

DAFTAR ISI

LEMBAR PENGESAHAN TUGAS AKHIR	ii
LEMBAR PENGESAHAN PEGUJI SIDANG	iii
LEMBAR PERNYATAAN KEASLIAN	iv
KATA PENGANTAR	v
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL	xv
LAMPIRAN	xvi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	3
1.3 Tujuan Tugas Akhir	3
1.4 Manfaat Tugas Akhir	4
1.5 Lingkup Tugas Akhir	4
1.6 Sistematika Penulisan	5
BAB II LANDASAN TEORI	6
2.1 Perangkat Keamanan Jaringan Komunikasi Data	6
2.1.1 <i>Traditional Firewal</i>	6
2.1.2 <i>Next Generation Firewall (NGFW)</i>	7
2.2 Metode Serangan Pada Jaringan Komunikasi Data	7
2.2.1 <i>Distributed Denial of Service (DDOS)</i>	8
2.2.2 Jenis – Jenis <i>Malware</i> Pada Komputer	9
2.2.2.1 <i>Virus</i>	9
2.2.2.1 <i>Spyware</i>	9
2.2.2.1 <i>Trojan</i>	10
2.3 <i>Software Development Life Cycle (SDLC) – Waterfall Model</i>	10
2.4 <i>PIECES</i>	11

BAB III ANALISA SISTEM BERJALAN	14
3.1 Profil Perusahaan	14
3.2 Visi dan Misi Perusahaan	15
3.3 Struktur Organisasi Perusahaan	15
3.4 Analisa Data	15
3.4.1 <i>Requirement Analysis</i>	15
3.4.1.1 Topologi Jaringan Berjalan	15
3.4.1.2 Identifikasi Masalah Menggunakan Metode <i>PIECES</i>	16
3.4.2 <i>System Design</i>	17
3.4.2.1 Spesifikasi Kebutuhan.....	17
3.4.2.2 Perangkat Untuk Uji Coba Serangan	19
3.4.2.2.1 Perangkat Lunak Untuk Uji Coba Serangan	20
3.4.2.2.2 Perangkat Keras Untuk Uji Coba Serangan.....	20
3.4.2.3 Topologi Jaringan Usulan	20
3.4.2.4 <i>Flow Chart</i> Uji Coba Serangan.....	21
3.4.2.5 Rancangan Konfigurasi <i>Next Generation Firewall</i>	21
3.4.2.6 Metode Uji Coba <i>Firewall</i>	22
BAB IV PEMBAHASAN.....	23
4.1 Perbedaan <i>Traditional Firewall</i> dan <i>NGFW</i>	23
4.1.1 Perbandingan Spesifikasi <i>Hardware</i> Kedua <i>Firewall</i>	23
4.1.2 Perbandingan Fitur <i>Firewall</i>	23
4.2 Identifikasi Aset	24
4.3 Konfigurasi <i>Mikrotik RB1100</i> dan <i>NGFW Checkpoint 4600</i>	25
4.3.1 Instalasi <i>VMware Workstation 12 Pro</i>	25
4.3.2 Konfigurasi <i>Mikrotik RB1100</i>	30
4.3.3 Konfigurasi <i>NGFW Checkpoint 4600</i>	34
4.4 Metode Serangan	45
4.4.1 Serangan <i>DDOS – UDP Flooding</i>	45
4.4.2 Serangan <i>wannacry ransomware</i>	47
4.5 Hasil Uji Coba Serangan.....	47
4.5.1 Hasil Uji Coba Serangan <i>DDOS – UDP Flooding</i>	47
4.5.2 Hasil Uji Coba Serangan <i>wannacry ransomware</i>	53

4.6 Hasil Pengujian Yang Diperoleh	55
4.7 Rekapitulasi <i>Benefit</i> yang Diperoleh.....	56
BAB V SIMPULAN DAN SARAN.....	57
5.1 Simpulan	57
5.2 Saran	57
DAFTAR PUSTAKA	59