BAB 1
PENDAHULUAN

Bab ini menguraikan konteks fundamental dan urgensi permasalahan yang melatarbelakangi dilakukannya penelitian mengenai analisis performa dan keamanan akses jarak jauh pada NAS. Pembahasan selanjutnya mencakup perumusan masalah, batasan ruang lingkup, tujuan dan manfaat penelitian, serta sistematika penulisan laporan tugas akhir.

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi telah mendorong kebutuhan akan akses data yang fleksibel dan tersedia dari mana saja. *Network Attached Storage* (NAS) telah menjadi solusi penyimpanan terpusat yang populer untuk kebutuhan pribadi maupun organisasi karena kemampuannya menyediakan akses *file* yang terpusat, mudah dikelola, dan dapat diakses oleh banyak pengguna secara bersamaan [1]. Namun, akses jarak jauh terhadap NAS menghadapi tantangan signifikan, terutama dalam lingkungan jaringan modern yang menerapkan *Carrier-Grade Network Address Translation* (CGNAT) [2].

CGNAT merupakan teknologi yang digunakan oleh penyedia layanan internet (ISP) untuk mengatasi kelangkaan alamat IPv4 dengan cara membagikan satu alamat IP publik kepada beberapa pelanggan secara bersamaan [2]. Teknologi ini, meskipun efektif dalam memperpanjang masa pakai IPv4, menciptakan hambatan bagi layanan yang memerlukan koneksi langsung dari internet, seperti akses jarak jauh ke *server* pribadi atau NAS. Dalam konteks CGNAT, metode tradisional seperti *port forwarding* tidak dapat diterapkan karena alamat IP publik tidak dialokasikan secara eksklusif kepada pengguna individu [3]. Hal ini menimbulkan kebutuhan akan solusi alternatif yang dapat menembus keterbatasan CGNAT sambil tetap menjaga aspek keamanan dan performa sistem.

Untuk mengatasi tantangan tersebut, arsitektur *hub-and-spoke* dengan *Virtual Private Server* (VPS) sebagai *gateway* terpusat menawarkan solusi yang efektif [4]. Dalam arsitektur ini, VPS yang memiliki alamat IP publik statis berperan sebagai *hub* yang berfungsi sebagai titik masuk terpusat, sementara *server* lokal di belakang CGNAT bertindak sebagai *spoke* yang terhubung ke *hub* melalui *tunnel* terenkripsi [4]. Pendekatan ini memungkinkan akses jarak jauh yang aman

tanpa memerlukan IP publik statis di sisi klien, sekaligus memberikan kontrol keamanan yang terpusat.

Dua metode utama yang dapat diimplementasikan dalam arsitektur *hub-and-spoke* untuk akses jarak jauh adalah *Virtual Private Network* (VPN) berbasis WireGuard dan *reverse proxy* berbasis Nginx [5]. WireGuard merupakan protokol VPN modern yang dirancang dengan fokus pada kesederhanaan, performa tinggi, dan keamanan yang kuat. Penelitian terbaru menunjukkan bahwa WireGuard memiliki keunggulan signifikan dalam hal *throughput* dan *latency* rendah dibandingkan dengan protokol VPN tradisional seperti OpenVPN dan IPsec [6]. Di sisi lain, Nginx sebagai *reverse proxy* menyediakan akses tingkat aplikasi yang lebih granular dengan kemampuan untuk mengelola lalu lintas HTTP/HTTPS, melakukan terminasi SSL/TLS, dan memberikan lapisan keamanan tambahan melalui kontrol akses berbasis domain [5].

Virtualisasi menggunakan Proxmox VE memungkinkan implementasi infrastruktur yang fleksibel dan efisien dalam pengelolaan beberapa layanan secara terisolasi [7]. Proxmox VE menyediakan *platform* yang memungkinkan pengelolaan mesin virtual dan kontainer dalam satu lingkungan terpadu, yang sangat sesuai untuk skenario pengujian dan *deployment* layanan yang memerlukan isolasi lingkungan seperti NAS berbasis OpenMediaVault, *server* VPN, dan *reverse proxy* [1]. Kombinasi antara virtualisasi, arsitektur *hub-and-spoke*, dan metode akses jarak jauh yang berbeda menciptakan peluang untuk melakukan analisis komparatif yang komprehensif terhadap aspek performa dan keamanan.

Aspek keamanan dalam akses jarak jauh menjadi perhatian kritis, terutama dalam konteks ancaman siber yang semakin kompleks. Prinsip *Zero Trust Network Access* (ZTNA) yang menekankan verifikasi berkelanjutan terhadap identitas pengguna dan perangkat, terlepas dari lokasi jaringan, telah menjadi paradigma keamanan terkini untuk akses jarak jauh [8]. Implementasi kontrol keamanan yang tepat pada *gateway* terpusat, seperti *firewall*, autentikasi multi-faktor, dan enkripsi *end-to-end*, sangat penting untuk melindungi data dan sumber daya dari akses yang tidak sah [9]. Oleh karena itu, evaluasi keamanan yang mencakup aspek kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) perlu dilakukan secara komprehensif untuk memastikan bahwa solusi yang diterapkan memenuhi standar keamanan yang diperlukan.

Penelitian ini bertujuan untuk menganalisis dan membandingkan performa serta tingkat keamanan antara dua metode akses jarak jauh terhadap NAS berbasis Proxmox, yaitu VPN WireGuard dan *reverse proxy* Nginx, dalam

skenario arsitektur *hub-and-spoke* yang terkendala oleh CGNAT. Melalui pengujian empiris yang mencakup pengukuran *throughput*, *latency*, serta evaluasi keamanan menggunakan berbagai *tools* analisis, penelitian ini diharapkan dapat memberikan rekomendasi berbasis data mengenai metode akses jarak jauh yang paling optimal untuk diterapkan dalam lingkungan jaringan modern [10-12].

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, penelitian ini merumuskan pertanyaan sebagai berikut:

1. Bagaimana perbandingan kinerja jaringan (*network performance*) pada akses jarak jauh NAS menggunakan VPN WireGuard dan *Reverse Proxy* Nginx ditinjau dari parameter *latency*, *throughput*, dan *transfer speed*?
2. Bagaimana efektivitas mekanisme keamanan kedua metode akses dalam melindungi kerahasiaan data (*confidentiality*) dan meminimalkan permukaan serangan (*attack surface*) berdasarkan audit keamanan teknis?
3. Metode akses manakah yang memberikan *trade-off* paling optimal antara performa dan keamanan untuk implementasi pada lingkungan *home lab* dengan sumber daya terbatas?

1.3 Batasan Permasalahan

Penelitian ini memiliki beberapa batasan yang penting untuk diakui guna memastikan interpretasi hasil yang tepat, yaitu sebagai berikut:

1. Penelitian ini hanya fokus pada perbandingan tiga metode akses jarak jauh spesifik (VPN WireGuard, Nginx *reverse proxy*, dan *hybrid configuration*) dalam konteks arsitektur *hub-and-spoke* dengan satu VPS *gateway* terpusat. Penelitian tidak mencakup perbandingan dengan metode akses jarak jauh lainnya seperti OpenVPN, IPsec, atau solusi komersial seperti Tailscale yang juga valid untuk mengatasi CGNAT. Selain itu, analisis keamanan dalam penelitian ini dilakukan melalui simulasi serangan tertentu dan tidak mencakup *penetration testing* komprehensif atau audit keamanan profesional yang lebih mendalam.

2. Lingkungan pengujian dan infrastruktur dilakukan dalam konteks *controlled lab environment* dengan spesifikasi terbatas. Pengujian menggunakan klien tunggal (Intel i5-12450H) dengan mekanisme eksekusi hibrida, di mana koneksi VPN berjalan pada Windows (*host*) sementara skrip pengujian berjalan pada WSL 2. Meskipun hal ini menimbulkan sedikit *overhead* translasi jaringan, dampaknya bersifat konstan pada seluruh skenario. Selain itu, *Gateway* VPS yang digunakan memiliki *resource* terbatas (1 vCPU, 1 GB RAM) yang merepresentasikan penggunaan *low-end cloud*, sehingga berpotensi menjadi *bottleneck* performa pada beban enkripsi tinggi dan hasilnya mungkin bersifat *conservative* dibandingkan lingkungan produksi skala besar.

3. Analisis dibatasi pada akses berbasis *web interface* OMV pada *port* 8080 dengan pengukuran *throughput* melalui HTTP *file download*. Hasil ini *representative* untuk *use case* transfer *file* via HTTP, namun mungkin berbeda untuk protokol alternatif seperti SMB/NFS. Pengujian juga dilakukan pada kondisi jaringan internet publik yang relatif stabil tanpa simulasi gangguan ekstrem (*jitter injection* atau *packet loss* buatan) maupun *stress condition* ekstrem, sehingga perilaku sistem di bawah beban puncak (*under extreme load*) tidak dianalisis secara mendalam.

4. Penelitian ini tidak mencakup analisis terhadap skalabilitas *long-term*, *durability*, atau *behavior* sistem dalam periode pengujian yang panjang. Semua pengujian dilakukan dalam *timeframe* terbatas dengan kontrol variabel yang ketat, sehingga temuan mungkin tidak sepenuhnya dapat digeneralisasi ke skenario *deployment* jangka panjang yang memiliki pola penggunaan (*usage pattern*) berbeda dari ekspektasi laboratorium.

5. Pengujian keamanan berfokus pada analisis arsitektur pertahanan (*Blue Teaming*), meliputi validasi enkripsi data (*Packet Capture*) dan pemindaian celah keamanan (*Vulnerability Assessment*) serta konfigurasi. Penelitian ini tidak mencakup simulasi serangan eksploitasi aktif (*Red Teaming*) seperti *Brute Force* atau *DDoS attack* secara intensif.

Meskipun terdapat batasan-batasan tersebut, penelitian ini tetap memberikan *insights* yang berharga mengenai *trade-off* performa dan keamanan antara metode akses jarak jauh dalam konteks spesifik yang telah didefinisikan. Hasil penelitian dapat menjadi referensi bagi implementasi NAS residensial dengan kendala

CGNAT yang serupa, dengan pemahaman bahwa generalisasi ke konteks berbeda memerlukan pengujian tambahan.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah ditetapkan, penelitian ini memiliki tujuan utama dan beberapa tujuan khusus sebagai berikut:

1. Mengukur dan menganalisis metrik performa (*latency*, *throughput*, *transfer speed*) pada skenario akses NAS menggunakan VPN WireGuard dan *Reverse Proxy* Nginx.
2. Memvalidasi efektivitas enkripsi protokol dan keamanan konfigurasi sistem melalui pengujian *packet sniffing* dan audit celah keamanan (*vulnerability scanning*).
3. Menentukan metode akses terbaik yang menyeimbangkan kebutuhan performa dan standar keamanan data untuk penggunaan pribadi skala residensial.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat yang signifikan pada berbagai tingkatan, baik dari perspektif akademis maupun praktis.

Manfaat Teoritis:

1. Kontribusi pada literatur keamanan jaringan mengenai perbandingan protokol enkripsi modern (WireGuard) versus solusi *proxy* tradisional dalam konteks *home lab* dan *edge computing*. Penelitian ini mengisi *gap* literatur dengan menyediakan data empiris terukur tentang *trade-off* antara kedua pendekatan dalam skenario CGNAT yang semakin umum di ISP modern.
2. Pemahaman mendalam tentang arsitektur *hub-and-spoke* dalam konteks mitigasi CGNAT. Studi ini memberikan *insights* bagaimana topologi ini dapat diimplementasikan dengan *resource* terbatas dan apa implikasinya terhadap performa serta keamanan sistem secara keseluruhan.
3. Evaluasi praktis *framework* keamanan CIA Triad (*Confidentiality, Integrity, Availability*) ketika diterapkan pada solusi akses jarak jauh modern.

Penelitian ini menunjukkan bagaimana prinsip-prinsip keamanan tradisional dapat diukur dan dibandingkan secara empiris dalam konteks teknologi VPN dan *proxy* kontemporer.

Manfaat Praktis:

1. Panduan implementasi untuk pengguna residensial yang menghadapi keterbatasan CGNAT dan ingin mengakses NAS pribadi dari jarak jauh. Rekomendasi berbasis data dari penelitian ini dapat membantu pengguna membuat keputusan *informed* mengenai metode akses mana yang paling sesuai dengan prioritas mereka (performa, keamanan, kemudahan *deployment*).
2. *Best practices* untuk mengkonfigurasi *gateway* terpusat menggunakan VPS dengan *resource* terbatas. Penelitian ini mendokumentasikan *lessons learned* dan *trade-offs* yang dihadapi, sehingga dapat menjadi referensi bagi implementasi serupa di komunitas *home lab* dan *self-hosting*.
3. Referensi teknis untuk pemilihan teknologi dalam konteks keterbatasan infrastruktur ISP. Dengan semakin banyaknya ISP yang menerapkan CGNAT untuk mengatasi kelangkaan IPv4, penelitian ini memberikan data faktual tentang solusi *viable* yang dapat diterapkan tanpa perlu *upgrade* layanan ISP atau membeli IP publik tambahan.
4. Dokumentasi skenario *testing* dan metodologi disusun secara komprehensif guna memfasilitasi replikasi studi pada evaluasi serupa. Mengingat seluruh *stack* teknologi yang digunakan (Proxmox VE, OpenMediaVault, WireGuard, Nginx) berbasis *open-source*, validasi hasil serta penerapan metodologi dapat dilakukan secara luas.

1.6 Sistematika Penulisan

Untuk memberikan gambaran yang jelas mengenai struktur laporan penelitian, berikut adalah sistematika penulisan yang digunakan:

1. BAB 1: PENDAHULUAN

   Bab ini menyajikan pengantar komprehensif mengenai penelitian, meliputi latar belakang masalah yang menjelaskan pentingnya akses jarak jauh terhadap NAS dalam konteks CGNAT, rumusan masalah dengan tiga

pertanyaan penelitian yang spesifik, batasan permasalahan yang mengakui *scope* dan keterbatasan penelitian, tujuan penelitian yang terukur dan dapat dicapai, manfaat penelitian baik secara teoritis maupun praktis, serta sistematika penulisan yang menjelaskan struktur laporan secara keseluruhan.

2. BAB II: LANDASAN TEORI
   Bab ini membahas konsep dan teknologi yang menjadi fondasi penelitian. Dimulai dengan tinjauan umum teknologi akses jarak jauh (*remote access*), dilanjutkan dengan pembahasan mendalam mengenai protokol VPN WireGuard sebagai solusi enkripsi *network-layer*, penjelasan tentang HTTPS dan *reverse proxy* Nginx sebagai solusi enkripsi *application-layer*, pemahaman tentang metrik performa jaringan (*throughput, latency, jitter*), serta *framework* keamanan tradisional seperti CIA Triad (*Confidentiality, Integrity, Availability*) dan standar keamanan modern dari NIST yang relevan dengan penelitian ini.

3. BAB III: METODOLOGI PENELITIAN
   Bab ini merinci aspek teknis dan prosedural penelitian. Bagian pertama menjelaskan desain penelitian kuantitatif-komparatif yang menggunakan pendekatan eksperimental dengan kontrol. Bagian kedua mendeskripsikan arsitektur sistem yang diimplementasikan, yaitu topologi *hub-and-spoke* dengan VPS sebagai *gateway* terpusat dan *server* Proxmox di rumah sebagai *node* lokal. Bagian ketiga mendefinisikan empat skenario pengujian (*baseline*, VPN WireGuard, Nginx *reverse proxy*, dan *hybrid*). Bagian keempat menjelaskan parameter pengujian yang diukur, termasuk *latency*, *throughput*, dan *transfer speed*. Bagian kelima menjustifikasi metrik dan ukuran sampel ($n = 300$ untuk *latency*, $n = 30 - 40$ untuk *throughput* dan *transfer speed*). Bagian keenam mendeskripsikan *tools* dan *software stack* yang digunakan. Bagian terakhir mendokumentasikan delapan batasan penelitian dengan penjelasan teknis dan mitigasi potensial, mencakup WSL *overhead*, *single point of failure* pada VPS, keterbatasan *resource* VPS, *fragmentation* pada *nested tunnel*, *scope* pengujian *web interface only*, perbedaan *layer* antara *network* dan aplikasi, *controlled lab environment*, dan limitasi pada *baseline* LAN.

4. BAB IV: HASIL DAN PEMBAHASAN
   Bab ini menyajikan dan menganalisis hasil pengujian. Bagian pertama

menampilkan hasil pengujian performa dengan sub-bab terpisah untuk analisis *latency* (300 sampel ICMP *ping* per skenario), analisis *throughput* iperf3 (30 sampel per skenario), dan analisis *transfer speed* HTTP (40 sampel per skenario). Bagian kedua menganalisis *trade-off* antara performa dan keamanan. Bagian ketiga memaparkan hasil audit keamanan teknis yang berfokus pada validasi kerahasiaan data (*confidentiality*) melalui pembuktian enkripsi *packet capture*, serta analisis permukaan serangan (*attack surface*) melalui *port scanning* dan verifikasi konfigurasi SSL/TLS. Bagian terakhir menyajikan tabel perbandingan komprehensif yang merangkum semua metrik performa dan postur keamanan.

5. BAB V: KESIMPULAN DAN SARAN

   Bab ini merangkum temuan utama penelitian dan memberikan rekomendasi. Bagian pertama menyajikan kesimpulan yang merangkum jawaban terhadap ketiga pertanyaan penelitian, ringkasan komparatif antara ketiga metode (VPN WireGuard, Nginx, *hybrid*), dan rekomendasi praktis mengenai metode yang paling sesuai untuk berbagai skenario penggunaan dan profil pengguna (*performa-first, security-first, balanced*). Bagian kedua memberikan saran untuk penelitian lanjutan, termasuk *testing* dengan *native* Linux *environment*, evaluasi dengan *multiple* VPS dan *failover mechanism*, *testing* dengan berbagai tipe klien dan jaringan, serta *penetration testing* yang lebih komprehensif.