

DAFTAR ISI

LEMBAR JUDUL	ii
LEMBAR PENGESAHAN TUGAS AKHIR	iii
LEMBAR PENGESAHAN PENGUJI SIDANG	iv
LEMBAR PERNYATAAN KEASLIAN MATERI	v
ABSTRAK	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR GAMBAR	xiv
DAFTAR TABEL	xvi
BAB I PENDAHULUAN	1
1.1. Latar Belakang Masalah	2
1.2. Perumusan Masalah	2
1.3. Batasan Masalah	2
1.4. Tujuan dan Manfaat	3
1.5. Metode Penelitian	3
1.6. Sistematika Penulisan	4
BAB II LANDASAN TEORI	5
2.1. Pengertian Jaringan Komputer	5
2.2. Jenis-jenis Jaringan Komputer	5
2.2.1. <i>Local Area Network (LAN)</i>	5
2.2.1.1. <i>Low Speed PC Network</i>	5
2.2.1.2. <i>Medium Speed Network</i>	6
2.2.1.3. <i>High Speed Network</i>	6
2.2.2. <i>Metropolitan Area Network (MAN)</i>	6

2.2.3.	<i>Wide Area Network (WAN)</i>	6
2.3.	Model Referensi ISO - OSI	7
2.3.1.	Lapisan Fisik (<i>Physical Layer</i>)	8
2.3.2.	Lapisan Data Link (<i>Data Link Layer</i>).....	8
2.3.3.	Lapisan Jaringan (<i>Network Layer</i>).....	8
2.3.4.	Lapisan Transport (<i>Transport Layer</i>).....	11
2.3.5.	Lapisan Session (<i>Session Layer</i>).....	11
2.3.6.	Lapisan Presentation (<i>Lapisan Presentation</i>)	11
2.3.7.	Lapisan Aplikasi (<i>Application Layer</i>).....	11
2.4.	Router.....	12
2.4.1.	Keuntungan menggunakan router.....	12
2.4.2.	Kerugian menggunakan router	13
2.5.	Firewall	14
2.5.1.	Teknik yang digunakan firewall	14
2.5.1.1.	<i>Service Control</i> (Kendali terhadap layanan) .	14
2.5.1.2.	<i>Direction Control</i> (Kendali terhadap arah) ...	14
2.5.1.3.	<i>User Control</i> (Kendali terhadap pengguna) ..	14
2.5.1.4.	<i>Behavior Control</i> (Kendali terhadap perlakuan)	15
2.5.2.	Tipe-tipe Firewall	15
2.5.2.1.	<i>Packet Filtering Router</i>	15
2.5.2.2.	<i>Application-level Gateway</i>	16
2.5.2.3.	<i>Circuit-level Gateway</i>	18
2.6.	Autentifikasi.....	18
2.7.	Enkripsi	20
2.7.1.	Fungsi dan Tujuan Kriptografi.....	21
2.7.2.	Kategori Enkripsi Kriptografi	22
2.8.	<i>Virtual Private Network (VPN)</i>	26
2.8.1.	Tunneling.....	26
2.8.2.	Jenis-jenis Jaringan VPN	27

2.8.3.	Faedah dan Sasaran VPN.....	29
2.9.	<i>Internet Protocol Security (IPSec)</i>	30
2.9.1.	Pengertian	30
2.9.2.	Layanan keamanan pada IPSec.....	31
2.10.	<i>Secure Socket Layer (SSL)</i>	31
2.10.1.	Pengertian	31
2.10.2.	Layanan keamanan pada SSL	32
BAB III METODOLOGI PENELITIAN		33
3.1.	Tahapan Penelitian	33
3.2.	Metodologi Penelitian	36
3.3.	Tempat dan Waktu Penelitian.....	36
3.4.	Jenis Data Penelitian	36
3.5.	Rancangan Sumber Data	36
BAB IV ANALISIS PERBANDINGAN DAN PEMBAHASAN.....		37
4.1.	<i>Internet Protocol Security (IPSec)</i>	37
4.1.1.	Pengertian	37
4.1.2.	Tinjauan IPSec VPN.....	37
4.1.3.	Otentikasi dan Integritas Data.....	39
4.1.4.	Tunneling Data	40
4.1.5.	Mode Enkripsi	42
4.1.5.1.	Tunnel Mode.....	42
4.1.5.2.	Transport Mode.....	43
4.1.6.	IPSec Protocol	44
4.1.7.	Security Association	45
4.1.8.	Internet Key Exchange (IKE)	47
4.1.9.	Tinjauan ISAKMP	48
4.1.10.	Tinjauan Operasional IPSec.....	49

4.1.10.1.	IKE Phase 1.....	50
4.1.10.2.	IKE Phase 2.....	52
4.1.11.	Algoritma Diffie-Hellman	53
4.1.12.	Contoh konfigurasi site-to-site IPSec VPN.....	55
4.1.13.	IPSec VPN Router	65
4.1.14.	Solusi IPSec VPN	66
4.1.15.	Kelebihan dan Kekurangan IPSec VPN.....	67
4.2.	<i>Secure Socket Layer (SSL)</i>	67
4.2.1.	Pengertian	67
4.2.2.	Tinjauan Operasional SSL.....	70
4.2.2.1.	SSL Protocol stack	70
4.2.2.2.	Alert	71
4.2.2.3.	Handshake.....	72
4.2.2.3.1.	<i>Client Hello</i> dan operasi kunci public	73
4.2.2.3.2.	Penurunan kunci simetri.....	74
4.2.2.3.3.	<i>Finish Handshake</i>	74
4.2.2.4.	Session	75
4.2.2.5.	Mengakhiri session.....	75
4.2.2.6.	HTTPS	76
4.2.3.	SSL VPN Router	77
4.2.4.	Solusi SSL VPN	78
4.2.5.	Kelebihan dan Kekurangan SSL VPN	79
4.3.	Analisis Perbandingan.....	80
4.3.1.	Fleksibilitas.....	81
4.4.	Analisis Perbandingan protokol IPSec dan SSLpada VPN.	83
4.4.1.	OSI Layer.....	83
4.4.2.	Metode Otentikasi.....	83
4.4.3.	MAC.....	83
4.4.4.	Mode Enkripsi	84

4.4.5. Pertukaran Operasi Kriptografi.....	85
4.4.6. Proposal List Cipher	85
4.4.7. Residing Layer.....	86
BAB V PENUTUP.....	87
5.1. Kesimpulan	87
5.2. Saran.....	88

DAFTAR PUSTAKA