PERANCANGAN DAN IMPLEMENTASI PFSENSE SEBAGAI CAPTIVE PORTAL, SISTEM OTENTIKASI, DAN MANAJEMEN BANDWIDTH BAGI WIRELESS HOTSPOT BERBASIS FREEBSD

Adam Aditya Nugraha[1], Tedi Gunawan[2], Simon Siregar[3]

[1,2,3] Fakultas Ilmu Terapan - Telkom University adamnugraha@yahoo.co.uk[1], tedi@tass.telkomuniversity.ac.id[2], simon@tass.telkomuniversity.ac.id [3]

Abstrak

Dalam beberapa tahun terakhir ini, wifi telah menarik banyak perhatian, terutama untuk para pengguna internet, dikarenakan kemudahan konfigurasi dan kemudahan akses yang disediakan. Namun dalam perkembangannya hingga saat ini, beberapa celah keamanan masih ditemukan dalam media koneksi ini, seperti spoofing atau pencurian data, baik itu data pribadi maupun data rahasia, manipulasi bandwidth dan kecurangan pemakaian bandwidth, serta masih banyak lagi. Agar celah keamanan pada jaringan wifi bisa diatasi maka dibangunlah suatu sistem terintegrasi yang dapat menangani masalah keamanan pada jaringan wifi, diantaranya, membangun sistem captive portal yang mengharuskan user melakukan login terlebih dahulu sebelum mengakses internet, juga implementasi ssl dan https pada captive portal untuk melindungi data user dari pihak luar, serta implementasi manajemen bandwidth untuk mengatur pemakaian bandwidth pada user dengan memanfaatkan open source firewall yaitu Pfsense yang berbasis freebsd.

Kata kunci: *Wireless hotspot*, keamanan jaringan, *pfsense*, *captive portal*, sertifikat ssl, manajemen bandwidth

Abstract

In recent years, the wifi has attracted a significant attention, especially for Internet users, because of ease of configuration and access. But in its development , some security holes has been founded in this connection, such as spoofing or data theft, either it is personal or confidential data, manipulation of bandwidth usage, and many more. To cover a gap of security holes on the wifi network, the solution was built an integrated system that can handle security problems on the wifi network includings, build an captive portal which requires the user to authenticate before they can access the Internet, ssl and https implementation for protect user data from outside, and also bandwidth management implementation for manage user bandwidth by using open source firewall, Pfsense with freebsd based

Keywords: Wireless hotspot, Authentication System, Bandwidth Management, Captive portal, SSL Certificate, HTTPS

1. Latar Belakang

Selama ini, keamanan jaringan *wireless* atau nirkabel 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*.

2. Dasar Teori

a. Pfsense

PfSense adalah sistem operasi untuk firewall dan mempunyai fitur yang lengkap. *Pfsense*, bila digunakan bersama dengan perangkat keras yang cocok, maka *pfsense* dapat memberikan semua fitur penting dari *firewall* komersial, diantaranya kemudahan penggunaan dan tidak terlalu menambah pengeluaran karena sifatnya yang opensource.

b. Wireless LAN

Wireless LAN atau kadang disingkat WLAN adalah sebuah sistem komunikasi data yang fleksibel yang dapat diaplikasikan sebagai ekstensi ataupun sebagai alternatif pengganti untuk jaringan LAN kabel. Wireless LAN menggunakan teknologi frekuensi radio, mengirim dan menerima data melalui media udara, dengan meminimalisasi kebutuhan akan sambungan kabel.

c. Keamanan pada wireless LAN

Umumnya dalam Wireless LAN terdapat 2 Kategori keamanan, yaitu teknik keamanan standar dan Teknik Keamanan lanjutan.

1. Teknik Keamanan Standar :
   a. *Non Broadcast SSID*, Jika ingin masuk ke dalam suatu jaringan, maka user harus memasukan SSID secara manual.
   b. *MAC Filtering*, Filtering atau penyaringan berdasarkan MAC Addres, dan dapat dikonfigurasi seperti allow (Mengizinkan) atau reject (menolak)
   c. *WEP*, Selain difungsikSSDan untuk autentikasi, juga sering digunakan untuk meng-enkripsi data yang dilewati oleh WLAN.

2. Teknik Keamanan Lanjutan :
   a. *WPA*, Evolusi dari WEP, Alogaritma Enkripsi yang jauh lebih baik dari WEP
   b. *Autentikasi* Lokal dan Terpusat
   c. *ACL* atau *Filtering*

3. Analisis dan Perancangan

Dalam proyek akhir ini dibutuhkan beberapa perangkat lunak dan perngakt keras. Tabel 3.1 berikut menjelaskan kebutuhan perangkat keras.

Tabel 3.1 Kebutuhan perangkat keras

Daftar Perangkat Keras	
Aplikasi	**Keterangan**
Laptop atau PC	AcerTravelmate
NIC (Ethernet Card) Realtek	PCI lan card up to 10/100 Mbps
Router Mikrotik RB950 2HND	Mikrotik router with wireless and usb connector, 4 ports with 1 ports for ADSL connection
Modem Huawei E173	GSM Modem, speed up to 7 Mbps
Wireless Access Point TP-LINK WA710ND	Wireless access point speed up to 150Mbps, PoE ports
Switch	Switch with 4 ports

dan Tabel 3.2 menjelaskan kebutuhan perangkat lunak yang digunakan.

Tabel 3.2 Kebutuhan perangkat lunak

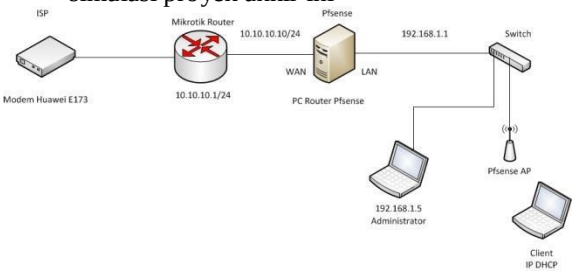
Daftar Perangkat Lunak	
Jenis	**Versi/Jenis**
Pfsense	2.2.3 / Firewall OS
Wireshark	1.7
DU Monitor	Bandwidth monitoring software / 2.3

3.1 Langkah Pengerjaan

Berikut merupakan langkah pengerjaan proyek akhir :

a. Instalasi awal Pfsense
b. Instalasi dan konfigurasi pfsense sebelum mengaktifkan fitur
c. Implementasi Captive portal
d. Implementasi ssl dan https
e. Implementasi manajemen bandwidth

Pada gambar 3.1 merupakan topologi dari simulasi proyek akhir ini



Gambar 3.1 Topologi yang akan diimplementasikan

4. Pengujian

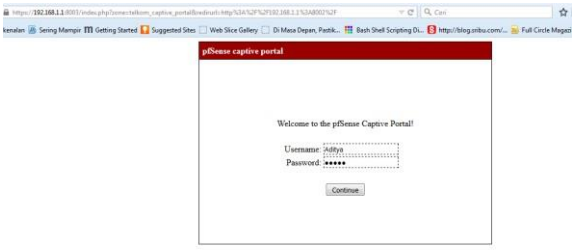
Skenario Pengujian untuk implementasi ini adalah sebagai berikut :

a. User captive portal masuk kedalam hotspot pfsense, dan akan langsung dialihkan ke halaman login dari captive portal
b. User melakukan login melalui captive portal dengan username dan password yang telah dibuat oleh admin
c. Jika user dari captive portal berhasil melakukan login maka akan langsung dialihkan oleh sistem captive portal ke halaman default dari captive portal
d. Pengujian captive portal dilakukan oleh user yang telah terdaftar dalam group pengguna captive portal.
e. Pengujian sertifikat SSL dan HTTPS dilakukan dengan memanfaatkan software wireshark untuk melakukan spoofing terhadap jaringan hotspot pfsense.
f. Pengujian SSL dan HTTPS akan dilakukan sebanyak 2 kali. Terdiri dari : pengujian pertama, sebelum penerapan SSL dan HTTPS, dan pengujian kedua sesudah penerapan SSL dan HTTPS
g. Pengujian SSL dan HTTPS dilakukan untuk mengetahui pengamanan dari SSL dan HTTPS pada username dan password dari user captive portal.

h. Pengujian manajemen bandwidth dilakukan oleh 4 user secara bersama-sama, dan dalam waktu yang sama.
i. Pengujian terdiri dari, pengukuran kecepatan melalui website speedtest secara realtime, pengukuran kecepatan download dan upload melalui web testmynet secara realtime, download file dengan ukuran yang sama, serta upload file dengan ukuran diatas 6 MB.
j. Pengujian Upload file, dimonitoring menggunakan software DU Meter
k. Pengujian manajemen bandwidth dilakukan 2 tahap yaitu sebelum dan sesudah penerapan manajemen bandwidth

4.1 Pengujian Captive portal

Dibawah ini adalah hasil dari pengujian captive portal dengan menggunakan pfsense :

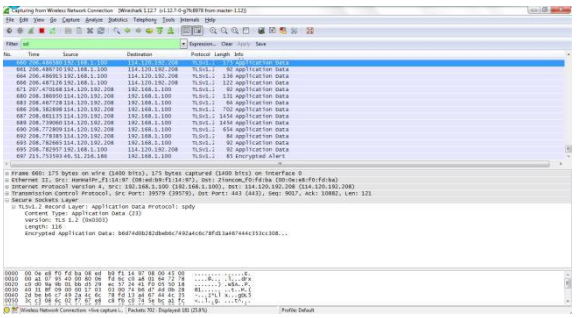


Gambar 4.1 Pengujian captive portal

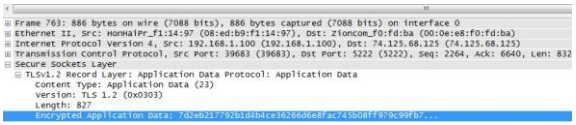
Gambar 4.2 Pengujian captive portal berhasil

4.2 Pengujian SSL dan HTTPS

Dibawah ini adalah hasil dari pengujian penerapan ssl dan https :



Gambar 4.3 Pengujian ssl dan https



Gambar 4.4 SSL dan HTTPS mengenkripsi data

4.1 Pengujian Manajemen bandwidth

Dibawah ini adalah hasil dari pengujian bandwidth, setelah penerapan dan sebelum penerapan manajemenbandwidth.

Nama user	*Kecepatan Speedtest, download dan upload*	*Kecepatan Download file melalui testmy.net*	*Kecepatan Upload file melalui testmy.net*	*Kecepatan download file*	*Kecepatan Upload file*
Adam	312 Kbps / 104 Kbps	337 Kbps	84 Kbps	40 Kbps	53,7 Kbps
Aditya	312 Kbps / 104 Kbps	331 Kbps	89 Kbps	37,6 Kbps	163 Kbps
Nugraha	374 Kbps / 102 Kbps	338 Kbps	83 Kbps	73 Kbps	43,3 Kbps
Nyoba	312 Kbps / 102 Kbps	257 Kbps	83 Kbps	40,2 Kbps	131 Kbps

Tabel 4.1 Perbandingan kecepatan sebelum manajemen bandwidth

Dibawah ini adalah hasil dari pengujian bandwidth, sebelum penerapan manajemen bandwidth :

Nama user	*Kecepatan Speedtest, download dan upload*	*Kecepatan Download file melalui testmy.net*	*Kecepatan Upload file melalui testmy.net*	*Kecepatan download file*	*Kecepatan Upload file*
Adam	148 Kbps / 84 Kbps	136 Kbps	61 Kbps	23,8 KB/s	44,3 Kbps
Aditya	164 Kbps / 62 Kbps	143 Kbps	76 Kbps	17,1 KB/s	51,4 Kbps
Nugraha	164 Kbps / 62 Kbps	144 Kbps	66 Kbps	17,1 KB/s	51,4 Kbps
Nyoba	143,36 Kbps / 62 Kbps	142 Kbps	66 Kbps	17,1 KB/s	42 Kbps

Tabel 4.2 Perbandingan kecepatan setelah manajemen bandwidth

5. Kesimpulan dan Saran

5.1 Kesimpulan

a. Berdasarkan hasil pengujian dan implementasi Proyek akhir ini, dapat diambil kesimpulan bahwa: Terbentuknya pengamanan wireless hotspot dengan sistem otentikasi captive portal menggunakan pfsense, sehingga user diwajibkan untuk melakukan login dengan

menggunakan username dan password yang telah dibuat terlebih dahulu oleh admin.

b. Tercapainya sistem pengamanan wireless hospot dengan memanfaatkan sertifikat ssl dan juga pengamanan https, Sehingga penyerang atau attacker tidak dapat membaca password dan username dari user captive portal. Yang dibuktikan dengan pengujian menggunakan wireshark.

c. Tercapainya implementasi pembatasan bandwidth bagi user yang akan menggunakan fasilitas hotspot, sehigga user dapat melakukan download dan upload, tanpa melewati batasan bandwidth yang telah ditetapkan.

5.2 Saran

Beberapa hal yang dapat dijadikan sebagai saran dalam proyek akhir ini, diantaranya adalah :

a. Penerapan captive portal dengan local user management menjadi salah satu kesulitan tersendiri bagi seorang sistem administrator dikarenakan seorang admin harus memasukan dan membuat username serta password satu persatu terhadap user yang ingin menggunakan fasilitas captive portal. Penggunaan radius server bisa menjadi solusi untuk menggantikan otentikasi dengan local user management karena tidak perlu mendaftarkan username serta password satu persatu.

b. Penerapan ssl dan sertifikat pada pengamanan http masih diperlukan proses instalasi sertifikat terhadap user, dan ini menjadi kendala karena tidak semua user mengerti akan hal tersebut. Maka dari itu penggunaan proxy bisa menjadi salah satu solusi untuk mempermudah user tanpa harus melakukan proses instalasi sertifikat pada user.

c. Implementasi pembatasan bandwidth secara keseluruhan mempengaruhi kualitas dari kecepatan internet dari ISP, dikarenakan hanya membatasi keseluruhan user secara merata. Dan tidak membatasi 1 IP ataupun mac address sehingga semua koneksi baik itu upload maupun download akan sama. Maka dari itu penggunaan traffic shaping dan limiter dengan queue bisa menjadi solusi untuk menyempurnakan sistem manajemen bandwidth untuk user pengguna hotspot.

Daftar Pustaka

[1] Williamson Matt, *pfSense 2 Cookbook : A practical, example-driven guide to configure even themost advance features of pfSense 2* . Birmingham: Packt Publishing, 2011.

[2] About pfSense . (2012) Captive Portal: [Online]. HYPERLINK : https://doc.pfsense.org/index.php/CaptivePortal [accessed June 23, 2015]

[3] Buechler M. Christoper, pf*Sense:* The Definitive Guide to the pfSense Open Source Firewall and RouterDistribution New York: pfSense, 2009.

[4] Instalasi Pfsense dan Settingan awalnya. (2011) : [Online] HYPERLINK https://forum.pfsense.org/index.php?topic=18932.0 [accessed July 12, 2015]

[5] How to setup SSL certificate[Online].(2011): HYPERLINK: https://www.sxl.net/guides/cloud-vps/pfsense/5482/ [accessed august 18, 2015]

[6] Cara Kerja dan kelebihan wireless LAN. [Online]. (2012): HYPERLINK : http://jaringankomputer.org/wireless-lan-pengertian-cara-kerja-dan-kelebihan-wireless-lan/ [accessed september 10, 2015]

[7] Wireless LAN. [Online]. (2012) : HYPERLINK: http://idkf.bogor.net/yuesbi/e-DU.KU/edukasi.net/TIK/JO8I88~F/materi4.html [accessed september 10, 2015]

[8] Traffic Shaping Guide. [Online]. (2012) : HYPERLINK: https://doc.pfsense.org/index.php/Traffic_Shaping_Guide [accessed september 15, 2015]

[9] Oktavian dwi,Ryan,*Proyek akhir:* Manajemen jaringan dengan menggunakan pfsense, studi kasus pada SMAN 1 Ciparay*: Politeknik Telkom,* 2010.