

**SIMULASI IMPLEMENTASI PFSENSE SEBAGAI *CAPTIVE PORTAL*
SISTEM AUTENTIKASI DAN MANAJEMEN *BANDWIDTH* PADA
WIRELESS HOTSPOT BERBASIS FREEBSD**

SKRIPSI



disusun oleh

Ade Ristia Zulkha Rindayanto

15.11.9145

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

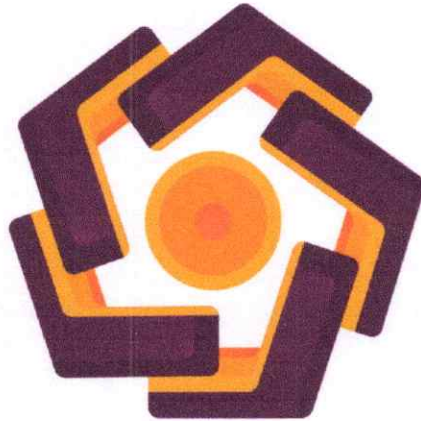
2019



**SIMULASI IMPLEMENTASI PFSense SEBAGAI *CAPTIVE PORTAL*
SISTEM AUTENTIKASI DAN MANAJEMEN *BANDWIDTH* PADA
WIRELESS HOTSPOT BERBASIS FREEBSD**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Ade Ristia Zulkha Rindayanto

15.11.9145

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019**

PERSETUJUAN

SKRIPSI

**SIMULASI IMPLEMENTASI PFSense SEBAGAI CAPTIVE
PORTAL SISTEM AUTENTIKASI DAN MANAJEMEN
BANDWIDTH PADA WIRELESS HOTSPOT BERBASIS FREEBSD**

yang dipersiapkan dan disusun oleh

Ade Ristia Zulkha Rindayanto

15.11.9145

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 22 Juli 2019

Dosen Pembimbing,


Sudarmawan, S.T., M.T.

NIK. 190302035

PENGESAHAN

SKRIPSI

SIMULASI IMPLEMENTASI PFSense SEBAGAI CAPTIVE PORTAL SISTEM AUTENTIKASI DAN MANAJEMEN BANDWIDTH PADA WIRELESS HOTSPOT BERBASIS FREEBSD

yang dipersiapkan dan disusun oleh

Ade Ristia Zulkha Rindayanto

15.11.9145

telah dipertahankan di depan Dewan Penguji
pada tanggal 15 Agustus 2019

Susunan Dewan Penguji

Nama Penguji

Sudarmawan, S.T., M.T.
NIK. 190302035

Eli Pujastuti, M.Kom
NIK. 190302227

Sumarni Adi, S.Kom, M.Cs
NIK. 190302256

Tanda Tangan



Skrripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 11 September 2019

DEKAN FAKULTAS ILMU KOMPUTER



Krisnawati, S.Si, M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertandatangan di bawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan ini dalam skripsi ini tidak terdapat karya yang pernah di ajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta 14 September 2019



Ade Ristia Zulkha R

NIM. 15.11.9145



MOTO

“Karena sesungguhnya sesudah kesulitan itu ada kemudahan.”

(QS. Alam Nasyroh: 5)

“Dan hanya kepada Tuhanmulah hendaknya kamu berharap”

(Q.S. Al-Insyirah: 8)



PERSEMBAHAN

Yang utama dari segalanya, sembah sujud dan syukur kepada Allah SWT., atas anugerah cinta dan kasih sayang-Nya telah memberikan kesehatan, kekuatan, umur dan ilmu pengetahuan. Serta atas kemudahan dan kelancaran yang diberikan akhirnya skripsi ini dapat diselesaikan.

Dengan bangga dan penuh cinta Saya persembahkan karya sederhana ini kepada mereka orang-orang tercinta:

1. Kepada kedua orang tua peneliti, Ayah Mukhlis Rindayanto dan Ibu Rosita. Terimakasih untuk selalu memberi motivasi, dukungan finansial, dan tentu doa yang tidak pernah berhenti disetiap sujudmu. Untuk adik kandung satu-satunya penulis, Ridho Riskia Putra yang selalu mendoakan dan menghibur. Serta semua keluarga besar yang selalu mendoakan dan memberi motivasi.
2. Hernila. Terimakasih untuk tidak pernah bosan memberi semangat dan dorongan untuk menyelesaikan skripsi ini. Terimakasih untuk kasih sayang dan kesabarannya selama ini.
3. Kepada Bapak Sudarmawan S.T., M.T selaku dosen pembimbing penulis, terima kasih atas segala waktu, motivasi, bimbingan serta nasehatnya.
4. Guru dan seluruh dosen yang sudah membagikan ilmu yang bermanfaat kepada saya.
5. Terimakasih kepada semua rekan kelas TI-10 khususnya sahabat kontrakan yang selalu melarang untuk tidak mengerjakan skripsi.

6. UNISBA, Terimakasih kepada Gus Susmanto dan rekan-rekan di UNISBA yang selalu memberi pengarahan nasehat dan doa.
7. Serta semua pihak yang tidak dapat disebutkan satu per satu, terimakasih atas partisipasinya.

Yogyakarta 14 September 2019



Ade Ristia Zulkha R

KATA PENGANTAR

Alhamdulillah robbil'alamin, puji syukur peneliti panjatkan kehadiran Allah SWT atas segala karunia dan rahmatnya sehingga peneliti dapat menyelesaikan skripsi ini dengan judul “**Simulasi Implementasi Pfsense Sebagai *Captive portal* Sistem Autentikasi Dan Manajemen *Bandwidth* Pada *Wireless Hotspot* Berbasis *Freebsd*”**. Skripsi ini merupakan salah satu bentuk persyaratan kelulusan jenjang Program Strata satu (S1) jurusan Informatika pada Universitas Amikom Yogyakarta.

Dalam pengerjaan skripsi ini telah melibatkan banyak pihak yang sangat membantu dan memberikan bimbingan, nasihat, dan doa. Yang akhirnya peneliti dapat menyelesaikan skripsi ini dengan baik dan maksimal. Oleh karena itu, dengan segala kerendahan hati dan ketulusan, penulis mengucapkan terima kasih kepada:

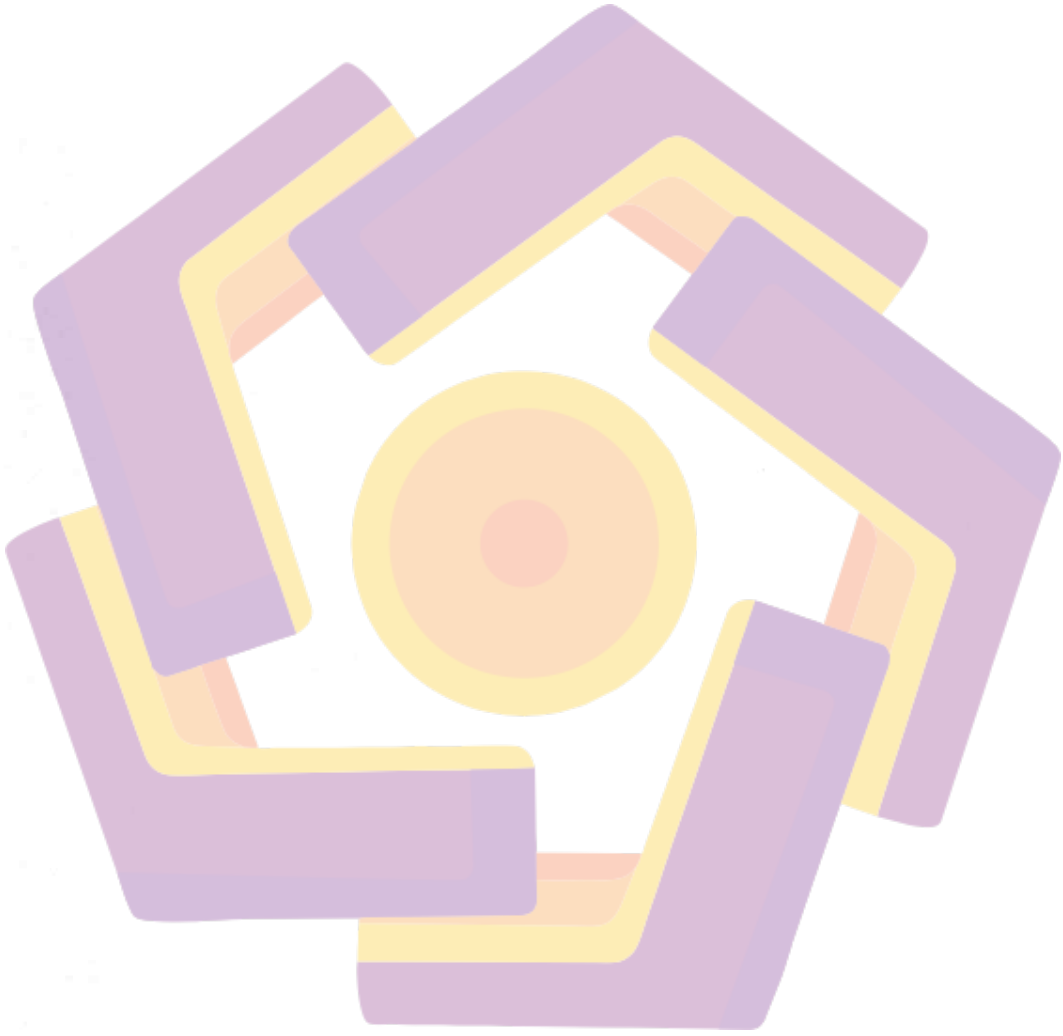
1. Bapak Prof. Dr. M. Suyanto, MM, selaku Ketua Universitas Amikom Yogyakarta.
2. Sudarmaan S.T., M.T. selaku Dosen pembimbing.
3. Ibu Mardhiya Hayaty, S.T., M.Kom selaku Dosen wali peneliti selama menempuh Pendidikan Strata 1 jurusan Informatika pada Universitas Amikom Yogyakarta.
4. Bapak dan Ibu dosen Universitas Amikom Yogyakarta yang telah memberi dan mengajarkan Ilmunya kepada peneliti.

DAFTAR ISI

JUDUL	ii
PERSETUJUAN	iii
PENGESAHAN	iv
PERNYATAAN	v
MOTO	vi
PERSEMBAHAN	vii
KATA PENGANTAR	ix
DAFTAR ISI	x
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
INTISARI	xvii
<i>ABSTRACT</i>	xviii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	4
1.4 Tujuan Penelitian	5
1.5 Manfaat Penelitian	5
1.6 Metode Penelitian	5
1.6.1 Studi Pustaka	6
1.6.2 Metode Perancangan	6
1.6.3 Metode Implementasi	6
1.6.4 Pengujian Sistem	6
1.7 Sistematika Penulisan	7
BAB II LANDASAN TEORI	8
2.1 Tinjauan Pustaka	8
2.2 Dasar Teori	11
2.2.1 Pengertian Jaringan Komputer	11
2.2.2 Keamanan Jaringan	15

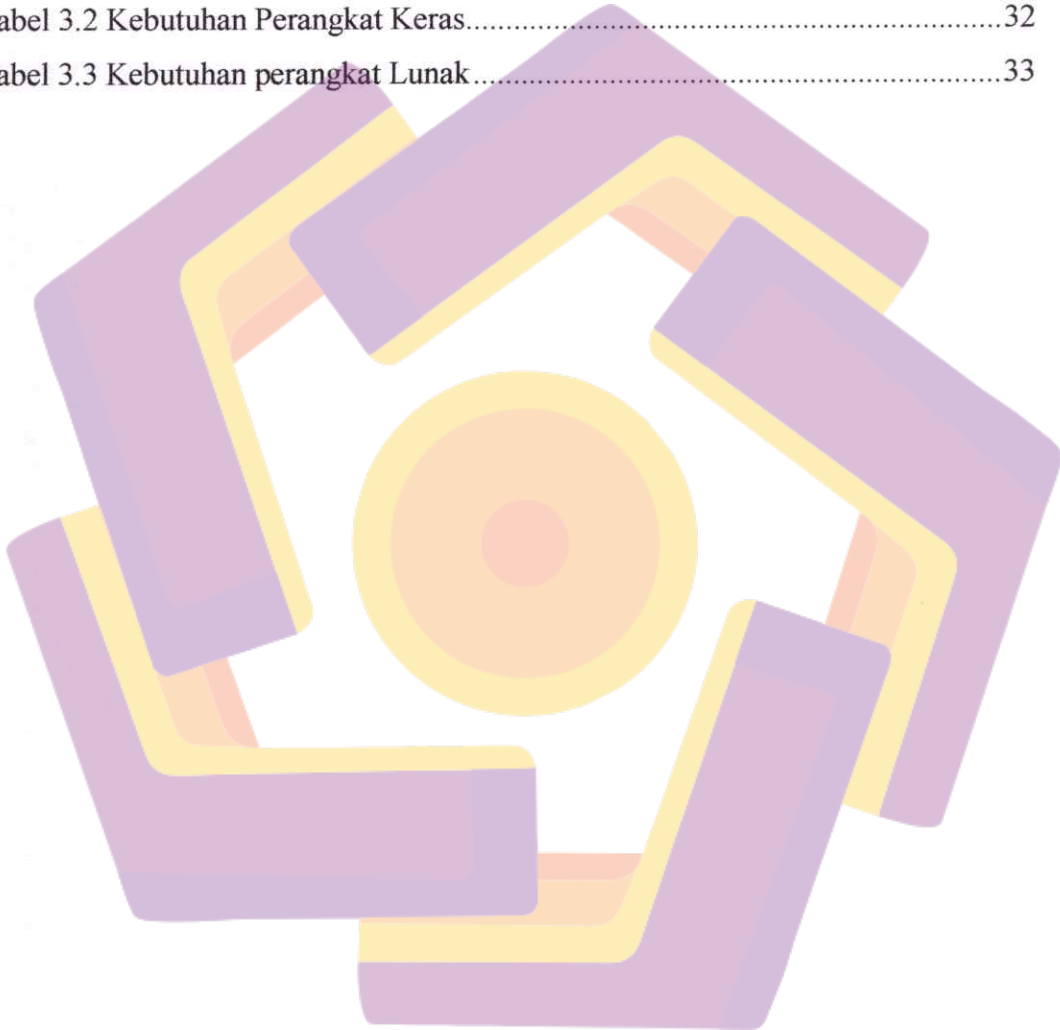
2.2.3	<i>Authentication</i>	15
2.2.4	<i>Captive Portal</i>	16
2.2.5	Pfsense	17
2.2.6	Router.....	19
2.2.7	<i>Wireless</i>	21
2.2.8	<i>Intrusion Detection System (IDS)</i>	22
2.2.9	Snort.....	24
2.2.10	<i>Distributed Denial of Service (DDoS)</i>	25
BAB III METODE PENELITIAN		28
3.1	Gambaran Umum	28
3.2	Arsitektur Jaringan.....	29
3.3	Diagram Alur Penelitian.....	30
3.4	Alat dan Bahan.....	32
3.4.1	Perangkat Keras (Hardware).....	32
3.4.2	Perangkat Lunak (Software).....	33
3.5	Sistem Kerja.....	33
3.6	Skenario Pengujian.....	34
3.6.1	Pengujian Hak Akses User Captive Portal.....	35
3.6.2	Pengujian Ketahanan Captive Portal	36
3.6.3	Pengujian Snort IDS (Intrusion Detection System).....	38
3.6.4	Pengujian <i>Bandwidth</i> Terhadap User Captive Portal.....	41
BAB IV IMPLEMENTASI DAN PENGUJIAN.....		42
4.1	Implementasi Sistem.....	42
4.1.1	Implementasi Captive Portal.....	42
4.1.2	Implementasi Snort IDS.....	46
4.1.3	Implementasi Manajemen <i>Bandwidth</i>	49
4.2	Pengujian Sistem.....	50
4.2.1	Pengujian Hak Akses User Captive Portal.....	50
4.2.2	Pengujian Ketahanan Captive Portal	52
4.2.3	Pengujian Snort IDS (Intrusion Detection System).....	56
4.2.4	Pengujian <i>Bandwidth</i>	63

4.3 Evaluasi64
BAB V PENUTUP66
5.1 Kesimpulan.....66
5.2 Saran.....66
DAFTAR PUSTAKA68



DAFTAR TABEL

Tabel 2.1 Perbedaan Penelitian.....	9
Tabel 2.2 Perbedaan Penelitian Lanjutan.....	10
Tabel 2.3 Kelebihan dan Kekurangan Pfsense	18
Tabel 3.1 IP Address.....	29
Tabel 3.2 Kebutuhan Perangkat Keras.....	32
Tabel 3.3 Kebutuhan perangkat Lunak.....	33

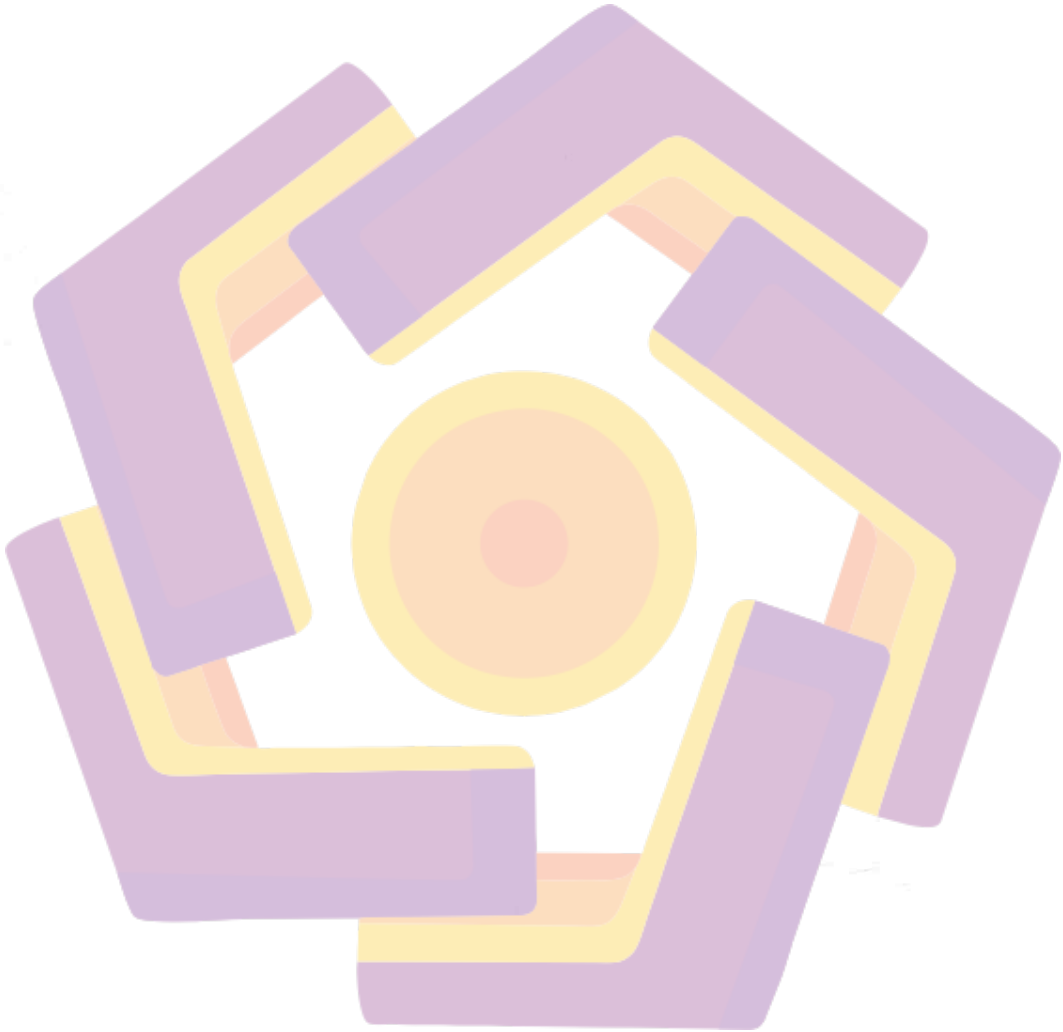


DAFTAR GAMBAR

Gambar 2.1 Topologi Bus.....	13
Gambar 2.2 Topologi Ring.....	13
Gambar 2.3 Topologi Star.....	14
Gambar 2.4 Topologi Tree.....	14
Gambar 2.5 Captive Portal.....	17
Gambar 2.6 Teknik Serangan DdoS.....	27
Gambar 3.1 Topologi Jaringan.....	29
Gambar 3.2 Diagram Alur Penelitian.....	31
Gambar 3.3 Sistem Kerja.....	33
Gambar 3.4 Skenario Pengujian.....	34
Gambar 3.5 Halaman Login.....	35
Gambar 3.6 Login Gagal.....	36
Gambar 3.7 Memilih Interfaces.....	37
Gambar 3.8 Proses Sniffing.....	37
Gambar 3.9 Serangan menggunakan Hping3.....	39
Gambar 3.10 Serangan menggunakan LOIC.....	40
Gambar 4.1 Range DHCP.....	42
Gambar 4.2 Domain Name Captive Portal.....	43
Gambar 4.3 DNS Forwarder.....	43
Gambar 4.4 Konfigurasi Captive Portal.....	44
Gambar 4.5 Pembuatan Sertifikat SSL.....	45
Gambar 4.6 Penambahan Sertifikat SSL.....	45
Gambar 4.7 Host Overrides.....	46
Gambar 4.8 Penerapan SSL dan HTTPS pada Captive Portal.....	46
Gambar 4.9 Instalasi Snort.....	46
Gambar 4.10 Pembuatan Akun Snort.....	47
Gambar 4.11 Menetapkan Interface Snort.....	47
Gambar 4.12 Snort Pada Interface LAN.....	47
Gambar 4.13 Pengaturan Rule Pada Snort.....	48
Gambar 4.14Tampilan <i>Alert</i> Snort.....	48

Gambar 4.15 Limit Upload.....	49
Gambar 4.16 Limit Download.....	49
Gambar 4.17 Rule Untuk Jalur LAN.....	50
Gambar 4.18 Proses Login.....	51
Gambar 4.19 Login Berhasil.....	51
Gambar 4.20 User Aktif.....	51
Gambar 4.21 Pengaturan Interface.....	52
Gambar 4.22 Proses Berjalan.....	52
Gambar 4.23 Proses Login.....	53
Gambar 4.24 Proses Spoffing <i>Username</i> dan <i>Password</i>	53
Gambar 4.25 Interface.....	54
Gambar 4.26 Proses IP Forwarding dan Mengkonfigurasi Tabel IP.....	54
Gambar 4.27 Proses Mencari IP <i>Gateway</i> dan IP Target.....	55
Gambar 4.28 Proses Spoffing.....	55
Gambar 4.29 Proses SSLStrip.....	55
Gambar 4.30 Proses Login.....	56
Gambar 4.31 Hasil Spoffing.....	56
Gambar 4.32 Kondisi Awal PC Client.....	57
Gambar 4.33 Kondisi Awal PC Router.....	57
Gambar 4.34 Serang DOS Dengan Hping Kali Linux.....	57
Gambar 4.35 Capture Paket Pada Wireshark.....	58
Gambar 4.36 Kondisi Akhir PC Client.....	59
Gambar 4.37 Kondisi Akhir PC Router.....	59
Gambar 4.38 Dampak Serangan.....	59
Gambar 4.39 Hasil <i>Alert</i>	60
Gambar 4.40 Kondisi Awal PC Client.....	61
Gambar 4.41 Kondisi Awal PC Router.....	61
Gambar 4.42 Serang DOS Dengan LOIC.....	61
Gambar 4.43 Capture Paket Pada Wireshark.....	62
Gambar 4.44 Kondisi Akhir PC Client.....	62
Gambar 4.45 Kondisi Akhir PC Router.....	63

Gambar 4.46 Hasil *Alert*63
Gambar 4.47 Kecepatan Sebelum Menejemen *Bandwidth*.....64
Gambar 4.48 Kecepatan Setelah Menejemen *Bandwidth* Cilen 164
Gambar 4.49 Kecepatan Setelah Menejemen *Bandwidth* Cilen 264



INTISARI

Pada saat ini, jaringan komputer nirkabel, atau yang lebih dikenal dengan *Wireless* adalah salah satu teknologi yang sekarang banyak digunakan. Namun perlu diketahui celah keamanan pada jaringan masih rentan terhadap pencurian data hak akses seperti membobol *username* dan *password* pada hotspot. Contoh lain adalah serangan *DOS (Denial Of Service)* bisa dikenal dengan sebagai tindak kejahatan dengan memanfaatkan serangan terhadap *server* yang akan menghabiskan *resource*.

Dari masalah yang ada penelitian ini menerapkan mekanisme *Captive Portal*, *Snort IDS (Intrusion Detection System)* dan Manajemen *Bandwidth* menggunakan Router *PfSense*.

Hasil dari penelitian ini adalah penerapan *Captive portal* dilengkapi dengan pengamanan *SSL* dan *HTTPS* dan pengamanan *Snort IDS (Intrusion Detection System)* untuk memberikan *alert* apabila terjadi serangan *DOS (Denial Of Service)* serta penerapan Manajemen *Bandwidth*. Melalui sistem ini, diharapkan dapat menjadi solusi untuk keamanan bagi pengguna jaringan hotspot.

Kata Kunci: *Captive Portal*, *DOS (Denial Of Service)*, *Snort IDS (Intrusion Detection System)*, *Bandwidth*.

ABSTRACT

At this time, Wireless computer networks, or better known as Wireless are one of the technologies that are now widely used. But keep in mind that security gaps in the network are still vulnerable to theft of data access rights such as breaking into usernames and passwords at the hotspot. Another example is a DOS attack (Denial of Service) can be known as a crime by exploiting attacks on servers that will use up resources.

From the problem, this research applies the Captive portal mechanism, Snort IDS (Intrusion Detection System) and Bandwidth Management using PfSense Router.

The results of this study are the application of a Captive portal equipped with SSL and HTTPS security and Snort IDS (Intrusion Detection System) security to provide alert in the event of a DOS (Denial of Service) attack and Bandwidth Management application. Through this system, it is expected to be a solution for security for hotspot network users.

Keywords: *Captive Portal, DOS (Denial Of Service), Snort IDS (Intrusion Detection System), Bandwidth.*

