

DAFTAR ISI

KATA PENGANTAR.....	i
ABSTRAK.....	iii
ABSTRACT.....	iv
DAFTAR ISI	v
DAFTAR GAMBAR.....	vii
DAFTAR TABEL	ix
DAFTAR LAMPIRAN.....	x
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	1
1.3 Tujuan	2
1.4 Batasan Masalah.....	2
1.5 Definisi Operasional.....	3
1.6 Metode Pengerjaan	4
1.7 Jadwal Pengerjaan	5
BAB 2 TINJAUAN PUSTAKA.....	6
2.1 <i>Firewall</i>	6
2.2 <i>Intrusion Prevention System (IPS)</i>	6
2.3 <i>IPFire</i>	7
2.4 <i>Intrusion Detection System (IDS)</i>	8
2.5 <i>Demilitarised Zone (DMZ)</i>	8
2.6 <i>URL Filtering</i>	8
2.7 <i>Denial Of Service (DoS Attack)</i>	9
2.8 <i>Port Scanning</i>	9
2.9 <i>Brute Force Attack</i>	10
2.10 Mikrotik Router OS	10
BAB 3 ANALISIS DAN PERANCANGAN	11
3.1 ANALISIS.....	11
3.1.1 Gambaran Sistem Saat Ini	11

3.1.2	Topologi Sistem	11
3.1.3	Cara Kerja Sistem	12
3.1.4	Analisis Kebutuhan Sistem	12
3.2	PERANCANGAN.....	13
3.2.1	Gambaran Sistem Usulan.....	13
3.2.2	Topologi Sistem.....	13
3.2.3	Cara Kerja Sistem Usulan	14
3.2.4	Spesifikasi Sistem	14
	BAB 4 IMPLEMENTASI DAN PENGUJIAN	16
4.1	Implementasi	16
4.2	Langkah Pengerjaan.....	16
4.2.1	Instalasi IPFire 2.19 core 111.....	16
4.2.2	Konfigurasi Jaringan pada Mikrotik <i>Router OS</i>	22
4.2.3	Konfigurasi Layanan <i>Server</i> pada <i>Ubuntu Server 16.10</i>	25
4.2.4	Konfigurasi IDS dan IPS pada IPFire.....	32
4.3	Pengujian	36
4.3.1	Pengujian <i>Port Scanning</i>	36
4.3.2	Pengujian <i>Denial of Service (DoS)</i>	37
4.3.3	Pengujian <i>SSH Brute Force Attack</i>	39
4.3.4	Pengujian <i>Url-Filter</i>	41
4.4	Skenario Pengujian	43
	BAB 5 KESIMPULAN DAN SARAN	44
5.1.	Kesimpulan	44
5.2.	Saran	44
	DAFTAR PUSTAKA	45
	LAMPIRAN.....	46