BAB 2
LANDASAN TEORI

Bab ini menguraikan landasan teori dan kerangka konseptual yang menjadi dasar dalam penelitian ini. Pembahasan mencakup teknologi akses jarak jauh, arsitektur jaringan, protokol VPN WireGuard, mekanisme *Reverse Proxy*, standar pengukuran performa jaringan, serta kerangka kerja keamanan informasi yang digunakan sebagai acuan analisis.

2.1 Remote Access Technologies dan CGNAT

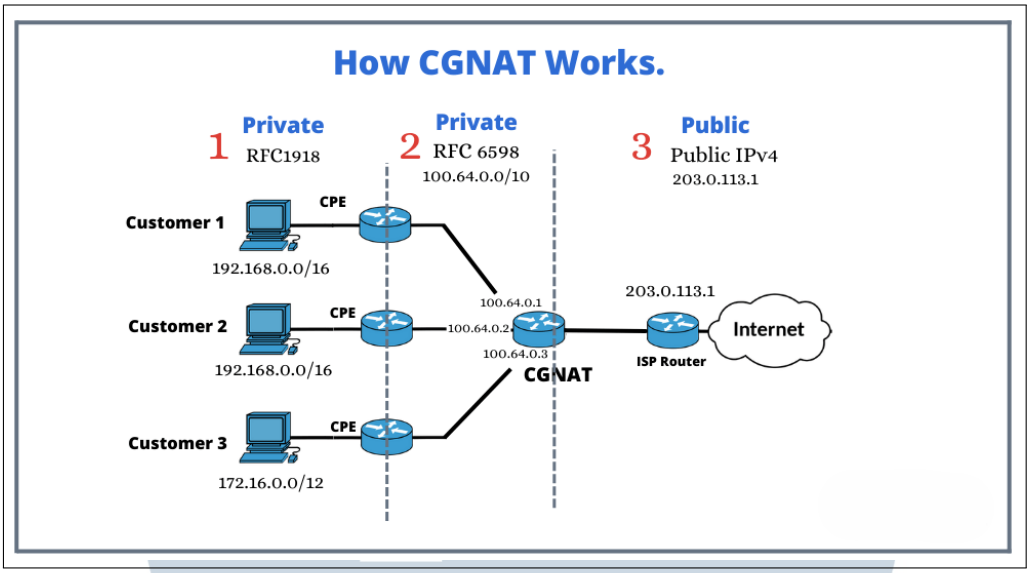
Akses jarak jauh (*remote access*) adalah kemampuan pengguna untuk terhubung ke sistem atau sumber daya yang berada di lokasi berbeda melalui jaringan. Dalam konteks penyimpanan data pribadi seperti NAS (*Network Attached Storage*), *remote access* memungkinkan pengguna mengakses *file* di *server* pribadi tanpa harus berada di lokasi fisik [1].

Pada praktiknya, implementasi *remote access* di jaringan residensial kerap terkendala oleh *Carrier-Grade Network Address Translation* (CGNAT). CGNAT digunakan ISP sebagai solusi transisi untuk kelangkaan IPv4; satu alamat IPv4 publik dibagi ke banyak pelanggan sehingga masing-masing pelanggan tidak memiliki IP publik eksklusif. Konsekuensinya, konektivitas masuk (*inbound*) dari internet publik ke *host* di belakang CGNAT menjadi sulit dilakukan tanpa bantuan pihak ketiga atau *tunneling* [2, 3].

Gambar 2.1 memperlihatkan bagaimana mekanisme CGNAT bekerja. Dampak langsung dari CGNAT adalah metode tradisional seperti *port forwarding* menjadi tidak efektif karena pengguna tidak memiliki kendali atas IP publik di sisi ISP. Untuk mengatasi hal ini, arsitektur *hub-and-spoke* yang memanfaatkan *Virtual Private Server* (VPS) ber-IP publik statis berperan sebagai *gateway* terpusat yang menjembatani koneksi dari klien internet ke *server* lokal di rumah [4].

2.2 Arsitektur Hub-and-Spoke dan VPS Gateway

Arsitektur *hub-and-spoke* adalah topologi jaringan yang menempatkan satu *node* pusat (*hub*) sebagai titik koneksi terpusat bagi beberapa *node* perifer (*spoke*). Dalam konteks mitigasi CGNAT, VPS berperan sebagai *hub* yang dapat diakses dari internet publik, sedangkan *server* NAS bertindak sebagai *spoke*.



Gambar 2.1. Ilustrasi mekanisme Carrier-Grade NAT (CGNAT)

Pola ini memungkinkan pengelolaan konektivitas melalui *tunnel* terenkripsi *outbound* dari rumah ke VPS, sehingga mengeliminasi kebutuhan IP publik statis di sisi pengguna residensial [4]. VPS berfungsi sebagai titik kontrol keamanan terpusat (*policy enforcement point*) yang menjalankan layanan seperti *WireGuard server* dan *reverse proxy* Nginx.

2.3 WireGuard VPN Protocol

WireGuard merupakan protokol VPN modern yang dirancang dengan prinsip kesederhanaan dan performa tinggi. Berbeda dengan protokol tradisional seperti OpenVPN yang memiliki ribuan baris kode, WireGuard menggunakan arsitektur yang jauh lebih ramping sehingga lebih mudah diaudit keamanannya dan memiliki *overhead* komputasi yang rendah [10].

2.3.1 Karakteristik Teknis WireGuard

Secara kriptografi, WireGuard memanfaatkan algoritma modern yang telah teruji: pertukaran kunci berbasis Curve25519 untuk ECDH, fungsi *hash* BLAKE2s, serta enkripsi simetris ChaCha20 dan autentikasi pesan Poly1305. Kombinasi AEAD ChaCha20-Poly1305 digunakan untuk memastikan kerahasiaan (*confidentiality*) dan integritas (*integrity*) paket data dalam satu operasi yang efisien [10].

2.3.2 Arsitektur WireGuard

WireGuard beroperasi pada lapisan jaringan (L3) dan diintegrasikan sebagai *interface* virtual di dalam *kernel space* Linux. Hal ini mengurangi *context switching* antara *user space* dan *kernel space*, yang berdampak pada peningkatan *throughput* dan penurunan *latency* dibandingkan arsitektur VPN berbasis *user space* [10].

2.4 Nginx Reverse Proxy dan HTTPS

Nginx sebagai *reverse proxy* berperan pada lapisan aplikasi (L7) untuk meneruskan permintaan klien ke layanan di belakangnya. Dalam penelitian ini, Nginx di VPS menerima koneksi HTTPS, melakukan terminasi TLS, dan meneruskan trafik ke antarmuka *web* NAS secara terkontrol [5].

2.4.1 TLS 1.3 dan Rekomendasi Konfigurasi

Transport Layer Security (TLS) versi 1.3 menyederhanakan proses *handshake* menjadi satu *round-trip*, yang mengurangi *latency* saat pembentukan koneksi awal. TLS 1.3 juga mewajibkan penggunaan *cipher suite* AEAD modern seperti AES-256-GCM atau ChaCha20-Poly1305, serta mendukung *forward secrecy* secara bawaan untuk memastikan keamanan data jangka panjang [9].

2.4.2 Kontrol Akses dan Proteksi Lapis Aplikasi

Nginx memungkinkan penerapan kebijakan keamanan yang granular, seperti pembatasan akses berbasis alamat IP (*Access Control List*), autentikasi dasar (*HTTP Basic Auth*), dan *rate limiting* untuk mencegah penyalahgunaan sumber daya. Selain itu, penggunaan *security headers* seperti HSTS dan *X-Frame-Options* membantu memperkuat postur keamanan antarmuka *web* dari berbagai serangan berbasis *browser* [5].

2.5 Network Performance Metrics

Evaluasi kinerja jaringan dalam penelitian ini didasarkan pada tiga metrik utama yang saling melengkapi [11]:

1. Latency: Waktu tempuh paket bolak-balik (*Round-Trip Time*/RTT) dari pengirim ke penerima, diukur dalam milidetik (ms).

2. Throughput: Laju data efektif yang berhasil ditransmisikan melalui kanal komunikasi dalam satuan waktu tertentu (Mbps).

3. Transfer Speed: Kecepatan rata-rata saat melakukan pengunduhan berkas melalui protokol HTTP/HTTPS (MB/s).

Untuk mengevaluasi kualitas performa jaringan, penelitian ini mengacu pada standar *Quality of Service* (QoS) yang diterbitkan oleh *European Telecommunications Standards Institute* (ETSI) dalam dokumen TIPHON TR 101 329. Standar ini menyediakan klasifikasi kualitas jaringan berdasarkan parameter *latency* yang relevan untuk aplikasi *real-time* dan akses data [12].

Tabel 2.1 menunjukkan kategori indeks performansi untuk parameter *latency* (delay).

Tabel 2.1. Kategori Latency Berdasarkan Standar TIPHON

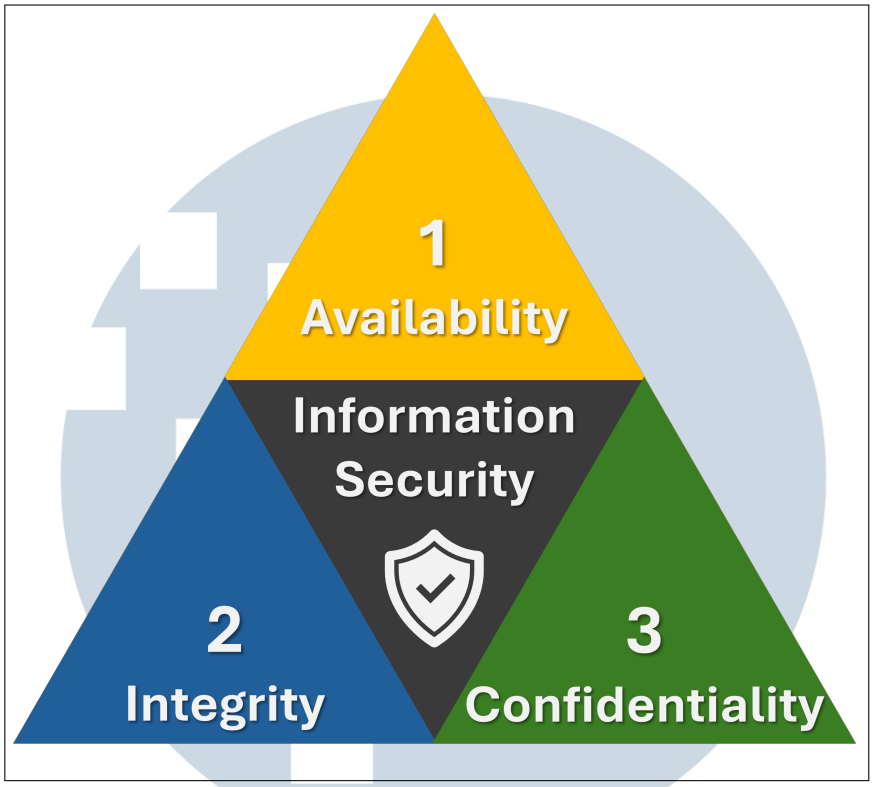
Kategori	**Latency (ms)**	**Indeks**
Sangat Bagus	< 150 ms	4
Bagus	$150 - 300$ ms	3
Sedang	$300 - 450$ ms	2
Buruk	> 450 ms	1

2.6 Kerangka Kerja Keamanan (Security Frameworks)

Kerangka kerja keamanan digunakan sebagai landasan utama untuk mengevaluasi efektivitas kontrol keamanan pada metode akses yang diuji dalam penelitian ini.

2.6.1 CIA Triad Model

Model CIA Triad terdiri dari tiga pilar fundamental yang saling berkaitan untuk menjamin keamanan informasi, sebagaimana diilustrasikan pada Gambar 2.2.



Gambar 2.2. Kerangka kerja keamanan CIA Triad

1. Confidentiality (Kerahasiaan): Aspek ini menjamin bahwa informasi sensitif hanya dapat diakses oleh entitas yang memiliki otorisasi sah. Dalam penelitian ini, validasi dilakukan melalui enkripsi WireGuard (L3) dan TLS (L7).

2. Integrity (Integritas): Aspek ini memastikan keaslian data dengan mencegah modifikasi tidak sah. WireGuard menggunakan *authentication tag* Poly1305, sedangkan TLS memanfaatkan mekanisme MAC [9].

3. Availability (Ketersediaan): Aspek ini menjamin layanan dapat diakses secara reliabel. Evaluasi dilakukan berdasarkan stabilitas koneksi dan dampak *overhead* enkripsi [11].

2.6.2 Attack Surface dan Blue Teaming

Selain CIA Triad, analisis keamanan juga mengadopsi konsep *Attack Surface* dan *Blue Teaming*. *Attack Surface* merujuk pada jumlah titik atau celah di mana penyerang dapat mencoba masuk atau mengekstraksi data dari suatu sistem.

Penelitian ini menggunakan pendekatan *Blue Teaming*, yaitu strategi pertahanan defensif yang berfokus pada audit konfigurasi, identifikasi celah, dan validasi pertahanan. Prosedur teknis pelaksanaan *assessment* ini mengacu secara eksplisit pada standar NIST SP 800-115 (*Technical Guide to Information Security Testing and Assessment*), khususnya pada fase penemuan (*Discovery*) dan verifikasi kerentanan (*Verification*) [13].

2.7 Perangkat dan Instrumen Penelitian

Implementasi dan pengujian dalam penelitian ini didukung oleh serangkaian perangkat lunak yang mencakup platform virtualisasi, sistem operasi, serta instrumen pengukuran. Pemilihan perangkat dan alat bantu ini disesuaikan dengan kebutuhan untuk membangun lingkungan simulasi yang mendekati kondisi riil serta untuk menjamin validitas data hasil pengujian.

2.7.1 Platform Virtualisasi dan Sistem Operasi

Proxmox VE digunakan sebagai lingkungan virtualisasi berbasis *Type-1 Hypervisor* yang memfasilitasi isolasi layanan dalam bentuk mesin virtual (VM) atau kontainer. Di atas platform ini, OpenMediaVault (OMV) diimplementasikan sebagai sistem operasi NAS yang menyediakan layanan manajemen berkas berbasis *web*, yang sekaligus berfungsi sebagai target utama dalam skenario akses jarak jauh [7].

2.7.2 Instrumen Pengukuran Performa

Pengukuran kinerja jaringan dilakukan menggunakan dua utilitas utama untuk mendapatkan parameter kuantitatif:

1. *iperf3:* Digunakan untuk mengukur *throughput* jaringan maksimum pada mode TCP guna mengetahui kapasitas *bandwidth* efektif.
2. *curl:* Digunakan untuk mengukur waktu respons total (*total response time*) dan kecepatan transfer data riil pada lapisan aplikasi (HTTP/HTTPS) [11, 14].

2.7.3 Standar Audit Keamanan (NIST SP 800-115)

Sebagai landasan validasi keamanan, penelitian ini mengacu pada standar NIST *Special Publication* (SP) 800-115 yang berfokus pada panduan teknis pengujian dan asesmen keamanan informasi. Standar ini mendefinisikan metodologi audit teknis melalui pendekatan *Blue Teaming* yang mencakup dua fase utama:

1. Discovery: Fase penemuan untuk memetakan permukaan serangan (*attack surface*) dan mengidentifikasi layanan yang terekspos [15].
2. Verification: Fase verifikasi untuk membuktikan efektivitas kontrol keamanan (seperti enkripsi) dalam melindungi data dari intersepsi pihak ketiga [15].

Metodologi ini menjadi dasar pemilihan instrumen audit jaringan yang digunakan pada bagian selanjutnya.

2.7.4 Instrumen Audit Keamanan

Proses audit keamanan dilakukan menggunakan perangkat lunak pemindaian dan analisis paket data sebagai berikut:

1. Wireshark/Tshark: Digunakan untuk melakukan *packet capture* dan analisis trafik jaringan secara mendalam. Instrumen ini berfungsi sebagai alat validasi utama untuk memastikan apakah *payload* data telah terenkripsi sempurna atau masih terbaca sebagai teks polos (*plaintext*) [16].
2. Nmap: Digunakan untuk melakukan pemindaian *port* (*port scanning*) guna mengidentifikasi layanan yang terbuka pada VPS. Proses ini bertujuan untuk memetakan *attack surface* dan memverifikasi bahwa tidak ada celah layanan non-esensial yang terekspos ke jaringan publik.

2.8 Hybrid Architecture: Dual-Layer Security

Arsitektur *hybrid* menggabungkan keamanan lapisan jaringan (VPN) dan lapisan aplikasi (*reverse proxy*). Dalam skema ini, Nginx di VPS menangani permintaan HTTPS dari internet, sementara trafik dari VPS diteruskan ke jaringan rumah melalui *tunnel* WireGuard. Pendekatan *defense-in-depth* ini memberikan perlindungan berlapis, namun memperkenalkan *overhead* tambahan akibat proses enkripsi ganda dan enkapsulasi paket (*nested tunneling*) [5, 10].