

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Dewasa ini, hampir semua fasilitas umum, baik itu yang dikelola oleh swasta maupun dikelola oleh pemerintah, hampir dapat dipastikan terdapat fasilitas wi-fi atau jaringan internet tanpa kabel. Bahkan sekarang ini, tidak hanya didalam fasilitas umum saja, namun juga sudah merambah pada taman kota, dan fasilitas lainnya, seperti rumah makan, mall, dan lain sebagainya. Tapi ada beberapa hal yang menjadi sorotan utama, yaitu tentang keamanan jaringan wi-fi atau yang sering disebut hotspot, Selama ini, keamanan jaringan difasilitas umum maupun swasta, baik itu di sebuah gedung, sekolah, sampai fasilitas pemerintahan masih sangat kurang. Padahal, pada masa sekarang ini, disaat semua hal terhubung dengan internet semua orang dapat mengakses apapun yang mereka inginkan. Termasuk perbuatan jahat, seperti melakukan penyadapan, maupun pencurian informasi pribadi. Dan pembagian jaringan atau bandwidth yang tidak merata.

Melihat akan hal tersebut maka dirancanglah suatu sistem pengamanan menggunakan captive portal, serta penerapan sertifikat ssl dan http pada captive portal juga manajemen bandwidth dengan memanfaatkan *firewall OS pfsense*. Proyek akhir ini terdiri dari implementasi dan perancangan pengamanan hotspot dengan sistem otentikasi captive portal dan ditambah dengan pengamanan ssl dan https pada proses otentikasi. Solusi tersebut dinilai tepat Karena dapat membatasi siapa saja yang dapat mengakses jaringan hotspot tersebut dan juga menghindari adanya kemungkinan spoofing atau pencurian username dan password. Dan ditambah dengan manajemen bandwidth atau pembatasan bandwidth untuk user, untuk mengoptimalkan bandwidth, terutama untuk jaringan wireless.

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 mengimplementasikan fitur pembatasan bandwith atau manajemen bandwidth untuk pengguna layanan jaringan hotspot pfsense?

1.3 Tujuan

Tujuan dari perancangan sistem ini adalah :

- a. Membuat pengamanan jaringan hotspot dengan sistem otentikasi captive portal dengan menggunakan pfsense
- b. Mengimplementasikan sistem pengamanan dengan metode ssl dan https dalam captive portal dengan menggunakan pfsense untuk pengamanan username dan password
- c. Mengimplementasikan fitur manajemen bandwidth (bandwidth limiter) atau pembatasan bandwidth untuk pengguna layanan hotspot pfsense

1.4 Batasan Masalah

- a. OS PC Router yang digunakan adalah *pfsense 2.2.3*
- b. Menggunakan PC (Personal computer) Sebagai PC Router
- c. Dalam pembahasan captive portal, pengamanan dengan ssl dan https, dan juga manajemen bandwidth, hanya akan membahas tentang fitur standar dan tidak membahas salah satu fitur secara mendalam.
- d. Untuk manajemen bandwidth, dilakukan percobaan terhadap user, dan penerapannya hanya bersifat umum, yaitu berarti tidak membatasi satu user atau satu ip tertentu.
- e. Dalam metode pengerjaan hanya sampai dengan tahap uji coba dan evaluasi yang mana dilakukan pengujian sistem oleh user secara langsung apakah konfigurasi yang telah dibuat sesuai atau tidak, jika terdapat kekurangan maka akan diperbaiki.
- f. Tidak membahas tentang mikrotik router sebagai internet gateway
- g. Tidak membahas tentang teori wireless access point, fitur wireless Access point, dan segala hal diluar bahasan utama.

1.5 Definisi Operasional

Otentikasi adalah suatu langkah untuk menentukan atau mengonfirmasi bahwa seseorang (atau sesuatu) adalah autentik atau asli. Melakukan autentikasi terhadap sebuah objek adalah melakukan konfirmasi terhadap kebenarannya. Sedangkan melakukan otentikasi terhadap seseorang biasanya adalah untuk memverifikasi identitasnya. Pada suatu sistem komputer, otentikasi biasanya terjadi pada saat login atau permintaan akses.

Wireless LAN dapat didefinisikan sebagai sebuah sistem komunikasi yang dapat digunakan user dalam melakukan koneksi internet tanpa menggunakan kabel (wireless). Fungsi yang ditawarkan disini dapat berupa konektivitas yang andal sehubungan dengan mobilitas user.

FreeBSD adalah *UNIX*-like operating system (sistem operasi seperti UNIX), tersedia gratis di internet, sangat banyak digunakan dalam dunia ISP (Internet service provider), embedded devices, serta bidang lain yang membutuhkan reliabilitas tinggi. FreeBSD dibuat dari source code UNIX original yang diproduksi oleh AT&T tahun 1970.

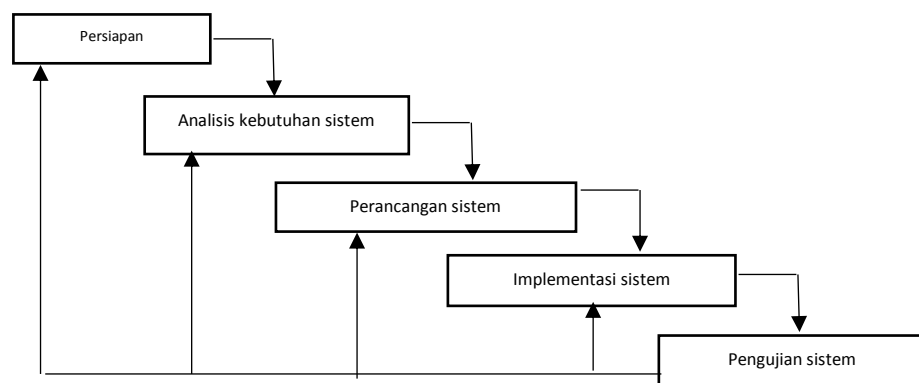
Open source adalah program komputer yang lisensinya memberi kebebasan kepada pengguna dalam menjalankan program tersebut untuk apa saja, mempelajari dan memodifikasi program tersebut, dan mendistribusikan penggandaan program asli atau yang sudah dimodifikasi tanpa harus membayar royalti kepada pembuat sebelumnya. Sehingga jika para pembuat aplikasi dapat mempelajari, mendistribusikan ulang, dan mengubah perangkat lunak tersebut, maka perangkat lunak itu akan berkembang. Inilah yang disebut masyarakat mengembangkannya, mengaplikasikannya, dan memperbaiki kelemahannya. Dari kita, oleh kita dan untuk kita bersama.

Pfsense adalah sebuah open source yang berbasis free BSD yang digunakan untuk firewall sekaligus router yang handal. bisa juga digunakan untuk proxy server menggunakan squid + lusa cacheboy.

Router adalah perangkat network yang digunakan untuk menghubungkan beberapa network, baik network yang sama maupun berbeda dari segi teknologinya seperti menghubungkan network yang menggunakan topologi Bus, Star dan Ring. Router minimal memiliki 2 network interface.

Captive Portal adalah suatu teknik autentikasi dan pengamanan data yang membuat user atau oengguna suatu jaringan harus melalui satu halaman web khusus, sebelum dapat mengakses internet.

1.6 Metode Pengerjaan



Gambar 1-1 Metode Pengerjaan

Adapun metode penelitian dalam pembuatan proyek akhir ini adalah metode waterfall, adapun metodenya sebagai berikut :

a. Persiapan

Mengumpulkan, mempelajari dan memahami teori-teori yang dibutuhkan dalam pembuatan proyek akhir ini dari buku-buku referensi, artikel di internet, jurnal, ebook, dan sumber lain yang terkait dengan Pfsense dan firewall.

b. Analisis Kebutuhan Sistem

Sebelum melakukan perancangan maka harus terlebih dahulu melakukan analisis kebutuhan yang diperlukan selama perancangan captive portal ini, mulai dari pemilihan computer, switch, dan sebagainya.

c. Perancangan Sistem

Perancangan dilakukan dengan mengacu kepada hasil analisis serta perancangan yang telah dilakukan sebelumnya.

d. Implementasi Sistem

Melakukan proses implementasi dari hasil analisis serta perancangan yang telah dilakukan sebelumnya.

e. Pengujian Sistem dan Evaluasi

Melakukan proses pengujian peralatan untuk memastikan Fitur dapat berjalan dengan baik dan sesuai dengan kebutuhan.

1.7 Jadwal Pengerjaan

Tabel 1-1 Jadwal Pengerjaan

No.	Kegiatan	Waktu Pengerjaan																			
		Juni 2015				Juli 2015				Agustus 2015				September 2015				Oktober 2015			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Persiapan																				
2	Analisis Kebutuhan																				
3	Perancangan																				
4	Implementasi dan Pengujian																				
5	Dokumentasi																				

Berdasarkan jadwal pengerjaan pada tabel 1-1, proyek akhir dikerjakan pada bulan juni, dan berakhir pada bulan oktober 2015