

**PERANCANGAN KEAMANAN JARINGAN HOTSPOT
MENGUNAKAN RADIUS SERVER**
(Studi Kasus : Fakultas Teknik Universitas Pasundan)

TUGAS AKHIR

Disusun sebagai salah satu syarat untuk kelulusan Program Strata 1,
di Program Studi Teknik Informatika, Universitas Pasundan Bandung

oleh :

Tanto Rianto
Nrp. 12.304.0006



**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG
DESEMBER 2016**

DAFTAR ISI

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR	i
ABSTRAK	ii
ABSTRACT	iii
KATA PENGANTAR.....	iv
DAFTAR ISI.....	vi
DAFTAR ISTILAH	vii
DAFTAR TABEL	x
DAFTAR GAMBAR	xi
DAFTAR LAMPIRAN	xiii
BAB 1 PENDAHULUAN	1-1
1.1. Latar Belakang.....	1-1
1.2. Identifikasi Masalah	1-1
1.3. Tujuan Tugas Akhir.....	1-2
1.4. Lingkup Tugas Akhir	1-2
1.5. Metodologi Tugas Akhir	1-2
1.6. Sistematika Penulisan Tugas Akhir.....	1-4
BAB 2 LANDASAN TEORI.....	2-1
2.1. Penelitian Terdahulu.....	2-1
2.2. Perancangan.....	2-2
2.3. Sistem Keamanan Jaringan Hotspot	2-2
2.4. Hotspot (WiFi).....	2-2
2.4.1 Definisi Hotspot	2-2
2.4.2 Kelebihan Kekurangan Jaringan Hotspot.....	2-3
2.4.3 Ancaman Pada Keamanan Jaringan Hotspot.....	2-3
2.4.4 Tujuan Dalam Keamanan Jaringan	2-4
2.5. Remote Autentifikasi Dial in User Service (Radius).....	2-5
2.5.1 Prinsip Kerja Radius.....	2-5
2.5.2 Kelebihan dan Kelemahan RADIUS.....	2-8
2.5.3 Protokol AAA	2-9
2.6. Pemfilteran alamat MAC.....	2-12

2.7. Mikrotik.....	2-13
2.7.1. Mikrotik Hotspot.....	2-14
2.8 Captive Portal.....	2-14
2.9. Metode Pengembangan Sistem	2-14
BAB 3 SKEMA PENELITIAN	3-1
3.1. Rancangan Penelitian.....	3-1
3.2. Rencana Analisis.....	3-3
3.3. Analisis.....	3-4
3.3.1. Manfaat Keamanan Jaringan Hotspot	3-4
3.3.2. Kerangka Berfikir Teoritis	3-5
3.4. Tempat Penelitian dan Objek Penelitian	3-6
3.4.1. Tempat Penelitian.....	3-6
3.4.2. Objek Penelitian	3-6
3.5. Analisis Keadaan Jaringan FT-Unpas	3-7
3.5.1. Analisis Sistem Keamanan Jaringan	3-9
3.5.2. Analisis Aset	3-9
3.5.3. Topologi Jaringan FT-UNPAS	3-10
3.5.4. Analisis Sebelum Penerapan Captive Portal	3-11
3.5.5. Perbandingan Sistem Tanpa Captive Portal dan dengan Captive Portal.....	3-11
3.5.6. Analisis Sistem Koneksi dan Autentikasi tanpa Captive Portal.....	3-11
3.5.7. Masalah Yang Dihadapi.....	3-12
3.5.8. Penanganan Masalah.....	3-13
3.6. Usulan Penggunaan Sistem Login Otentikasi	3-13
3.6.1. Usulan Model Otentikasi Pengguna.....	3-13
3.6.2. Kebutuhan Sistem	3-14
3.7. Perancangan	3-14
3.7.1 Perangkat Penelitian.....	3-14
3.7.1 Perancangan Fisik	3-15
3.8. Kesimpulan Sementara.....	3-17
BAB 4 IMPLEMENTASI DAN PENGUJIAN	4-1
4.1. Implementasi	4-1
4.1.1 Implementasi Kebutuhan Perangkat Lunak	4-1
4.1.2 Perancangan Logik.....	4-1

4.1.3	Implementasi RADIUS Server	4-4
4.1.4	Membuat Halaman Login (Captive Portal) Radius Server.....	4-14
4.1.5	Monitoring Sistem RADIUS Server.....	4-15
4.2.	Pengujian Sistem Sistem RADIUS Server	4-16
4.2.1.	Pengujian Sistem RADIUS Dengan Sniffing.....	4-17
4.3.	Evaluasi Sistem Yang Telah Dibangun	4-18
BAB 5 KESIMPULAN DAN SARAN.....		5-1
5.1.	Kesimpulan.....	5-1
5.2.	Saran.....	5-1
DAFTAR PUSTAKA		5-1

DAFTAR ISTILAH

Tabel i Daftar Istilah

No	DAFTAR ISTILAH	KETERANGAN
1	Wireless	adalah jika dari arti katanya dapat diartikan "tanpa kabel", yaitu melakukan suatu hubungan telekomunikasi menggunakan gelombang elektromagnetik sebagai pengganti media kabel
2	TCP/IP	TCP (Transmission Control Protocol) dan IP (Internet Protocol) sebagai sekelompok protokol yang mengatur komunikasi data dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan internet yang akan memastikan pengiriman data sampai ke alamat yang dituju.
3	UDP	UDP adalah kependekan dari User Datagram Protocol merupakan bagian dari internet protocol. Dengan UDP, aplikasi komputer dapat mengirimkan pesan kepada komputer lain dalam jaringan lain tanpa melakukan komunikasi awal.
4	NAS	Network Attached Storage (NAS) adalah sebuah server dengan sistem operasi yang dikhususkan untuk melayani kebutuhan berkas data. NAS dapat di akses langsung melalui jaringan area lokal dengan protokol seperti TCP/IP
5	Authentication	Proses membuktikan siapa anda (identitas) inilah yang disebut authentication. Bila authentication berhasil, maka akan terjalin hubungan trust antara pemberi layanan dan pengguna layanan.
6	Authorization	proses menentukan apa sajakah layanan yang bisa dinikmati pengguna yang telah jelas identitasnya (authenticated user).
7	Accounting	merupakan proses yang dilakukan oleh NAS dan AAA server yang mencatat semua aktivitas user dalam jaringan, seperti kapan user mulai menggunakan jaringan, kapan user mengakhiri koneksinya dengan jaringan, berapa lama user menggunakan jaringan, berapa banyak data yang diakses user dari jaringan, dan lain sebagainya.
8	RFC 2685 dan RFC 2866	Sebuah dokumen Request for Comments (RFC) adalah salah satu dari seri dokumen informasi dan standar Internet bernomor yang diikuti secara luas oleh perangkat lunak untuk digunakan dalam jaringan, Internet dan beberapa sistem operasi jaringan, mulai dari Unix, Windows, dan Novell NetWare
9	<i>Challenge / Response</i>	Authenticator membuat sebuah frame yang dinamakan challenge dan dikirimkan ke initiator. Frame ini berisi text sederhana yang disebut challenge text. Response initiator menggunakan password untuk melakukan proses encrypt pada challenge text
10	<i>Succes or Failure</i>	Proses pencocokan pesan yang di encrypt tersebut dengan challenge text yang di encrypt dengan password yang sama. Jika hasil encrypt initiator sama dengan hasil encrypt authenticator, maka authenticator menyatakan proses otentikasi sukses, sebaliknya jika tidak ditemukan kecocokan maka proses otentikasi failure

DAFTAR TABEL

Tabel i Daftar Istilah	i
Tabel 2. 1 Penelitian Terdahulu	2-1
Tabel 3. 1 Detail Skema Analisis.....	3-4
Tabel 3. 2 Ssid Jaringan FT-Unpas.....	3-7
Tabel 3. 3 Analisis Aset	3-9
Tabel 3. 4 Analisis Resiko	3-10
Tabel 3. 5 Perbandingan Captive Portal.....	3-11
Tabel 3. 6 Hasil Analisis Jaringan Hotspot FT-Unpas.....	3-12
Tabel 3. 7 Perangkat Keras	3-15
Tabel 3. 8 Perangkat Lunak	3-15
Tabel 4. 1 Perangkat lunak yang digunakan	4-1
Tabel 4. 2 List IP Address.....	4-6

DAFTAR GAMBAR

Gambar 1. 1 Metodologi Tugas Akhir	1-3
Gambar 2. 1 Autentikasi antara Nas dengan Radius.....	2-6
Gambar 2. 2 Struktur Paket data tidak adanya Radius.....	2-7
Gambar 2. 3 Struktur paket data RADIUS.....	2-7
Gambar 2. 4 Arsitektur Jaringan AAA	2-9
Gambar 2. 5 Proses Autentikasi.....	2-10
Gambar 2. 6 Proses di mulainya pencatatan	2-12
Gambar 2. 7 Proses diakhirinya pencatatan.....	2-12
Gambar 2.8 Pemfilteran Alamat MAC dengan menggunakan RADIUS.....	2-13
Gambar 2. 9 The Security Policy Development Life Cycle (Goldman, 2004)	2-15
Gambar 3. 1 Kerangka Tugas Akhir	3-2
Gambar 3. 2 Skema Analisis.....	3-3
Gambar 3. 3 Struktur Organisasi.....	3-6
Gambar 3. 4 Kondisi Jaringan Saat ini	3-8
Gambar 3. 5 Ping paket data jaringan Hotspot FT-Unpas	3-8
Gambar 3. 6 User yang terhubung Hotspot FT-Unpas.....	3-9
Gambar 3. 7 Topologi Jaringan FT-UNPAS.....	3-10
Gambar 3. 8 Skema Jaringan Saat Ini	3-11
Gambar 3. 9 Hotspot tanpa Autentikasi	3-12
Gambar 3. 10 Rancangan Topologi Radius Server.....	3-16
Gambar 3. 11 Acces Point dan Switch pada Lingkungan Ujicoba	3-16
Gambar 3. 12 Acces Point sebagai Hotspot Ujicoba	3-16
Gambar 3. 13 Router Mikrotik RB750GL.....	3-16
Gambar 4. 1 Use Case Diagram User	4-1
Gambar 4. 2 Use Case Diagram Admin.....	4-2
Gambar 4. 3 Flowchart Login User	4-3
Gambar 4. 4 Flowchart Login Administrator.....	4-4
Gambar 4. 5 Tampilan Awal Winbox	4-5
Gambar 4. 6 Remote Melalui Winbox	4-5
Gambar 4. 7 Interface Yang Dibangun	4-6
Gambar 4. 8 IP Address	4-7
Gambar 4. 9 IP Pool.....	4-7
Gambar 4. 10 DHCP Server.....	4-8
Gambar 4. 11 DHCP Network	4-8
Gambar 4. 12 Konfigurasi NAT	4-8
Gambar 4. 13 Konfigurasi Routing.....	4-9

Gambar 4. 14 Tampilan Routing.....	4-9
Gambar 4. 15 Package List.....	4-10
Gambar 4. 16 Setting Radius Server	4-10
Gambar 4. 17 Konfigurasi Hotspot Server Profil.....	4-11
Gambar 4. 18 Konfigurasi Hotspot User Profiles	4-11
Gambar 4. 19 Form Login User Manager	4-13
Gambar 4. 20 Tampilan Utama User Manager	4-13
Gambar 4. 21 Daftar User Pengguna Hotspot	4-14
Gambar 4. 22 Tampilan Standar Halaman Login Hotspot.....	4-14
Gambar 4. 23 Tampilan Login Hotspot (Captive Portal).....	4-15
Gambar 4. 24 Monitoring User Melalui User Manger	4-15
Gambar 4. 25 Monitoring User Melalui Winbox	4-16
Gambar 4. 26 User Melakukan Login	4-17
Gambar 4. 27 Status User Berhasil	4-17
Gambar 4. 28 Sniffing Login Hotspot Dengan Wireshark.....	4-18

DAFTAR LAMPIRAN

Gambar A. 1 Surat Izin Penelitian Tugas Akhir	A-1
Gambar B. 1 Berita Acara Wawancara	B-1
Gambar B. 2 Berita Acara Wawancara (2).....	B-2
Gambar B. 3 Berita Acara Wawancara (3).....	B-3