BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam era digital yang semakin maju ini, keamanan dan privasi data menjadi salah satu prioritas utama bagi banyak organisasi. Penggunaan jaringan publik, seperti internet, untuk transmisi data sering kali meningkatkan risiko terjadinya penyadapan dan serangan *cyber*. Oleh karena itu, banyak perusahaan dan organisasi yang memilih untuk menggunakan *Virtual Private Network* (VPN) sebagai solusi untuk meningkatkan keamanan komunikasi data mereka.

VPN End Point memungkinkan pengguna untuk membuat koneksi yang aman dan terenkripsi antara perangkat mereka dan jaringan tujuan. Ini sangat penting terutama untuk perusahaan yang memiliki karyawan yang bekerja secara remote atau memiliki cabang di berbagai lokasi. Dengan menggunakan VPN End Point, perusahaan dapat memastikan bahwa data yang dikirimkan melalui jaringan internet publik tetap aman dan terjaga privasinya.

Amazon Web Services (AWS) adalah salah satu penyedia layanan cloud terbesar dan paling terpercaya di dunia. AWS menawarkan berbagai layanan yang dapat digunakan untuk membangun dan mengelola infrastruktur IT, termasuk layanan VPN. Keunggulan menggunakan AWS sebagai basis untuk VPN adalah skalabilitas, fleksibilitas, dan keamanannya yang tinggi. AWS menawarkan berbagai alat dan fitur keamanan yang dapat membantu perusahaan dalam melindungi data mereka. Oleh karena itu, ada kebutuhan untuk memahami dan mendokumentasikan proses konfigurasi VPN End Point dengan AWS, sehingga memudahkan perusahaan untuk mengadopsi dan mengelola teknologi ini [1].

Selain itu, memastikan keamanan dalam komunikasi antar jaringan sangat penting, sehingga diperlukan penelitian mendalam mengenai implementasi dan optimasi VPN Endpoint. Solusi yang tidak hanya aman, tetapi juga efisien dan mudah diintegrasikan menjadi kebutuhan yang krusial.

1.2 Rumusan Masalah

Rumusan masalah untuk penelitian mengenai implementasi dan analisis konektivitas VPN antara AWS dan jaringan lokal dapat dibagi menjadi empat pertanyaan penelitian utama:

1. Bagaimana memastikan keamanan jaringan saat menghubungkan jaringan lokal dengan lingkungan komputasi awan *Amazon Web Services* (AWS)?
2. Bagaimana merancang infrastruktur VPN berbasis *Amazon Web Services* (AWS) yang efisien dan hemat biaya?
3. Bagaimana menentukan kebutuhan dan konfigurasi spesifik layanan AWS untuk membangun infrastruktur VPN yang optimal?
4. Bagaimana mengukur dan memastikan performa serta efektivitas infrastruktur VPN berbasis AWS setelah implementasi?

1.3 Batasan Masalah

1. Fokus pada infrastruktur VPN berbasis AWS: Penelitian ini akan difokuskan pada perancangan dan implementasi solusi VPN yang menggunakan layanan dan fitur yang disediakan oleh AWS. Pemilihan dan penggunaan layanan lain di luar AWS akan dikecualikan dari lingkup tugas akhir ini.
2. Penekanan pada keamanan jaringan: Tujuan utama penelitian ini adalah meningkatkan keamanan jaringan melalui solusi VPN. Namun, penelitian ini tidak akan secara mendalam membahas aspek keamanan lainnya seperti pengelolaan akses pengguna, enkripsi *end-to-end*, atau deteksi serangan spesifik.
3. Keterbatasan finansial: Meskipun tujuannya adalah merancang VPN dengan harga yang murah, penelitian ini akan mempertimbangkan keterbatasan finansial yang relatif rendah. Pemilihan dan konfigurasi layanan AWS akan didasarkan pada opsi harga terjangkau dan strategi penghematan biaya yang rasional.
4. Cipher yang Digunakan: Pada implementasi VPN ini, digunakan algoritma enkripsi AES-256-GCM dan CHACHA20-POLY1305 untuk menjamin

keamanan data selama proses transmisi. Kedua cipher ini dikenal memiliki tingkat keamanan yang tinggi dan efisiensi yang baik dalam enkripsi data, sesuai dengan standar keamanan modern untuk VPN.

1.4 Metode Penelitian

Penelitian ini akan menggunakan metode penelitian deskriptif dengan pendekatan studi kasus untuk merancang dan mengimplementasikan infrastruktur VPN berbasis AWS. Metode ini akan melibatkan beberapa tahapan, mulai dari analisis kebutuhan, perancangan, implementasi, hingga evaluasi performa dan efektivitas. Berikut adalah tahapan metode penelitian yang akan dilakukan:

1.4.1 Analisis Kebutuhan

1.4.1.1 Pengumpulan Data

1. Dokumentasi Teknis: Mengumpulkan dokumentasi teknis dan referensi dari AWS dan sumber terkait lainnya yang membahas infrastruktur VPN, layanan AWS, dan praktik keamanan jaringan.
2. Kebutuhan Organisasi: Melakukan wawancara dan diskusi dengan pihak terkait di organisasi untuk memahami kebutuhan spesifik mereka terkait keamanan, konektivitas, dan efisiensi biaya.

1.4.1.2 Identifikasi Ancaman dan Risiko

1. Melakukan analisis terhadap ancaman keamanan yang mungkin dihadapi oleh infrastruktur VPN.
2. Melakukan evaluasi risiko dengan mempertimbangkan kemungkinan terjadinya ancaman dan dampaknya terhadap sistem.

1.4.2 Perancangan Infrastruktur

1.4.2.1 Pemilihan Lokasi Server

Pada tahap awal perancangan infrastruktur VPN, pemilihan lokasi server menjadi langkah penting. Wilayah North Virginia dipilih meskipun memiliki latensi yang relatif tinggi dan koneksi yang kurang stabil. Pemilihan lokasi ini tetap dilakukan karena terdapat kelebihan lain seperti jangkauan global yang luas

serta aksesibilitas yang lebih mudah bagi pengguna di kawasan Amerika Utara. Selain itu, North Virginia merupakan salah satu wilayah dengan ketersediaan layanan AWS yang paling lengkap dan mendukung integrasi dengan berbagai layanan cloud lainnya, sehingga memudahkan dalam skenario pengembangan lebih lanjut.

1.4.2.2 Pemilihan Tipe Instans Server

Setelah lokasi server ditentukan, langkah selanjutnya adalah pemilihan tipe instans server yang sesuai dengan kebutuhan tugas akhir dan anggaran. Dalam hal ini, instans **T2 Micro** dipilih karena termasuk dalam tier gratis AWS yang memungkinkan penggunaan hingga 750 jam per bulan tanpa biaya tambahan. Tipe instans ini juga memiliki performa yang cukup memadai untuk menjalankan layanan OpenVPN dalam skala kecil hingga menengah.

1.4.2.3 Konfigurasi Virtual Private Cloud (VPC)

Infrastruktur jaringan VPN di AWS membutuhkan konfigurasi Virtual Private Cloud (VPC) yang berfungsi sebagai fondasi untuk memastikan isolasi trafik dan keamanan. Desain VPC melibatkan pembagian subnet, konfigurasi gateway internet, dan penentuan rute yang sesuai untuk mendukung aliran data yang aman dan efisien. VPC juga diatur agar dapat diintegrasikan dengan instans server yang dipilih.

1.4.2.4 Pengaturan Security Groups

Pengaturan *Security Groups* menjadi aspek vital dalam perancangan ini. *Security Groups* digunakan untuk mengontrol akses masuk dan keluar dari instans dengan mengatur aturan firewall yang spesifik. Hanya port yang diperlukan untuk komunikasi VPN, seperti port 1194 (OpenVPN) dan port 22 (SSH), yang dibuka untuk meminimalkan risiko serangan. Setiap aturan disesuaikan agar hanya pengguna terotorisasi yang dapat mengakses layanan.

1.4.2.5 Instalasi dan Konfigurasi OpenVPN

Setelah infrastruktur dasar siap, tahap berikutnya adalah instalasi dan konfigurasi perangkat lunak OpenVPN pada instans server. Pengujian dan Evaluasi.

1.4.2.6 Pengujian Koneksi VPN

1. Melakukan pengujian koneksi VPN untuk memastikan bahwa koneksi antara jaringan lokal dan AWS berfungsi dengan baik dan aman.
2. Mengukur *latency*, *throughput,* dan *uptime* dari koneksi VPN.

1.4.2.7 Evaluasi Keamanan

Evaluasi keamanan pada infrastruktur VPN dilakukan untuk memastikan bahwa koneksi yang dihasilkan aman dari potensi ancaman dan kebocoran data. Dalam evaluasi ini, digunakan dua metode utama: analisis lalu lintas jaringan menggunakan Wireshark dan pemindaian port (*port scanning*).

Analisis menggunakan Wireshark bertujuan untuk memonitor dan menganalisis paket data yang melewati jaringan VPN. Proses ini melibatkan identifikasi terhadap pola-pola yang mencurigakan, seperti adanya paket yang tidak terenkripsi. Dengan Wireshark, seluruh lalu lintas jaringan dapat dipantau secara real-time, sehingga potensi kebocoran informasi sensitif dapat diidentifikasi dan ditindaklanjutin cepat.

Selain itu, pemindaian port dilakukan untuk mengidentifikasi port-port terbuka pada server VPN yang berpotensi menjadi titik masuk bagi serangan. Port scanning membantu mendeteksi port yang tidak diperlukan tetapi tetap terbuka, sehingga dapat ditutup untuk meminimalisir risiko. Alat-alat seperti Nmap digunakan dalam pemindaian ini untuk memberikan laporan rinci mengenai status setiap port yang ada.

1.4.2.8 Evaluasi Biaya Operasional

1. Menghitung biaya operasional bulanan berdasarkan penggunaan layanan AWS.

2. Membandingkan biaya dengan anggaran yang telah direncanakan untuk menilai efisiensi biaya.

1.4.2.9 Analisis Hasil

1. Menganalisis hasil pengujian dan evaluasi untuk menilai performa dan efektivitas infrastruktur VPN.
2. Mengidentifikasi area yang perlu perbaikan dan mengembangkan rekomendasi untuk optimasi lebih lanjut.

1.4.2.10 Dokumentasi dan Pelaporan

1. Mendokumentasikan setiap tahap proses perancangan, implementasi, pengujian, dan evaluasi.
2. Menyusun laporan akhir yang mencakup hasil penelitian, analisis, dan rekomendasi.

1.5 Sistematika Penulisan

Penulisan tugas akhir ini dibagi menjadi beberapa bagian, yaitu:

Bab I Pendahuluan

Bab ini membahas pendahuluan mengenai tugas akhir, termasuk latar belakang, rumusan masalah, definisi masalah, tujuan dan manfaat penulisan, metodologi penelitian, dan sistematika penulisan tugas akhir.

Bab II Dasar Teori

Bab ini menjelaskan teori dasar yang menjadi dasar penelitian tugas akhir ini, termasuk konsep VPN, keamanan jaringan, dan layanan AWS yang relevan untuk implementasi VPN.

Bab III Perancangan Infrastruktur VPN Berbasis AWS

Bab ini membahas tahapan perancangan infrastruktur VPN berbasis AWS dengan fokus pada keamanan jaringan dan penghematan biaya. Berisi rincian perancangan dan konfigurasi layanan AWS yang dipilih untuk implementasi VPN.

Bab IV Hasil dan Analisa

Bab ini berisi tentang implementasi infrastruktur VPN berbasis

AWS yang telah dirancang. Menjelaskan langkah-langkah implementasi, pengujian, dan evaluasi terhadap keamanan, kinerja, dan fungsionalitas VPN yang diimplementasikan.

Bab V Penutup

Bab ini menyajikan hasil dari implementasi dan pengujian infrastruktur VPN berbasis AWS. Dilakukan analisis terhadap hasil yang diperoleh dan membandingkannya dengan solusi VPN tradisional untuk mengevaluasi keefektifan solusi yang diusulkan.

1.6 Jadwal Penelitian

Tabel 1. 1 Jadwal Penelitian

No	Tahapan Penelitian	Mei 2024 - Agustus 2024			
		Mei	Juni	Juli	Agustus
1.	Identifikasi Masalah				
2.	Analisis Kebutuhan Sistem				
3.	Perancangan Infrastruktur VPN berbasis AWS				
4.	Uji Coba Sistem				
5.	*Maintenance* Sistem				
6.	Implementasi Sistem				
7.	Penulisan Laporan Akhir				

Penelitian dilakukan selama 4 bulan, dimulai dari Bulan Mei 2024 - Agustus 2024. Proses dimulai dengan identifikasi masalah yang dilakukan selama 1 bulan, dilanjutkan dengan analisis kebutuhan sistem selama 1 bulan. Perancangan infrastruktur VPN berbasis AWS dilakukan selama 2 bulan. Uji coba sistem dan maintenance masing-masing dilakukan selama 1 bulan. Implementasi sistem dilakukan selama 1 bulan dan diakhiri dengan penulisan laporan akhir yang memakan waktu 2 bulan.