Intrusion Detection System (IDS)* dan *Port Blocking* mampu mengamankan router dengan baik.
2. Manfaat dari penerapan *Virtual Private Network (VPN)* yaitu mampu melakukan proteksi terhap orang yang ingin mencoba login ke router.
3. Manfaat bagi pengguna adalah bisa membuat yang menggunakannya merasa aman saat memakai *Virtual Private Network (VPN)* untuk meremote suatu server maupun perangkat lainnya.
4. Mempermudah memantau kondisi jaringan karena sudah adanya sistem monitoring dan dapat juga digunakan melihat jika ada yang menyerang.

1.6 Sistematika Penulisan

Pada penulisan skripsi ini, mempunyai sistematika sebagai berikut :

BAB I PENDAHULUAN

Bab ini merupakan pendahuluan yang menjelaskan tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi landasan teori yang digunakan dalam penyusunan skripsi. Literatur yang digunakan bersumber dari buku maupun dari jurnal.

BAB III METODE PENELITIAN

Bab ini membahas metodologi penelitian, metode tersebut seperti analisis masalah, metode implementasi, dan pengujian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas tahapan penerapan sistem dari hasil penelitian yang dilakukan sebelumnya yaitu keamanan jaringan.

BAB V PENUTUP

Bab ini berisi kesimpulan dan saran yang penulis rangkum dari hasil penelitian.

LAMPIRAN

Bab ini berisi detail konfigurasi dari penelitian yang dilakukan.