DAFTAR ISI

LEMBAR PENGESAHAN ..... **i**
LEMBAR PERNYATAAN ORISINILITAS ..... **ii**
ABSTRAK ..... **iii**
ABSTRACT ..... **iv**
KATA PENGANTAR ..... **v**
UCAPAN TERIMA KASIH ..... **vi**
DAFTAR ISI ..... **vii**
DAFTAR GAMBAR ..... **xi**
DAFTAR TABEL ..... **xii**
BAB I PENDAHULUAN **1**
1.1 Latar Belakang Masalah 1
1.2 Rumusan Masalah 2
1.3 Batasan Masalah 2
1.4 Metode Penelitian 3
1.4.1 Analisis Kebutuhan 3
1.4.1.1 Pengumpulan Data 3
1.4.1.2 Identifikasi Ancaman dan Risiko 3
1.4.2 Perancangan Infrastruktur 3
1.4.2.1 Pemilihan Lokasi Server 3
1.4.2.2 Pemilihan Tipe Instans Server 4
1.4.2.3 Konfigurasi Virtual Private Cloud (VPC) 4
1.4.2.4 Pengaturan Security Groups 4
1.4.2.5 Instalasi dan Konfigurasi OpenVPN 5
1.4.2.6 Pengujian Koneksi VPN 5
1.4.2.7 Evaluasi Keamanan 5
1.4.2.8 Evaluasi Biaya Operasional 5
1.4.2.9 Analisis Hasil 6
1.5 Sistematika Penulisan 6
1.6 Jadwal Penelitian 7
BAB II DASAR TEORI **8**
2.1 *Cloud Computing* 8

2.1.1 AES-256-GCM 9
2.1.2 ChaCha20-Poly1305 9
2.2 Amazon Web Services (AWS) 10
2.3 *Virtual Private Network (VPN)* 11
2.4 *Wireshark* 12
2.5 Pengaturan Jaringan dan Manajemen 13
2.6 *Classless Inter-Domain Routing* (CIDR) 14
2.6.1 Konsep Dasar CIDR 14
2.6.2 Keuntungan CIDR 15
2.7 *Port Scanning* 15
2.8 Subnet 16
2.8.1 Konsep Dasar Subnet 16
2.8.2 Keuntungan Subnet 17
2.8.3 Implementasi Subnet dalam AWS 17
2.9 Open VPN 17
2.10 *Quality of Service* (QoS) 18
2.10.1 Latency 18
2.10.2 Throughput 19
2.10.3 Uptime 19
2.10.4 Packet Loss 19
2.10.5 Evaluasi QoS 19
2.11 Perbandingan Jurnal 20
BAB III PERANCANGAN INFRASTRUKTUR VPN BERBASIS AWS 23
3.1 Perancangan Sistem 23
3.2 Analisis Keamanan Jaringan 24
3.2.1 Risiko Keamanan dalam Koneksi Tanpa Enkripsi pada Jaringan Lokal dan AWS 25
3.2.2 Identifikasi Keamanan Jaringan 25
3.2.3 Evaluasi Risiko 26
3.2.4 Kebutuhan Keamanan 26
3.3 Perancangan Infrastruktur VPN 26
3.3.1 Pemilihan Lokasi Server 27
3.3.2 Pemilihan Tipe Instans Server 27

3.3.3 Konfigurasi *Virtual Private Cloud* (VPC) 27
3.3.4 Pengaturan *Security Groups* 28
3.3.5 Instalasi dan Konfigurasi OpenVPN 28
3.3.6 Pengujian Kinerja dan Keamanan 28
3.4 Evaluasi Risiko dan Kebutuhan Keamanan 28
3.4.1 Evaluasi Risiko 28
3.4.1.1 Monitoring Lalu Lintas dengan Wireshark 29
BAB IV HASIL DAN ANALISIS 31
4.1 Rancangan Final dalam Implementasi AWS VPN 31
4.2 Perbandingan Biaya, Keamanan, dan Kinerja AWS VPN vs Turbo VPN 32
4.3 Hasil Perkiraan Hitungan Setelah Perancangan Arsitektur 34
4.3.1 Detail Mengenai Hasil Perhitungan 34
4.3.2 Layanan VPC 35
4.3.3 Layanan EC2 35
4.4 Uji Keamanan dan Analisis Data Menggunakan Wireshark dan Port Scanning 35
4.4.1 Tujuan 35
4.4.2 Metode 36
4.4.2.1 Alat dan Bahan 36
4.4.2.2 Langkah-Langkah 36
4.4.2.3 Pemantauan dan Penghentian 38
4.4.3 Hasil 38
4.4.4 Analisis 38
4.4.4.1 Analisis Hasil 38
4.4.4.2 Analisis Perbandingan dengan Solusi VPN Tradisional 39
4.4.4.3 Potensi Kelemahan 40
4.4.5 Kesimpulan 40
4.5 Langkah- Langkah Implementasi Arsitektur 40
4.5.1 Pembuatan Akun AWS dan Pemilihan Lokasi Server 41
4.5.2 Pembuatan Instans EC2 dan Pemilihan AMI (*Amazon Machine Image*) 41
4.5.3 Konfigurasi Kunci Akses dan Peluncuran Instans 42
4.5.4 Menghubungkan ke Instans EC2 dan Membuat Pengguna VPN 42

4.5.5 Konfigurasi OpenVPN melalui Dashboard Admin 43
4.5.6 Penggunaan OpenVPN Client di Perangkat Pengguna 44
4.6 Hasil Tampilan di Klien 44
4.7 Analisis Hasil Kerja 45
BAB V PENUTUP 51
5.1 Kesimpulan 51
DAFTAR PUSTAKA 54