BAB 1

PENDAHULUAN

1.1 Latar Belakang

Wireless merupakan salah satu teknologi bidang telekomunikasi yang berkembang pesat. Teknologi ini memiliki kelebihan dengan menawarkan kemudahan konfigurasi serta flesibilitas dalam mengaksesnya. Bahkan sekarang ini semua fasilitas umum seperti taman kota, rumah makan, mall dan lain sebagainya sudah dilengkapi dengan jaringan *wireless*. Namun perlu diketehui celah keamanan pada jaringan tersebut masih rentan terhadap pencurian data hak akses seperti membobol *username* dan *password* pada *Wireless*. Selain itu, contoh lainnya adalah serangan *DOS (Denial Of Service)* bisa dikenal sebagai tindak kejahatan dengan memanfaatkan serangan terhadap *server* yang menghabiskan *resource*. Dan pembagian jaringan atau *bandwidth* yang tidak merata.

Peranan *wireless* device semakin penting dan menjadi kebutuhan utama sebagian masyarakat. Tidak hanya laptop dan telepon seluler,konsul game pun bisa dihubungkan dengan *Wireless*. Oleh karena itu setiap pemilik tempat yang mempunyai layanan Wi-Fi dapat mengimplementasikan *Captive portal* agar tidak semua orang dapat menggunakannya tanpa memiliki *username* dan *password*.

Captive portal merupakan mesin router atau *gateway* yang memanfaatkan web browser sebagai sarana atau perangkat *autentikasi* yang aman dan terkendali dalam mengijinkan adanya trafik hingga user melakukan registrasi. Hal ini dilakukan untuk mencegah semua paket berupa data dalam bentuk apapun dan

kemanapun, sampai user membuka web browser dan mencoba untuk mengakses internet. Browser telah diarahkan ke suatu web khusus yang telah ditentukan untuk melakukan otentikasi, atau sekedar menampilkan halaman kebijakan yang berlaku dan mengharuskan pengguna untuk menyetujuinya. *Captive portal* sering kali digunakan pada jaringan *(Wi-Fi, hotspot).Hotspot* adalah lokasi dimana user dapat mengakses melalui mobile komputer seperti laptop tanpa mengguakan koneksi kabel dengan tujuan suatu jarigan seperti internet [1].

Fitur *Snort IDS (Intrusion Detection System)* bisa digunakan sebagai deteksi serangan berupa *alert* dengan menambahkan rule secara manual berdasarkan definisi deteksi serangan yang ingin dihasilkan. Dalam penerapan mekanisme *Captive portal* ini penulis akan memanfaatkan *Router Pfsense*, karna penggunaaan *Router Pfsense*ini masih belom banyak. Pada *Router PfSense* terdapat banyak fitur untuk membantu mengamankan sistem jaringan yang dibangun, salah satunya adalah fitur *Snort IDS (Intrusion Detection System)*.

Hasil dari implementasi tersebut yaitu adanya mekanisme otentikasi *Captive portal* pada hostpot, user diwajibkan melakukan login menggunakan *username* dan *password*. Selain itu penerapan *SSL* dimaksudkan sebagai enkripsi pada protokol *HTTPS web Captive Portal*. Serta Konfigurasi *Snort IDS (Intrusion Detection System)* dan *rule TCP Flooding, UDP Flooding* yang akan membarikan *alert* bila terjadi serangan *DOS (Denial Of Service)* oleh seorang attacker. Selain itu hasil akhir penelitian ini penulis juga membahas tentang manajemen *bandwidth* pada *Pfsense* yaitu menggunakan metode *trafic shaper*yang dimiliki *Pfsense*.

Pada kajian pustaka yang telah dipelajari, kebanyakan penelitian sebelumnya tidak menerapkan *Snort IDS (Intrusion Detection System)*menggunakan *Pfsense* untuk keamanan jaringan*hotspot*, hanya sebatas perancangan *pfsense* sebagai *captive portal*. Pada penelitian ini juga akan membahasa tentang pengamanan jaringan menggunakan *Snort IDS (Intrusion Detection System)* yang akan memberikan *alert* bila terjadi serangan. Serta membahas tentang penerapan pengamanan *Captive portal* menggunakan Satifikat SSL dan HTTPS dan manejemen *Bandwidht* menggunakan metode *Trafic Shaper* yang membatasi *Upload* dan *Download*. Dari permasalahan yang ada penulis akan mengangkat judul penelitian tentang *Simulasi Implementasi Pfsense Sebagai Captive Portal, Sistem Autentikasi Dan Manajemen Bandwidth Pada Wireless Hotspot Berbasis FreeBSD*.

1.2 Rumusan Masalah

Dari latar belakang diatas, rumusan masalah yang dapat disimpulkan adalah:

a. Bagaimana cara untuk membangun sistem otentikasi dengan *Captive portal* menggunakan pfsense untuk pengamanan jaringan hotspot?
b. Bagaimana cara untuk mengimplementasikan fitur pengamanan dengan menggunakan sertifikat SSL dan HTTPS pada *Captive portal* dengan menggunakan pfsense untuk pengamanan *username* dan *password*?
c. Bagaimana cara untuk mengimplementasikanfiturpengamanan dengan menggunakan*Snort IDS (Intrusion Detection System)* dengan menggunakan pfsense untuk pengamanan dari serangan *DOS (Denial Of Service)*.

d. Bagaimana mengimplementasikan fitur pembatasan *bandwith* atau manajemen *bandwidth* untuk pengguna layanan jaringan hotspot *pfsense*?

1.3 Batasan Masalah

Batasan permasalahan dibatasi dengan tujuan agar pembahasan lebih terfokus dalam peneltiain. Diberian batasan sebagai berikut:

a. Menggunakan modem Modem Huawei HG8245H, *Wireless* Access Point TP-Link TD-W8961ndan PC sebagai router.
b. Hanya membahas instalasi dan konfigurasi sistem routerPfsense.
c. Dalam pembahasan captive portal, pengamanan dengan ssl dan https dan juga manajemen bandwith serta penerapan *IDS (Intrusion Detection System)* hanya akan membahas tentang fitur standar dan tidak membahas salah satu fitur secara mandalam.
d. Untuk pengaturan *bandwidth* akan membatasi upload dan download.
e. Pengujian sartifikat *SSL* dan *HTTPS* menggunakan software Wireshark dan *SSLStrip* pada Kali Linux.
f. Pengujian *Snort IDS (Intrusion Detection System)*dengan melakukan serangan *DOS (Denial Of Service)*menggunakan *Hping3 Kali linux* dan *Loic (Low Orbit Ion Cannon)*.
g. Tidak membahas tentang perbandingan dengan metode lain.
h. Dalam metode pengerjaan hanya sampai dengan tahap uji coba apakah konfigurasi yang telah dibuat sesuai atau tidak.

1.4 Tujuan Penelitian

Tujuan pembuatan tugas akhir ini adalah menerapkan penggunaan sistem routerpfsense sebagai autentikasi dalam jaringan *Wireless* sehingga meningkatkan keamanan dan kinerja jaringan *Wireless*.

1.5 Manfaat Penelitian

Manfaat dari perancangan sistem ini adalah :

a. Membuat pengamanan jaringan hotspot dengan sistem otentikasi *Captive portal* dengan menggunakan *Pfsense*.
b. Mengetahui sejauh mana pengamanan dengan metode ssl dan https dalam *Captive portal* dengan menggunakan *Pfsense* untuk pengamanan *username* dan *password*.
c. Mengimplementasikan sistem pengamanan dengan menggunakan *Snort IDS (Intrusion Detection System)*pada*Pfsense* untuk memberikan peringatan ketika terjadi serangan dalam jaringan *Captive Portal*.
d. Mengimplementasikan fitur manajemen bandwith (bandwith limiter) atau pembatasan *bandwidth* untuk pengguna layanan hotspot pfsense.
e. Berbasis opensource sehingga dapat mengurangi ketergantungan pada software berbayar karena tidak perlu membayar lisensi

1.6 Metode Penelitian

Peneliti menggunakan beberapa metode penelitian untuk mengarahkan penelitian (perancangan) ini agar tujuan penelitian yang telah ditentukan dapat tercapai. Adapun beberapa metode penelitian yang digunakan peneliti sebagai berikut:

1.6.1 Studi Pustaka

Metode ini ditempuh peneliti guna mendapatkan informasi dan pengetahuan dari literatur-literatur yang berkaitan dengan objek yang dikaji dalam peneliti ini. Adapun literatur yang dimaksud berupa penelitian-penelitian sebelumnya, buku, majalah dan internet.

1.6.2 Metode Perancangan

Perancangan sistem dimulai dengan menentukan komponen-komponen yang dibutuhkan dalam sistem seperti *hardware* dan *software* yang digunakan kemudian membuat topologi jaringannya. Topologi jaringan yang akan dirancang terdiri dari *Modem* , *Pfsense* dan*Access Point.Pfsense* yang digunakan yaitu*Pfsense 2.3.5* .

1.6.3 Metode Implementasi

Dalam penelitian ini metode implementasi yang ditempuh peneliti meliputi langkah-langkah seperti:

1. Implementasi*Captive Portal.*
2. Implementasi *Bandwidth.*
3. Implementasi *SSL* dan *HTTPS* pada halaman login *Captive Portal.*
4. Implementasi *Snort IDS (Intrusion Detection System).*

1.6.4 Pengujian Sistem

Untuk mengetahui keakuratan dan kesempurnaan sistem, peneliti melakukan pengujian dengan tahapan pengujian yang mana akan terangkan lengkap pada bab 4.

1.7 Sistematika Penulisan

Untuk memberikan gambaran mengenai laporan yang akan dibuat, adapun sistematika penulisan laporan sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang permasalahan, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, metode penelitian dan sistematika penulisan. Bab ini merupakan bagian pengantar dari penelitian yang akan dibahas pada skripsi ini.

BAB II TINJAUAN PUSTAKA

Bab ini berisikan tinjauan pustaka dan teori-teori pendukung yang berkaitan dengan skripsi untuk menunjang dalam proses penelitian ini. Teori yang akan diangkat yaitu mengenai perancangan *Pfsense* sebagai *Captive portal* dan manajemen *bandwidth*.

BAB III METODE PENELITIAN

Bab ini menjelaskan mengenai analisa kebutuhan sistem, metode yang digunakan, perancangan topologi, perancangan perangkat lunak dan juga tahapan dalam mengimplementasikan metode yang ada.

BAB IV HASIL DAN PEMBAHASAN

Memaparkan dari hasil-hasil tahapan penelitian, mulai dari analisis, desain, hasil testing dan implementasinya.

BAB V PENUTUP

Menguraikan kesimpulan dari penelitian dan saran-saran sebagai bahan pertimbangan untuk penelitian selanjutnya.