BAB 2
DASAR TEORI

2.1 KAJIAN PUSTAKA

Penelitian [1] membahas mengenai studi ini bertujuan untuk membandingkan kinerja dan tingkat keamanan dari beberapa metode jaringan VPN, yaitu QoS, PPTP, L2TP, SSTP, dan IPsec pada perangkat Mikrotik. Penelitian ini melibatkan analisis terhadap setiap metode yang diterapkan, dan hasilnya dianalisis dengan menggunakan aplikasi Wireshark dengan menggunakan parameter *Quality of Service* (QoS), termasuk *Packet Loss*, *Delay* dan *Throughput*. Pengujian dilakukan pada 4 *client* yang terhubung ke *access point* dengan dua skenario jaringan yang berbeda. Pada skenario pertama, semua *client* mengakses web berbasis *download*, sedangkan pada skenario kedua, semua *client* mengakses web *streaming video*. Hasil pengujian menunjukkan bahwa tingkat keamanan yang dibangun oleh *tunnel* IPsec lebih unggul dibandingkan *tunnel* PPTP, L2TP, dan SSTP. Selain itu, dari segi performa, keamanan, dan temuan pengujian lainnya, *tunnel* VPN IPsec juga menunjukkan performa yang lebih baik daripada *tunnel* VPN PPTP, L2TP dan SSTP.

Penelitian [2] membicarakan perbandingan kinerja antara dua metode jaringan, yaitu *Secure Socket Tunneling Protokol* (SSTP) dan *Layer Two Tunneling Protokol* (L2TP) + *Internet Protokol Security* (IPsec), dengan menggunakan metode *Quality of Service* (QoS). Berdasarkan penelitian tersebut, penulis menyimpulkan bahwa metode L2TP+IPsec lebih unggul dibandingkan dengan SSTP. Hal ini dapat diamati dari parameter *throughput* yang diukur, dimana L2TP+IPsec menunjukkan jumlah paket yang dikirim dan diterima lebih banyak dalam waktu 5 menit. Selain itu, parameter *delay* pada L2TP+IPsec juga lebih baik, karena total *delay* yang dihasilkan memiliki nilai yang lebih kecil. Meskipun nilai *throughput*, *packet loss*, *delay*, dan *jitter* pada L2TP+IPsec ada yang lebih besar atau lebih kecil dibandingkan dengan SSTP, namun ketika dianalisis dengan menggunakan Wireshark, dapat terlihat bahwa jumlah paket yang dikirim pada

satuan waktu yang sama oleh L2TP+IPsec lebih banyak dan tidak ada paket yang hilang selama proses transmisi data berlangsung, berbeda dengan SSTP.

Penelitian [3] membicarakan tentang perbandingan kinerja *Virtual Private Network* (VPN) antara VPN *Tunnel* dan Internet Protokols Security (IPsec). Penelitian melakukan pengujian dalam segi kinerja atau performa dari masing-masing VPN dalam mengirimkan paket data antara server dan *client* dalam jaringan VPN tersebut. Pengujian dilakukan dengan mengukur *Quality of Service* (QoS) berdasarkan empat parameter yaitu *throughput*, *delay*, *packet loss*, dan *jitter*. Dari hasil perbandingan data yang telah disajikan, dapat disimpulkan bahwa IPsec memiliki tingkat keamanan yang lebih tinggi dibandingkan dengan VPN *Tunnel* dengan jalur komunikasi dilengkapi dengan kriptografi. Selain itu, IPsec yang berjalan pada L2TP menunjukkan tingkat kinerja yang lebih baik dibandingkan dengan VPN *Tunnel.*

Penelitian [4] membahas mengenai Implementasi Keamanan Akses Terhadap *Website* Menggunakan WireGuard VPN Di *Router*board Mikrotik. Pada penelitian ini, melakukan implementasi WireGuard VPN menggunakan metode *remote access*. Hasil dari penelitian ini disimpulkan bahwa, VPN WireGuard ini mempunyai kelebihan yaitu mudah diimplementasikan dengan kemampuan melakukan enkripsi yang baik menggunakan kunci yang ada pada kedua *peer* dan mekanisme kombinasi antara authentikasi dan VPN WireGuard terbukti mampu menyembunyikan isi komunikasi di protokol http pada sistem.

Penelitian [5] mengulas tentang analisis jaringan VPN menggunakan protokol PPTP dan L2TP berbasis Mikrotik pada Diskominfo Kabupaten Muko Muko. Berdasarkan hasil pengujian yang dilakukan untuk menganalisis performansi jaringan VPN, diketahui bahwa sistem keamanan yang diterapkan menunjukkan bahwa protokol L2TP berkinerja lebih baik daripada PPTP. Hal ini karena L2TP dengan IPsec memberikan keamanan berlapis yang dapat menjamin keamanan data yang dikirimkan. Meskipun nilai *delay*, *bandwidth* dan *packet loss* pada kedua protokol PPTP dan L2TP-VPN tidak terlalu jauh berbeda dan tampak serupa, parameter *latency* menunjukkan bahwa PPTP memiliki *latency* lebih pendek dari L2TP. Namun, dalam hal *throughput*, PPTP lebih penting daripada L2TP di setiap pengujian.

Pada penelitian ini bertujuan untuk mengetahui kinerja dari jaringan VPN menggunakan protokol WireGuard dan IPsec. Berbeda dengan penelitian sebelumnya yang menggunakan protokol PPTP, L2TP, SSTP dan OpenVPN, pada penelitian ini menggunakan protokol IPsec yang dianggap sebagai protokol VPN yang kompleks saat ini dan WireGuard adalah protokol VPN terbaru yang diklaim cepat, aman dan modern . Untuk mengetahui kinerja kedua protokol tersebut dilihat dari data yang akan diambil yaitu berupa *throughput*, *delay*, *jitter* dan *packet loss*.

Beberapa penelitian yang dijadikan acuan pada penelitian ini ditampilkan pada Tabel 2.1.

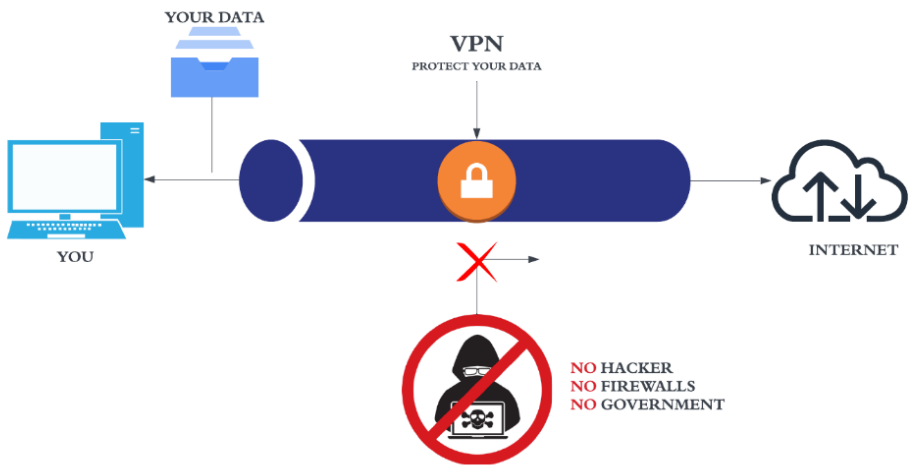
Tabel 2.1 Penelitian Terdahulu

Year	***Author***	***Objective***	***Protocol***	***Result***
2018	Wa Ode Zamalia	Melakukan analisis dan perbandingan protokol PPTP, L2TP, SSTP dan IPSEC	PPTP, L2TP, SSTP dan IPSEC	Hasil pengujian keamanan pada tunnel PPTP, L2TP, SSTP, dan IPsec mengindikasikan bahwa tingkat keamanan yang ditegakkan oleh tunnel IPsec menonjol dengan jelas dibandingkan dengan *tunnel* PPTP, L2TP, dan SSTP. Sementara itu, analisis hasil pengujian yang melibatkan berbagai aspek seperti performa, keamanan, serta temuan-temuan pengujian, secara konsisten menegaskan bahwa *tunnel* VPN berbasis IPsec memiliki superioritas yang tidak dapat disaingi oleh *tunnel-tunnel* VPN lainnya, termasuk PPTP, L2TP, dan SSTP.

2020	Lukman, Aiman Mukhlishah	Melakukan analisis dan perbandingan protokol SSTP dan L2TP+IPsec	SSTP dan L2TP+IPsec	Hasil pengujian dari kinerja jaringan bisa diambil *Secure Socket Tunneling Protokol* (SSTP) Dan *Layer Two Tunneling Protokol* (L2TP) + *Internet Protokol Security* (IPSEC) bahwa L2TP+IPsec lebih baik dibanding SSTP, dinilai dari parameter QoS yang sudah diuji dan dibandingkan
2021	Tamsir Ariyadi	Melakukan analisis dan perbandingan protokol IPsec dan VPN *tunnel*	IPsec dan VPN *Tunnel*	Dari hasil perbandingan data IPsec memiliki tingkat keamanan yang lebih tinggi dibandingkan dengan VPN *Tunnel* dengan jalur komunikasi dilengkapi dengan kriptografi.
2022	Dian Novianto, Yohanes Setiawan Japriadi, Lukas Tommy	Melakukan implementasi WireGuard VPN menggunakan metode *remote access*	WireGuard	VPN WireGuard ini mempunyai kelebihan yaitu mudah diimplementasikan dengan kemampuan melakukan enkripsi yang baik menggunakan kunci yang ada pada kedua *peer* dan mekanisme kombinasi antara authentikasi
2021	Adji Putra Pamungkas, Muhammad Reza Putra, Muhammad Hafizh	Melakukan perbandingan protokol PPTP dan L2TP	PPTP Dan L2TP	Berdasarkan pengujian yang dilakukan dengan protokol PPTP dan L2TP, sistem keamanan yang diterapkan menunjukkan bahwa kedua protokol L2TP berkinerja lebih baik daripada PPTP

2.2 *VIRTUAL PRIVATE NETWORK* (VPN)

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan pengguna untuk terhubung ke jaringan publik dan menggunakan jaringan tersebut untuk bergabung dengan jaringan lokal. VPN bekerja dengan menghubungkan satu titik atau node pada jaringan komputer ke titik lainnya melalui perantaraan jaringan lain yang dapat diilustrasikan pada gambar 2.1. Titik ini bisa berupa jaringan komputer lokal (dikenal sebagai LAN) atau sebuah komputer. VPN merupakan cara aman untuk mengakses *Local Area Network* (LAN) yang berada di suatu lokasi dengan menggunakan internet atau jaringan publik lainnya untuk mentransmisikan data paket secara pribadi melalui enkripsi. Hal ini memerlukan penerapan teknologi tertentu untuk memastikan bahwa meskipun menggunakan jaringan umum, *traffic* antara *remote site* tidak dapat disadap dengan mudah dan mencegah akses yang tidak sah ke dalam *remote site*. Dengan adanya jaringan VPN, privasi jaringan dapat diperluas di jaringan publik, sehingga pengguna dapat mengirim dan menerima informasi melalui jaringan publik seolah-olah mereka terhubung langsung ke dalam sistem tertutup. Oleh karena itu, aplikasi yang berjalan melalui VPN memberikan manfaat dalam hal fungsionalitas, keamanan, dan pengelolaan jaringan pribadi [6].



Gambar 2.1 Ilustrasi Kerja VPN [7]

Keuntungan menggunakan VPN termasuk penghematan biaya dan kemampuan untuk mentransfer data atau melakukan *remote view* untuk

mengendalikan komputer dari rumah atau kantor, serta dari tempat mana pun. VPN dapat menjadi alternatif teknologi yang relatif murah untuk menghubungkan jaringan lokal yang luas, karena transmisi data menggunakan infrastruktur jaringan publik yang sudah ada, tanpa memerlukan pembangunan jaringan pribadi. Namun, ada beberapa kelemahan dari penggunaan VPN, terutama karena mengandalkan jaringan publik seperti internet yang tidak dapat kita prediksi. Ini bisa dimengerti karena koneksi terjadi pada jaringan milik pihak lain, sehingga kita tidak memiliki kontrol penuh atas jaringan tersebut [8].

2.2.1 Fungsi VPN

Teknologi VPN menawarkan berbagai fungsi utama untuk penggunaannya, di antaranya adalah sebagai berikut [9]:

1. *Confidentially* (Kerahasiaan)

   VPN adalah teknologi yang menggunakan jaringan internet atau jaringan publik yang memiliki potensi rawan terhadap pencurian informasi atau data. Oleh karena itu, VPN menggunakan metode enkripsi untuk mengacak data yang melewati jaringan. Dengan penggunaan metode enkripsi ini, keamanan data menjadi lebih terjamin dari pencurian data. Meskipun ada kemungkinan bagi pihak-pihak tertentu untuk menyadap data yang melewati jaringan internet atau jalur VPN itu sendiri, namun data yang disadap tersebut tidak dapat dibaca karena telah diacak sebelumnya. Fungsi *confidentially* dalam VPN bertujuan untuk memastikan bahwa data yang ditransmisikan hanya dapat diakses oleh orang yang memiliki hak akses yang sah. Dengan demikian, data tersebut tetap terlindungi dari akses yang tidak sah.

2. Data *Intergrity* (Keutuhan data)

   Teknologi VPN memiliki kemampuan untuk menjaga keutuhan informasi atau data sejak data dikirim hingga sampai ke tujuan akhir. Dengan demikian, data yang sedang dalam perjalanan dapat terhindar dari berbagai gangguan seperti hilangnya data, kerusakan data, atau manipulasi data oleh pihak-pihak yang tidak bertanggung jawab.

3. *Origin Authentication* (Autentikasi sumber)

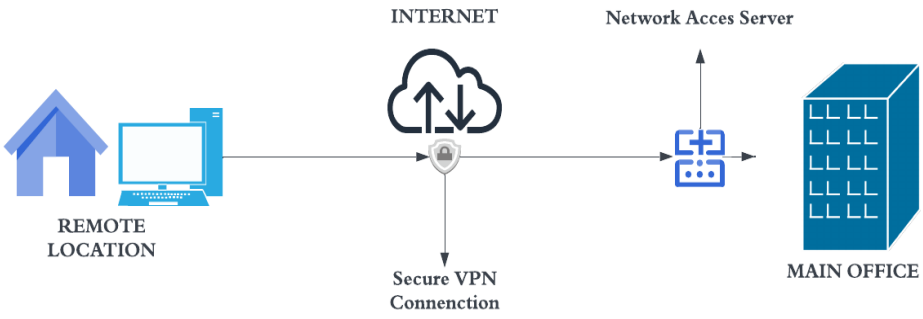
VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber pengiriman data sebelum data diterima. Dengan demikian, VPN dapat memeriksa dan mengakses informasi tentang sumber data yang masuk. Jika proses autentikasi berhasil, alamat sumber data akan disetujui. Hal ini memastikan bahwa VPN dapat menjamin semua data yang dikirimkan dan diterima berasal dari sumber yang sah dan benar-benar seharusnya. Dengan adanya autentikasi ini, tidak ada informasi atau data yang dapat dikirimkan oleh pihak lain atau data yang dipalsukan yang dapat lolos dan diterima oleh VPN.

2.2.2 Jenis-jenis VPN

Seiring berjalannya waktu, teknologi VPN berkembang menjadi beberapa jenis, yaitu [10]:

1. *Remote Access* VPN

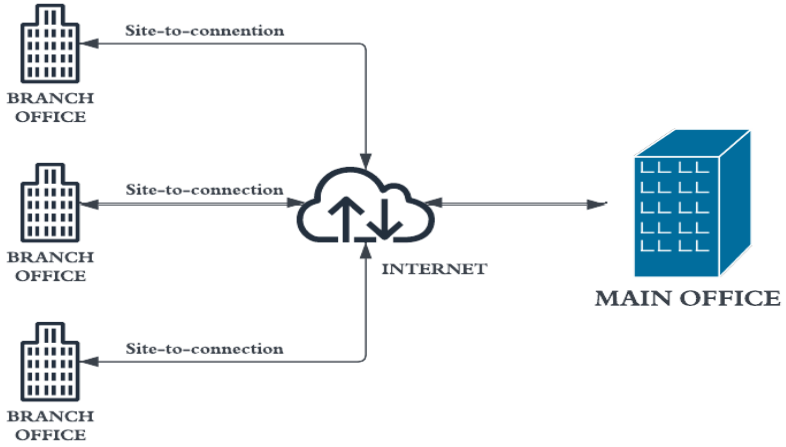
   Tipe VPN ini memungkinkan pegawai yang sedang bekerja di luar kantor atau di luar negara untuk mengakses jaringan LAN di kantor pusat melalui internet. Keunggulan ini terutama bermanfaat untuk menerima *email* yang tersedia di jaringan LAN kantor pusat. Selain itu, manfaat serupa juga berlaku untuk kantor cabang yang tidak memiliki koneksi langsung ke kantor pusat. Kantor cabang tersebut dapat melakukan koneksi lokal melalui layanan *dial-up* ke sebuah ISP dan selanjutnya terhubung ke kantor pusat, sebagaimana diilustrasikan dalam Gambar 2.2.



Gambar 2.2 *Remote Access* VPN [11]

2. *Site-to-Site* VPN

Site-to-Site VPN merupakan solusi yang memungkinkan perluasan jaringan pribadi (*private network*) melalui jaringan internet atau layanan publik lainnya dengan cara yang aman, seperti terlihat pada gambar 2.2. Dikenal juga dengan sebutan LAN to LAN VPN, *Site-to-Site* VPN berfungsi sebagai alternatif dari infrastruktur WAN yang biasanya menghubungkan kantor cabang, kantor pusat, atau mitra bisnis dengan seluruh jaringan yang ada di perusahaan sebagaimana diilustrasikan dalam gambar 2.3.



Gambar 2.3 *Site-to-Site* VPN [12]

Site-to-Site VPN juga dibedahkan menjadi dua jenis yaitu:

a. Internet VPN

VPN internet digunakan untuk menghubungkan kantor pusat dengan kantor cabang atau lokasi kantor yang berjauhan melalui infrastruktur publik.

b. *Extranet* VPN

Extranet VPN adalah bentuk perluasan dari internet suatu perusahaan yang memungkinkan integrasi pengguna dari luar perusahaan, seperti pemasok, penjual, pelanggan, dan mitra bisnis lainnya. Melalui *Extranet* VPN, kedua perusahaan dapat saling bertukar informasi dengan cepat dan mudah, sambil tetap menjaga keamanan jaringan internet dengan menggunakan *firewall*.

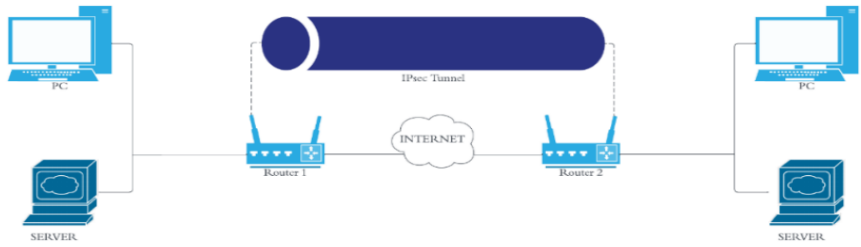
2.3 VPN PROTOKOL

Protokol adalah bahasa atau standarisasi yang digunakan oleh dua buah media komputer atau lebih untuk agar dapat saling berkomunikasi. Beberapa protokol yang digunakan untuk pengembangan VPN adalah sebagai berikut:

a. IPsec

Teknologi keamanan yang paling banyak digunakan dan sangat penting adalah *Internet Protokol Security* (IPsec). IPsec digunakan di otentikasi dan enkripsi di internet publik untuk memberikan akses yang aman. IPsec adalah sekumpulan protokol yang fungsinya untuk mengamankan komunikasi melalui Internet Protokol (IP) dengan mengautentikasi dan atau mengenkripsi setiap paket IP dalam aliran data sebagaimana diilustrasikan dalam gambar 2.4. IPsec juga termasuk protokol untuk membangun kunci enkripsi. Protokol IPsec bekerja pada lapisan jaringan, lapisan 3 dari model OSI. Protokol keamanan internet tambahan lainnya seperti SSL, TLS dan SSH beroperasi dari lapisan aplikasi (Lapisan 7 model OSI). Ini membuat IPsec lebih fleksibel karena dapat digunakan untuk melindungi Layer 4 protokol, termasuk TCP dan UDP [13].

IPsec, singkatan dari *Internet Protocol Security*, merupakan sebuah kerangka standar terbuka yang merangkumi sekumpulan Protokol Internet (IP) yang bertindak sebagai solusi krusial dalam menjaga keamanan komunikasi. Fokus utamanya meliputi pelaksanaan enkripsi yang kuat, otentikasi yang andal, dan pertukaran kunci yang terpercaya dengan memanfaatkan berbagai algoritma yang sudah tersedia. Dalam mengusung standar ini, Cisco telah muncul sebagai pionir yang tak hanya mengusulkan, tetapi juga sukses menerapkan IPsec sebagai standar atau rangkaian standar serta teknologi yang merumuskan akses VPN Jarak Jauh. IPsec beroperasi melintasi tiga lapisan dalam model OSI, dan mengemban tugas penting dalam melindungi serta mengotentikasi paket-paket IP yang berpindah antara perangkat-perangkat IPsec yang berpartisipasi, atau sering disebut sebagai peer. Terutama digunakan untuk mewujudkan Jaringan Pribadi Virtual (VPN) dan memfasilitasi akses pengguna dari lokasi yang jauh. Salah satu keunggulan krusial dari IPsec adalah kemampuannya dalam mengelola pengaturan keamanan [14].

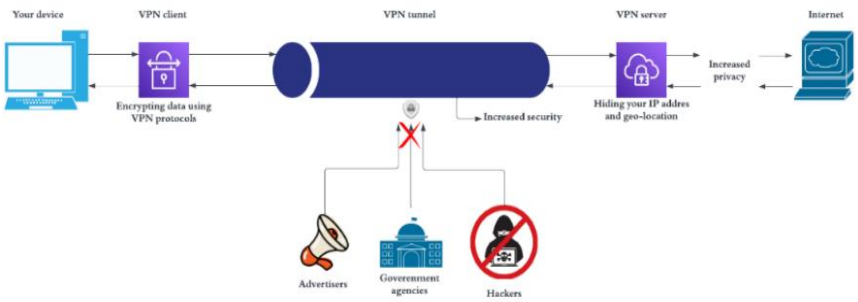


Gambar 2.4 Ilustrasi Kerja IPsec [15]

b. WireGuard

WireGuard adalah salah satu tipe VPN yang sederhana namun cepat , aman dan modern. Saat ini WireGuard juga sudah mendukung *cross platform* (Linux, windows, macOS, BSD, iOS, dan Android). WireGuard tidak mengenal yang namanya server dan *client* karena WireGuard menggunakan konsep *peer* (saling berhubungan) sebagaimana diilustrasikan dalam gambar 2.5. WireGuard merupakan VPN L3 baru yang diusulkan oleh Jason Donenfeld pada tahun 2017. Ini mendefinisikan protokolnya sendiri dan dilengkapi dengan implementasi referensi sebagai modul kernel Linux pada tahun 2019 dengan modul kernel ini sebelum WireGuard tersedia di kernel jalur utama. [16].

Protokol WireGuard dikembangkan dari awal, berbasis pada praktik kriptografi terbaik dan menggunakan cipher terbaru. Bertentangan dengan protokol yang dipandu komite seperti IPsec, WireGuard sangat berpendirian pada topik tertentu dan termasuk ide radikal. Hal tersebut menghilangkan kelincahan kriptografi dengan mengunci dalam satu *cipher* AEAD dan algoritma autentikasi tanpa negosiasi fitur : ChaCha20-poly1305 [17].



Gambar 2.5 Ilustrasi Kerja WireGuard [18]

Penggunaan primitif kriptografi berkecepatan tinggi menjadikan WireGuard hidup di dalam kernel Linux dimana dapat membuat jaringan menjadi aman dan berkecepatan tinggi. Performa WireGuard yang baik membuatnya cocok untuk perangkat kecil seperti *smartphone* dan *router backbone* yang dimuat. Kekhasan penting lainnya tentang protokol WireGuard VPN adalah bahwa keseimbangan koneksi terjadi setiap beberapa menit untuk memberikan *rotating key* untuk kerahasiaan ke depan yang sempurna. Hal ini dilakukan berdasarkan waktu daripada paket data [19].

2.3.1 Enkripsi Algoritma VPN

Enkripsi algoritma VPN mengacu pada penggunaan algoritma kriptografi yang kuat untuk melindungi data yang dikirim melalui jaringan dalam sebuah VPN (*Virtual Private Network*). Tujuan utama enkripsi algoritma VPN adalah untuk menjaga kerahasiaan, integritas, dan keaslian data yang ditransmisikan antara perangkat yang terhubung dalam jaringan VPN [20].

AES (*Advanced Encryption Standard*) adalah sebuah algoritma enkripsi yang kuat dan sangat umum digunakan dalam berbagai aplikasi dan protokol yang melibatkan keamanan data. AES merupakan pengganti dari algoritma DES (*Data Encryption Standard*) yang sudah usang. Enkripsi algoritma AES menggunakan blok enkripsi simetris dengan panjang kunci yang bisa menjadi 128-bit, 192-bit, atau 256-bit. Algoritma ini bekerja dengan membagi data yang akan dienkripsi menjadi blok-blok yang sama besar, dan kemudian setiap blok akan dienkripsi secara independen menggunakan kunci enkripsi yang sama. AES menggunakan serangkaian langkah enkripsi yang meliputi penggantian (substitusi), pergeseran (*shift*), dan pencampuran (*mixing*) bit untuk mengacak dan mengubah data. Proses ini melibatkan iterasi sejumlah putaran enkripsi (10, 12, atau 14 putaran tergantung pada panjang kunci) untuk mencapai tingkat keamanan yang diinginkan [21].

2.4 KEAMANAN JARINGAN

Istilah "keamanan jaringan" mencakup berbagai teknik, alat, dan teknologi. Secara sederhana dijelaskan, sistem keamanan jaringan adalah cara untuk mengidentifikasi dan memblokir pengguna yang tidak sah untuk bergabung ke dalam jaringan. Keamanan jaringan berupaya meramalkan kemungkinan cedera

fisik, serangan, dan pencurian data [22]. Keamanan jaringan adalah teknik atau sistem yang digunakan untuk mempertahankan jaringan dari beberapa serangan eksternal yang dapat merusak jaringan dan mencuri informasi [23].

Keamanan jaringan adalah konsep yang tidak jelas. Hal ini dilakukan untuk memastikan keamanan bahkan ketika perintah atau program tertentu digunakan oleh okultisme atau entitas rahasia. Dengan memeriksa pengguna yang mencoba mengakses jaringan melalui *proxy* atau *firewall*, keamanan jaringan ditunjukkan [24]. Menurut survei, salah satu aspek terpenting dalam menyiapkan jaringan komputer adalah keamanan jaringan. Sebagian besar jaringan komputer yang mengalami masalah adalah akibat dari kelalaian administrator jaringan selama penyiapan jaringan. Sehingga, mungkin ada peluang bagi peretas untuk berkompromi dengan jaringan bawaan. Lebih banyak keamanan jaringan harus dikembangkan untuk mencegah peretas menyalahgunakan jaringan [25].

Karena keamanan merupakan salah satu kebutuhan yang sangat penting bagi perusahaan, khususnya korporasi, keamanan jaringan merupakan kemajuan teknologi yang sangat signifikan. Karena bisnis di industri jasa sangat bergantung pada akses jaringan internet yang andal dan pertumbuhan dunia digital, keamanan sangat penting untuk kelancaran operasi perusahaan yang menawarkan layanan tur dan perjalanan. Jaringan internet sekarang digunakan oleh organisasi selain konsumen dan bisnis. Anak-anak dapat mengakses berbagai sumber informasi buku pelajaran atau sekedar pengetahuan dasar melalui jaringan internet. Jaringan di internet khususnya dapat dimanfaatkan oleh pelaku bisnis untuk mencari sumber informasi yang cepat dan terpercaya [26].

2.5 TCP DAN UDP

a. TCP (*Transmission Control Panel*)

Dalam buku Hasnul Arifin (2011), dijelaskan bahwa TCP/IP adalah salah satu perangkat lunak jaringan komputer yang ada dalam sistem dan digunakan untuk mengirim dan menerima data dalam Local Area Network (LAN) maupun Internet. TCP merupakan singkatan dari *Transmission Control Protocol* dan IP merupakan singkatan dari Internet Protokol. Nama "TCP/IP" digunakan karena keduanya selalu berperan bersama dalam proses komunikasi data. Saat ini,

TCP/IP sering digunakan dalam banyak jaringan komputer lokal (LAN) yang terhubung ke Internet karena memiliki beberapa sifat penting:

1. TCP/IP adalah protokol standar yang bersifat terbuka, gratis, dan dikembangkan secara independen dari perangkat keras komputer tertentu. Keberadaan protokol ini mendapatkan dukungan luas dari vendor perangkat keras, sehingga TCP/IP berfungsi sebagai penyatuan berbagai merek perangkat keras komputer. Ini memungkinkan komputer-komputer yang menggunakan perangkat keras dan perangkat lunak yang berbeda untuk tetap dapat berkomunikasi dan bertukar data melalui Internet
2. TCP/IP memiliki sifat yang mandiri dari perangkat keras jaringan apa pun, yang memungkinkannya untuk terhubung dengan berbagai jaringan komputer. Protokol TCP/IP dapat beroperasi melalui berbagai jenis koneksi, termasuk ethernet, saluran *dial-up*, dan bahkan dapat berfungsi secara virtual melalui berbagai media fisik untuk mentransmisikan data.
3. Protokol TCP/IP dapat berfungsi sebagai alamat umum, sehingga setiap perangkat yang menggunakan TCP/IP akan memiliki alamat yang unik dalam jaringan komputer lokal maupun dalam jaringan komputer global seperti internet [27].

b. UDP (*User Datagram Protokol*)

UDP merupakan salah satu protokol utama yang beroperasi di atas IP dan memiliki karakteristik sebagai protokol transport yang lebih sederhana jika dibandingkan dengan TCP. UDP digunakan dalam situasi di mana mekanisme reliabilitas tidak menjadi hal utama. Dengan kata lain, komunikasi menggunakan protokol UDP akan terus berlangsung tanpa memperhatikan koneksi antara sumber dan tujuan data [28].

2.6 PARAMETER QUALITY OF SERVICE

Quality of Service diartikan sebagai sebuah mekanisme yang memberikan kemampuan admistrator jaringan untuk mengelola *bandwidth, delay, jitter, loss,* dan *congestion* dari *throughput* dalam sebuah jaringan. QoS diperuntukkan untuk memenuhi kebutuhan layanan yang berbeda tetapi menggunakan infrakstruktur yang sama dan untuk mendefinisikan atribut layanan yang disediakan baik secara

kualitas dan kuantitas. Tingkatan QoS yang digunakan pada penelitian ini yaitu *Best-effort service* [29]. Tujuan dari QoS adalah untuk memberikan jaminan atas kemampuan sebuah jaringan untuk memberikan hasil yang dapat diprediksi. Berbagai parameter bisa menunjukkan kinerja jaringan akses Internet, seperti parameter *throughput*, *delay*, *jitter*, *packet loss* yang dapat dikategorikan pada tabel 2.2.

Tabel 2.2 Standar TIPHON QoS [30]

Nilai	Presentase (%)	Indeks
3,8 – 4	100	Sangat bagus
3 – 3,79	75 – 94,75	Bagus
2 – 2,99	50 – 74,75	Sedang
1 – 1,99	25 – 49,75	Buruk

a. *Delay*

Delay diartikan sebagai besarnya waktu yang diperlukan untuk menempuh jarak pengiriman antara titik awal dan titik akhir. Jarak, media fisik, kongesti, atau waktu proses yang berkepanjangan semuanya dapat berperan dalam menciptakan munculnya *delay* [31]. Menurut TIPHON versi terbaru, *delay* dapat dikategorikan pada tabel 2.2.

Tabel 2.3 Kategori *Delay*[30]

Kategori *Delay*	*Delay*
Sangat Bagus	< 150 m/s
Bagus	150 s/d 300 m/s
Sedang	300 s/d 450 m/s
Buruk	> 450 m/s

Adapun perhitungan *delay* menggunakan persamaan (2.1):

$$Delay(\text{ms}) = \frac{\text{Total } delay}{\text{Total paket yang diterima}} \quad \textbf{(2. 1)}$$

b. *Packet Loss*

Packet loss adalah salah satu QoS yang paling signifikan untuk metrik kinerja karena akan mempengaruhi banyak aplikasi seperti VoIP. Kinerja

menurun drastis jika paket *loss* melebihi batas tertentu, dan akan menjadi tidak dapat digunakan jika *packet loss* sangat besar [31]. Nilai standar *packet loss* rekomendasi menggunakan standar TIPHON TR 101 328, dapat dilihat pada Tabel 2.3.

Tabel 2.4 Kategori *Packet Loss* [30]

Kategori	*Packet Loss*
Sangat Bagus	0%
Bagus	3%
Sedang	15%
Buruk	25%

Adapun perhitungan *Packet Loss* menggunakan persamaan (2.2):

$$Packet\ Loss = \frac{Packet\ Send - Packet\ Received}{Packet\ Sent} \times 100\% \qquad \textbf{(2. 2)}$$

c. *Throughput*

Troughput didefinisikan sebagai ukuran seberapa cepat (*rate*) proses transfer data efektif yang dapat dilakukan. Ini adalah ukuran angka paket data yang dikirim atau diterima melalui jaringan sehingga bisa didefinisikan sebagai *bandwidth* aktual yang tersedia untuk jaringan, diukur dalam bit per detik (bps). Dengan bertambahnya di latensi jaringan, *throughput* jaringan berkurang. Adapun besaran *throughput* sendiri dihitung dengan bps. *Troughput* juga dapat diartikan sebagau jumlah total penyampaian paket data yang berhasil terkirim. Nilai *Throughput* dapat dikategorikan pada tabel 2.5 [31].

Tabel 2.5 Kategori *Throughput* [32]

Kategori *Throughput*	*Throughput*	Indeks
Sangat Bagus	>2,1Mbps	4
Bagus	1200 kbps – 2,1 Mbps	3
Sedang	700 – 1200 kbps	2
Buruk	<700 kbps	1

Adapun Perhitungan *throughput* menggunakan persamaan (2.3):

$$Throughput = \frac{\text{Jumlah data yang dikirim}}{\text{Waktu pengiriman data}} \quad \textbf{(2. 3)}$$

d. *Jitter*

Jitter adalah efek yang tidak diinginkan yang disebabkan oleh ketidaksetaraan penyimpangan dalam interval waktu perjalanan paket data. Alih-alih tetap konstan, penundaan antara setiap paket bervariasi. *Jitter* dalam jaringan dapat disebabkan oleh antrian yang tidak tepat, kemacetan jaringan, atau kesalahan konfigurasi. *Jitter* pun bisa menyebabkan kemacetan jaringan dan kehilangan paket. Jaringan penyedia layanan harus menyediakan *bandwidth* yang cukup dan kemungkinan latensi untuk memastikan koneksi jaringan yang berkualitas, itu dapat membantu mengurangi *jitter*. Nilai *jitter* dapat dikategorikan pada tabel 2.6 [31].

Tabel 2.6 Kategori *Jitter* [30]

Kategori *Jitter*	Peak *Jitter*
Sangat Bagus	0 m/s
Bagus	0 s/d 75 m/s
Sedang	76 s/d 125 m/s
Buruk	> 225 m/s

Adapung perhitungan *jitter* menggunakan persamaan (2.4):

$$Jitter = \frac{\text{Total variasi } delay}{\text{paket data diterima-1}} \quad \textbf{(2. 4)}$$