Analisis Perbandingan Performansi QoS VPN *Encryption Protocol* Pada Jaringan Berbasis *Hybrid Cloud* (Studi kasus disalah satu Group Perusahaan Retail dan Industrial)

Tubagus Entus Madhadi dan Lintang Yuniar Banowosari

Sistem Informasi, Ilmu Komputer, Universitas Gunadarma
Jalan Margonda Raya No. 100, Pondok Cina, Depok, Jawa Barat 16424
E-mail : tb.entus.madhadi@gmail.com, lintang@staff.gunadarma.ac.id

Abstrak

Penelitian dilakukan pada salah satu grup perusahaan yang bergerak pada sektor ritel dan industrial dengan 975 *store* yang tersebar diwilayah Indonesia, dalam menunjang operasionalnya IT Corporate menyediakan *core system* yang terbagi di private dan *public cloud* atau dikenal dengan *hybrid cloud* terdiri dari *storage*, *database*, SAP, dan aplikasi pendukung lainnya. Media komunikasi antara *branch store* dan *main office* sebagian besar menggunakan VPN *tunnel* jenis EOIP, L2TP, PPTP dan SSTP, tanpa dukungan kombinasi enkripsi yang maksimal sehingga perlindungan data belum memenuhi standar keamanan informasi ISO 27001. Grup perusahaan tersebut juga terdaftar di Kominfo sebagai penyelenggara sistem elektronik karena mengelola data pelanggan, hal ini menjadi bahan pertimbangan penelitian yang mengacu pada analisis perbandingan VPN *tunnel* jenis L2TP/IPSec, OpenVPN, dan IKEV2/IPSec karena ketiganya dapat dikombinasikan dengan enkripsi IPSec dan SSL sebagai peningkatan perlindungan *traffic data*, ketiganya akan diuji pada performansi QoS dengan metode *Applied Research* guna memastikan performansi yang diuji sesuai dengan kebutuhan dan kompabilitas *core system* dengan basis jaringan *hybrid cloud*. Hasil penelitian yang diperoleh menunjukan bahwa IKEV2/IPSec secara signifikan memiliki nilai QoS yang lebih baik dengan rata-rata *throughput* 22 Mb/s, *packet loss* 0,12%, delay 0,408 ms dan *jitter* 0,408 ms, yang artinya secara kualitas jaringan lebih baik mulai dari peningkatan kecepatan transfer data, kecilnya total kehilangan paket dan delay waktu yang dibutuhkan saat paket dikirim dari sumber ke tujuan.

Kata kunci : Analisis, VPN, QoS, *Hybrid Cloud* dan *Applied Research*

Pendahuluan

Pemanfaatan koneksi internet saat ini menjadi pilihan utama dalam mendukung tersedianya komunikasi yang handal dan tanpa batas waktu, infrastruktur internet service provider hingga tahun 2021 dibangun sangat masif dan maju sehingga mempermudah siapa saja menggunakan internet dengan berbagai macam perangkat yang ada, pemanfaatan lain koneksi internet di sektor industry dan retail adalah membangun media komunikasi untuk mempersingkat proses kerja dan mengolah informasi disisi branch dan *data center*, terlebih sebagai layanan transmisi data, namun disamping banyaknya kelebihan terdapat juga kelemahan yang perlu diwaspadai seperti data leak atau kebocoran data, konsekuensi yang perlu diperhatikan adalah bagaimana menjamin keamanan komunikasi yang dibangun melalui jaringan koneksi internet, upaya yang dapat dilakukan adalah dengan membangun jaringan private yang terenkripsi pada jaringan public atau internet yang dikenal dengan *virtual private network*.

Virtual Private Network (VPN) adalah teknologi komunikasi yang memanfaatkan koneksi internet untuk membangun *tunnel* melalui jaringan publik dan menggunakannya untuk terkoneksi ke jaringan lokal secara langsung, dengan cara tersebut maka diperoleh hak akses dan policy yang sama seperti halnya berada di dalam jaringan lokal walaupun sebenarnya menggunakan jaringan publik. Jaringan VPN merupakan jaringan yang dibangun di atas sebuah *tunnel* [1].

Studi kasus pada penelitian dilakukan disalah satu group perusahaan yang bergerak di sektor per-

DOI : http://dx.doi.org/10.32409/jikstik.20.1.2695

dagangan dibagi menjadi beberapa bisnis unit yang terdiri dari retail, industrial, e-commerce, *food* and *beverages, manufacturing, service* and *property*, semua bisnis unit tersebut tersebar dibeberapa wilayah dan internet menjadi salah satu penunjang operasional perusahaan. Semua aktifitas kerja yang dilakukan karyawan grup perusahaan berjalan di dua lokasi berbeda baik *main office* maupun *branch store*, untuk memenuhi kelancaran dan keamanan komunikasinya perusahaan menyediakan koneksi point to point dengan harapan memiliki koneksi cepat, reliable maupun aman, hal ini dapat dipenuhi dengan mempertimbangankan berbagai layanan VPN yang tersedia, baik yang bersifat proprietary maupun komersial. Prosedur pemilihan VPN untuk interkoneksi branch dan *main office* di group perusahaan tersebut dipilih secara acak bergantung pada kompabilitas koneksi ISP dengan VPN yang dipilih, umumnya yang digunakan adalah EOIP, PPTP, L2TP dan SSTP, model VPN tersebut berjalan menggunakan *tunnel* sebagai encapsulation traffic tanpa dukungan kombinasi IPSec atau pun SSL sehingga retan terhadap pemindaian dan kebocoran informasi. Pilihan layanan VPN dapat mempengaruhi bisnis proses yang berjalan kaitannya terhadap regulasi keamanan informasi elektronik yang ditetapkan oleh Kominfo karena perusahaan tersebut terdaftar sebagai penyelenggara sistem elektronik.

Secara bisnis informasi elektronik yang dikelola group perusahaan ini berupa pengelolaan informasi pelanggan (member card) yang terdiri dari 3 bisnis unit (Ace Hardware Indonesia, Informa dan Chatime) dengan total jumlah member sekitar 5 juta ditahun 2020, selain itu perusahaan tersebut juga terdaftar dan diawasi oleh OJK (Otoritas Jasa Keuangan) sebagai penyelenggara transaksi keuangan untuk salah satu bisnis unit lain yaitu PT. Dana Kini Indonesia, sehingga perlu mengikuti regulasi dan *security* compliance ISO 27001 sebagai salah satu syarat standar keamanan informasi yang ditetapkan Kominfo maupun OJK.

ISO 27001 menyediakan informasi kerangka kerja dalam penggunaan teknologi informasi dan pengelolaan asset yang dapat membantu sebuah organisasi atau perusahaan dengan memastikan bahwa keamanan informasi yang diterapkan sudah efektif, ada juga ISO 27002 yang menyediakan kerangka kerja tentang kontrol keamanan yang dapat dijalankan oleh sebuah instansi yang telah mengimplementasikan ISO 27001, hal ini termasuk kemampuan akses data dalam menjaga kerahasiaan, berkelanjutan, dan integritas atas informasi yang dimiliki [2].

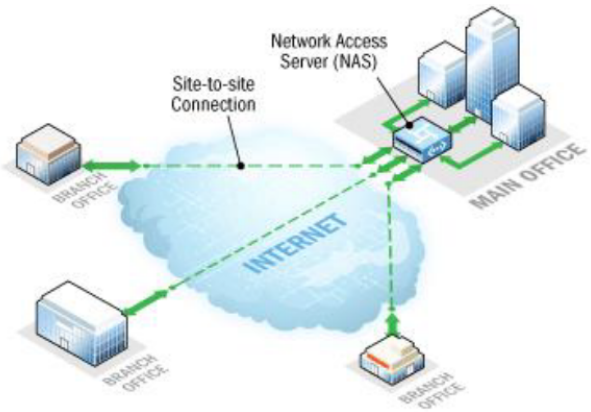
Pemenuhan evidence di ISO 27001 untuk keamanan informasi baru berjalan di *main office*, sedangkan di *site* atau *branch* pelaksanaa audit belum dapat dilakukan hingga kesiapan infrastruktur yang memadai, namun dengan berkembangnya teknologi VPN dari berbagai model yang ada telah melakukan pengembangan akan keamanan dan performansi koneksinya seperti OVPN, L2TP/IPSEC dan IKEV2, alasannya adalah selain menyediakan *tunnel interface* untuk enkapsulasi koneksi ketiganya dapat dikombinasikan juga dengan IPSec ataupun SSL. Kombinasi ini penting mengingat syarat transmisi data yang aman adalah berlangsungnya proses enkripsi dan dekripsi sehingga dapat menjadi pertimbangan untuk menggantikan model VPN yang berjalan *base on tunnel interface* di group perusahaan tersebut. IPSec merupakan skema keamanan *end to end* yang beroperasi didalam jaringan internet. Penggunaa IPSec dapat mengenkripsi data yang di transmisikan melalui *tunnel* antara *host to host* dan *network* to *network* atau di sebagian *network* tertentu dengan *host* [3].

Penelitian ini dilakukan untuk menguji 3 model VPN *tunnel* OpenVPN, L2TP/IPSec, dan IKEV2 terhadap performansi QoS, dengan harapan dapat menerapkan salah satu permodelan VPN terbaik berdasarkan hasil analisis sesuai dengan performansi dan kompabilitasnya.

Adapun manfaat yang didapatkan perusahaan/instansi, bidang keilmuan dan masyarakat sebagai hasil dari penelitian ini adalah yang pertama menjadi bahan pertimbangan untuk meningkatkan keamanan dan performansi koneksi VPN khususnya dalam transmisi data store ke *data center* di group perusahaan tersebut. Kedua, memberikan opsi dan alternatif menggunakan VPN untuk menghubungkan jaringan lokal yang luas, aman dengan biaya implementasi yang lebih rendah.

Virtual Private Network (VPN)

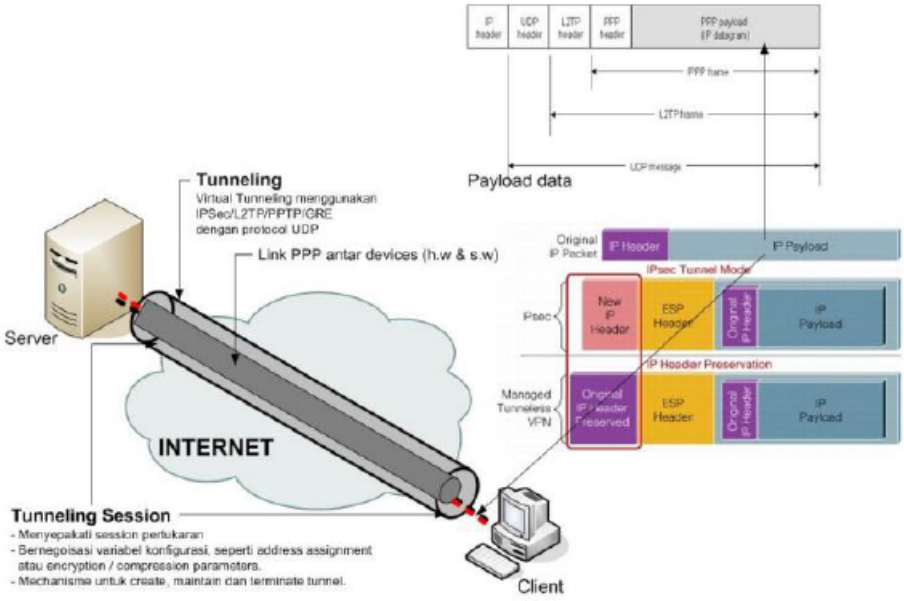
Virtual Private Network (VPN), perluasan jaringan *private* pada jaringan *public* yang memungkinkan pengguna untuk kirim dan memperoleh informasi melalui lintas koneksi yang disatukan atau jaringan *public* yang seolah-olah memanuver komputasi koneksi langsung dengan sistem tertutup. Aplikasi yang berjalan melalui VPN dapat memperoleh berbagai manfaat mulai dari fungsionalitas, keamanan, dan manajemen yang utuh [4]. Gambar 1 menunjukan jenis VPN tipe site-to-site dengan menyajikan satu VPN concentrator yang ditempatkan pada *main office* dan VPN *client* di *branch office*.



Gambar 1: Ilustrasi VPN

Saat ini VPN digunakan oleh hampir semua bisnis yang membutuhkan perluasan operasi secara geografis tanpa banyak berinvestasi dalam pengembangan infrastruktur TI lebih dulu dengan menggunakan solusi hemat dan teknologi tepat seperti VPN.

Gambar 2 menunjukan skema *tunneling* IPSec yang terhubung antara *client* VPN dan *gateway* IPSec. Pertama, *traffic* dari *client* dienkripsi, selanjutnya dienkapsulasi dalam paket IP baru, setelah itu dikirim ke ujung lainnya, ketika *traffic* dienkripsi oleh firewall, paket IP dari *client* dikirim ke jaringan lokal [6].



Gambar 2: Skema *Tunneling* VPN [5]

Keamanan Jaringan

Keamanan jaringan komputer didefinisikan sebagai perlindungan sumber daya terhadap upaya perubahan dan penghancuran yang disebabkan oleh seseorang yang tidak diperbolehkan, ada dua hal yang terkait dengan keamanan dan kerahasiaan data dalam jaringan komputer yaitu keterwakilan data dan kompresi data, yang kemudian dikaitkan dengan masalah enkripsi [7].

Enkripsi dan Dekripsi

Enkripsi merupakan proses merubah data ke dalam bentuk yang hanya bisa dibaca oleh penerima yang diinginkan didukung dengan kombinasi algoritma enkripsi yang digunakan, untuk dapat membaca pesan yang telah dienkripsi penerima data harus memiliki kunci enkripsi yang sama [8]. Sedangkan Dekripsi merupakan proses mengembalikan data rahasia ke data aslinya, dekripsi juga merupakan satu kaidah upaya pengolahan data menjadi sesuatu yang dapat secara jelas dan tetap dengan tujuan agar dapat dimengerti oleh manusia secara langsung [9].

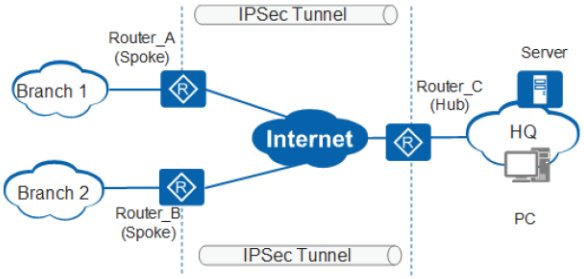
Internet Security Protocol (IPSec)

IPSec merupakan sebuah metode enkripsi yang digunakan untuk melindungi kerahasiaan, dan keutuhan data pengguna layanan di jaringan internet [3]. IPSec merupakan jalur data antara komputer atau perangkat pengguna pada jaringan VPN, jalur data hanya bisa diakses dikedua ujung *tunnel* yang di enkapsulasi. Paket IPSec melewati satu ujung tunnel yang lain dan berisi paket data yang dipertukarkan antara pengguna lokal dengan jaringan private. Enkripsi paket data dapat memastikan bahwa data tidak dapat dirusak dimanupulasi dan dibajak pihak ketiga yang berusaha mengakses data diluar koneksi IPSec [10].

IPSec mendukung dua buah sesi komunikasi keamanan, yang pertama adalah protokol *authentication header* (AH), menawarkan otentikasi pengguna dan perlindungan dari beberapa serangan (umumnya serangan man in the middle) dan juga menyediakan fungsi otentikasi terhadap data serta integritas terhadap data. Protokol ini mengizinkan penerima berdasarkan identitas pengirim yang teridentifikasi dan data pun tidak dimanipulasi atau modifikasi selama transmisi berlangsung. Namun, protokol AH tidak menawarkan fungsi enkripsi terhadap data yang ditransmisikannya. Informasi AH dimasukk-

an ke dalam header paket IP yang dikirimkan dan dapat digunakan secara independent atau bersamaan dengan protokol *encapsulating security payload*. Sedangkan yang kedua adalah protokol *encapsulation security payload* (ESP), protokol ini melakukan enkapsulasi serta enkripsi terhadap data pengguna untuk meningkatkan kerahasiaan data. ESP juga dapat memiliki skema algortima otentikasi dan perlindungan dari beberapa serangan dan dapat digunakan secara independen atau bersamaan dengan *authentication header*. Sama seperti halnya AH, informasi mengenai ESP juga dimasukkan ke dalam header paket IP yang dikirimkan [11].

VPN berbasis IPsec menjadi standar industri karena IPsec bersama dengan protokol lainnya menyediakan enkripsi, kompleksitas, dan keamanan yang memadai untuk memastikan integritas data yang dipertahankan sepanjang sesi berjalan [12].



Gambar 3: Typical site-to-multisite IPSec VPN network

Pada Gambar 3 menunjukan tipikal VPN berbasis IPSec yang menjadi standar industri dengan skala *site-to-multisite*, karena menempatkan lebih dari satu koneksi *tunnel*. IPsec bersama dengan protokol lainnya menyediakan enkripsi, kompleksitas, dan keamanan yang memadai untuk memastikan integritas data yang dipertahankan sepanjang sesi berjalan [12].

Socket Secure Layer (SSL/TLS)

Protokol SSL/TLS memiliki dua bagian, yang pertama adalah *handshaking protocol*, yaitu protokol menegosiasi *suite cipher*, mengotentikasi *server* dan secara opsional mengotentikasi *client* dan menetapkan *session key*. Kedua adalah *record protocol*, yaitu protokol mengamankan data aplikasi dengan *session keys* yang dibuat pada *record protocol* dan memverifikasi keaslian dan integritas aplikasi [13]. Dalam sesi menggunakan SSL/TLS, proses yang disebut *client* berkomunikasi dengan proses yang disebut *server*. Secara garis besar, sesi antara *client* dan *server* diamankan dengan, pertama melakukan handshake, lalu mengenkripsi komunikasi antara *client* dan *server* selama sesi berlangsung. Tujuan dari *handshake* adalah *server authentication*, menentukan parameter enkripsi dan *client authentication* [14].

OpenVPN

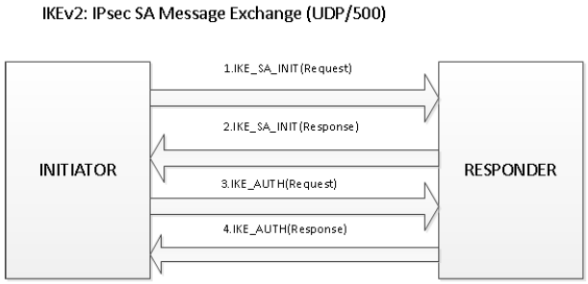
OpenVPN merupakan aplikasi open source untuk membuat *Virtual Private Network* (VPN), aplikasi ini dapat membangun koneksi *point-to-point tunnel* yang terenkripsi dengan mengguinakan kombinasi *keys, certificate*, atau username-password, kombinasi enkripsi tersebut diperlukan pada proses otentikasi berlangsung [7]. L2TP/IPSEC L2TP adalah pengembangan dari teknologi PPTP yaitu *tunneling* yang bekerja di layer 2, L2TP tidak memiliki pengamanan khusus secara umum menggunakan kombinasi IPSec untuk menambah sistem keamanannya. Pengamanan VPN dengan menggunakan enkripsi tertentu sangat diperlukan agar data yang melewati *tunneling* dapat terjaga kerahasiannya [15]. L2TP juga merupakan *tunnel* standar dari satu *router* ke *router* lain atau dari *client* ke host gateway melewati Network Access Server (NAS) ISP yang dianalisa terlebih dahulu oleh Server NAS ISP dan jika proses autentikasi berhasil maka ISP akan membuat saluran dari *client* ke host gateway secara *point-to-point*. L2TP merupakan basis dan kombinasi dari protokol L2F dari Cisco system dan PPTP dari Microsoft [16].

IKEV2

IKEV2 adalah kombinasi protokol IKEV1, ISAKMP dan oakley. IKEV1 dan ISAKMP menentukan cara dua pihak *tunnel* membentuk *security* association. oakley memberikan kerahasiaan yang sempurna dengan menggunakan algoritma pertukaran kunci diffie-hellman. Pihak IKEV2 dapat mengidentifikasi diri mereka sendiri dengan certificate, yaitu protokol otentikasi yang diperluas, atau kunci yang dibagikan sebelumnya di kedua sisi *tunnel*, dengan menggunakan kunci yang dibagikan sebelumnya dalam bentuk kata sandi sederhana dan dikenal oleh kedua belah pihak. IKEV2 berfungsi dalam pertukaran pesan, setiap pesan permintaan yang valid akan memiliki satu pesan balasan yang sesuai. Setiap IKE SA memiliki initiator dan responder. Peran initiator diberikan kepada pihak yang mengirim permintaan Inisialisasi. Sesi IKE dimulai dengan bertukar pesan inisialisasi dan authentication. Setelah mengatur IKE SA, keduanya membuat lebih banyak SA atau mulai mentransfer informasi [17].

Perbedaan yang paling mendasar antara IKEV2 dengan IKEV1 adalah pada pesan yang dikirimkan ketika terjadi pembangunan *tunnel* IPSec. Pada IKEV1 dibutuhkan 9 messages sedangkan pada IKEV2 hanya dibutuhkan 4 messages, oleh karena itulah maka pembangunan *tunnel* IKEV2/IPSec lebih cepat, proses pertukaran otentikasi ditunjukan pada Gambar 4.

Pertukaran Inisialisasi ini (disebut IKE SA INIT) digunakan untuk menegosiasikan algoritma kriptografi, nonce, dan nilai diffie-Hellman.



Gambar 4: Proses pertukaran pesan otentikasi antara initiator dan responder

Cloud Computing

Cloud computing adalah sebuah model komputasi, dimana sumber daya *(hardware) processor/computing power*, *storage*, *network* dan *software* menjadi satu layanan yang saling terintegrasi di jaringan/internet menggunakan pola akses *remote* [18].

Cloud Computing berdasarkan IP service terbagi menjadi tiga, yang pertama adalah Software as a Service (SaaS) yaitu bagian dari *cloud computing* yang terdiri aplikasi untuk digunakan oleh *end user*. Aplikasi biasanya disesuaikan dengan kebutuhan end user. Kedua adalah Platform as a Service (PaaS) yaitu, bagian *cloud computing* yang terdiri aplikasi-aplikasi dasar contohnya sistem operasi, bahasa pemrograman dasar, *database* dan *web server*, dan ketiga adalah Infrastruture as a Service (IaaS) yaitu, bagian *cloud computing* yang berisi blok bangunan dasar untuk IT cloud dan biasanya menyediakan akses ke fitur jaringan, komputer (virtual atau pada perangkat keras khusus), dan ruang penyimpanan data.

Metode Quality of Service (QoS)

Quality of Service (QoS) merupakan metode pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari satu servis. QoS digunakan untuk mengukur sekumpulan atribut kinerja yang telah dispesifikasikan dan diasosiasikan dengan suatu servis [19]. Dalam pengujian performansi QoS mengacu kepada kemampuan memberikan pelayanan berbeda kepada lalu lintas jaringan dengan kelas-kelas yang berbeda. Tujuannya adalah memberikan network service yang lebih baik dan terencana dengan *dedicated bandwidth, jitter* dan *latency* yang terkontrol dan meningkatkan karakteristik *loss* [20].

Parameter Quality of Service (QoS)

Teori trafik yang digunakan untuk menganalisa dan merencanakan jaringan telekomunikasi yang digunakan untuk membawa masing-masing informasi [11]. QoS juga menawarkan kemampuan mendefinisikan atribut-atribut layanan jaringan yang disediakan, baik secara kualitatif maupun kuantitatif, dijelaskan pada Tabel 1.

Tabel 1: Presentase dan Nilai QoS

Nilai	Presentase (%)	Indeks
3,8 – 4	95 – 100	Sangat Memuaskan
3 - 3,79	75 - 94,75	Memuaskan
2 - 2,99	50 - 74,75	Kurang Memuaskan
1 - 1,99	25 - 49,75	Jelek

Menurut versi Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) parameter pengukuran QoS terdiri dari:

Throughput

Kecepatan (rate) transfer data efektif, yang diukur dalam bit per second (bps). *Throughput* adalah jumlah total kedatangan paket yang sukses yang diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut, kategori dan indeks *throughput* ditunjukan pada Tabel 2.

Tabel 2: Kategori *Throughput*

Kategori *Throughput*	*Throughput* (bps)	Indeks
Sangat Bagus	100	4
Bagus	75	3
Sedang	50	2
Jelek	< 25	1

Indeks *throughput* diperoleh melalui persamaan 1:

$$Throughput = \frac{Paket\ data\ diterima}{Lama\ pengamatan} \quad (1)$$

Packet Loss

Parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang dapat terjadi karena collision dan congestion pada jaringan, kategori dan indeks *packet loss* ditunjukan pada Tabel 3.

Tabel 3: Kategori *Packet Loss*

Kategori *Packet Loss*	*Packet Loss (%)*	Indeks
Sangat Bagus	0	4
Bagus	3	3
Sedang	15	2
Jelek	25	1

Indeks *packet loss* diperoleh melalui persamaan 2:

$$Packet\ Loss = \frac{(Paket\ data\ dikirim - Paket\ data\ diterima) x 100\%}{Paket\ data\ dikirim} \quad (2)$$

Delay (Latency)

Waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, congesti atau juga waktu proses yang lama, kategori dan indeks *delay* ditunjukan pada Tabel 4.

Tabel 4: Kategori Delay

Kategori *Delay*	*Delay (ms)*	Indeks
Sangat Bagus	< 150 ms	4
Bagus	150 ms s/d 300 ms	3
Sedang	300 ms s/d 450 ms	2
Jelek	> 450 ms	1

Indeks *delay* diperoleh melalui persamaan 3:

$$Delay = \frac{Paket\ length}{Link\ bandwidth} \quad (3)$$

Jitter

Paket *jitter* diakibatkan oleh variasi-variasi dalam panjang antrian, dalam waktu pengolahan data, dan juga dalam waktu penghimpunan ulang paket-paket diakhir perjalanan *jitter*. *Jitter* lazimnya disebut variasi delay, berhubungan erat dengan latency yang menunjukan banyaknya variasi *delay* pada transmisi data di jaringan, kategori dan indeks *jitter* ditunjukan pada Tabel 5.

Tabel 5: Kategori *Jitter*

Kategori *Jitter*	*Jitter* (ms)	Indeks
Sangat Bagus	0 ms	4
Bagus	3 ms s/d 75 ms	3
Sedang	75 ms s/d 125 ms	2
Jelek	125 ms s/d 225	1

Indeks *jitter* diperoleh melalui persamaan 4:

$$Jitter = \frac{Total\ variasi\ delay}{Total\ paket\ yang\ diterima} \quad (4)$$

Total Variasi *Delay* = *Delay* – (rata-rata *Delay*)

Metode Penelitian

Metodologi dalam penelitian analisis perbandingan performansi QoS VPN *encryption protocol* pada jaringan berbasis *hybrid cloud* merupakan jenis penelitian terapan (*Applied Research*) dilakukan disalah satu group perusahaan retail dan industrial di Jakarta. Studi Literatur, merupakan tahap awal penelitian dan ditujukan untuk memperoleh informasi melalui studi kepustakaan melalui referensi buku, jurnal hingga membandingkan dengan karya ilmiah orang lain yang masih terkait dengan penelitian untuk mendapatkan data yang bersifat teoritis.

Pengumpulan Data

Pada tahap pengumpulan data dilakukan dengan pengamatan (observasi) untuk mendapatkan gambaran awal tentang keadaan sistem jaringan yang sedang berjalan dilengkapi dengan studi literatur.

Pengamatan (Observasi)

Metode ini dilakukan dengan observasi atau penelitian yang diarahkan ke objek yang sedang diteliti, dengan penelitian bereksperimen mengenai keamanan dan performansi jaringan, kemudian memberikan solusi untuk pemecahan masalah dengan menggunakan sistem keamanan yang baru.

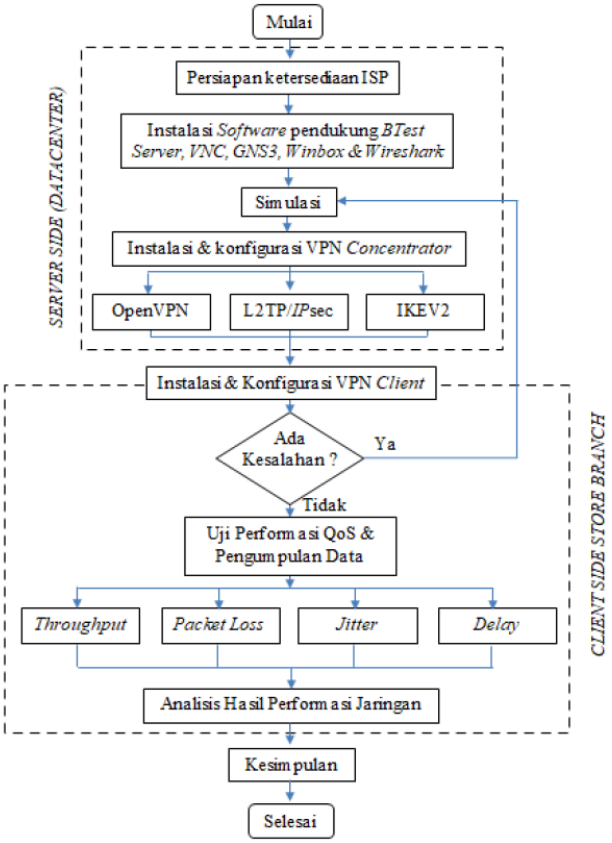
Tahapan Penelitian

Tahapan penelitian dibuat berdasarkan hasil observasi terlebih dahulu pada prosesnya meliputi melakukan pengkajian baik dari literatur, penelitian yang sejenis hingga envirotment yang digunakan pada objek penelitian. Tahapan penelitian dimulai dengan kesiapan ketersedian ISP didua lokasi baik *server side* disisi *main office* dan *client* side disisi branch, selanjutnya. Gambar 5 menunjukan tahap-tahap penelitian yang dilakukan secara menyeluruh dengan setiap tahapan diukur dengan beberapa tools pendukung.

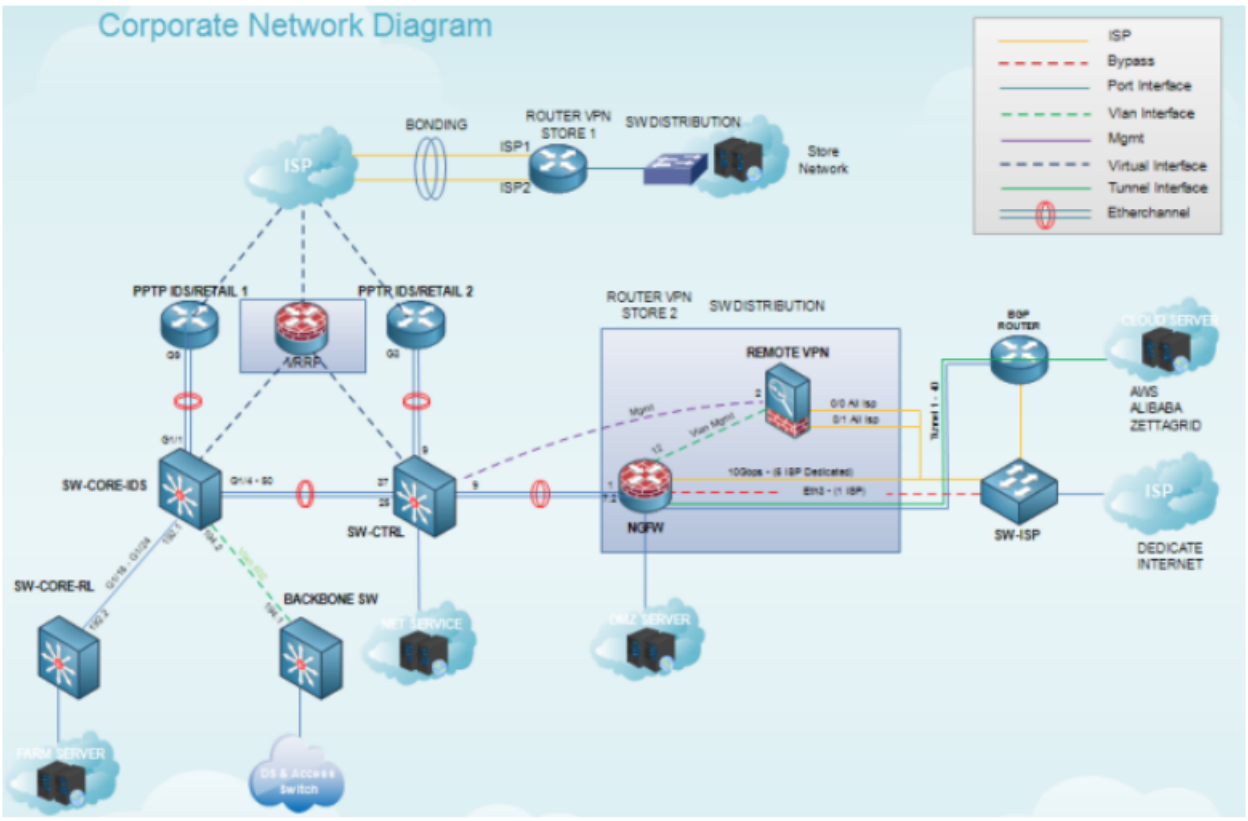
Tahap Analisis

Pada tahap analisis dibutuhkan informasi sistem jaringan yang sedang berjalan dan kebutuhan sistem jaringan yang akan digunakan, karena envirotmentnya sama maka gambaran topologi tersebut dapat dipresentasikan pada Gambar 6.

Core system yang berjalan di group perusahaan ini mengintegrasikan beberapa interkoneksi diantaranta *private cloud*, *public cloud*, core, distribution, access, dan VPN concentrator, penelitian akan difokuskan pada performansi penggunaan VPN-nya dengan memanfaatkan VPN concentrator sebagai *tunnel gateway* antara *store* dan *datacenter*, tiga model VPN tersebut yaitu L2TP/IPSec, OpenVPN dan IKEV2 akan diinstalasi pada VPN concentrator yang masing-masing diuji perbandingan performansi koneksinya, lokasi *store* yang dipilih untuk kebutuhan pengujian adalah Living World Alam Sutra karena memiliki jumlah tenant yang cukup banyak yang terdiri dari ritel maupun industrial. Secara sederhana topologi *store* living word presentasikan pada Gambar 7.

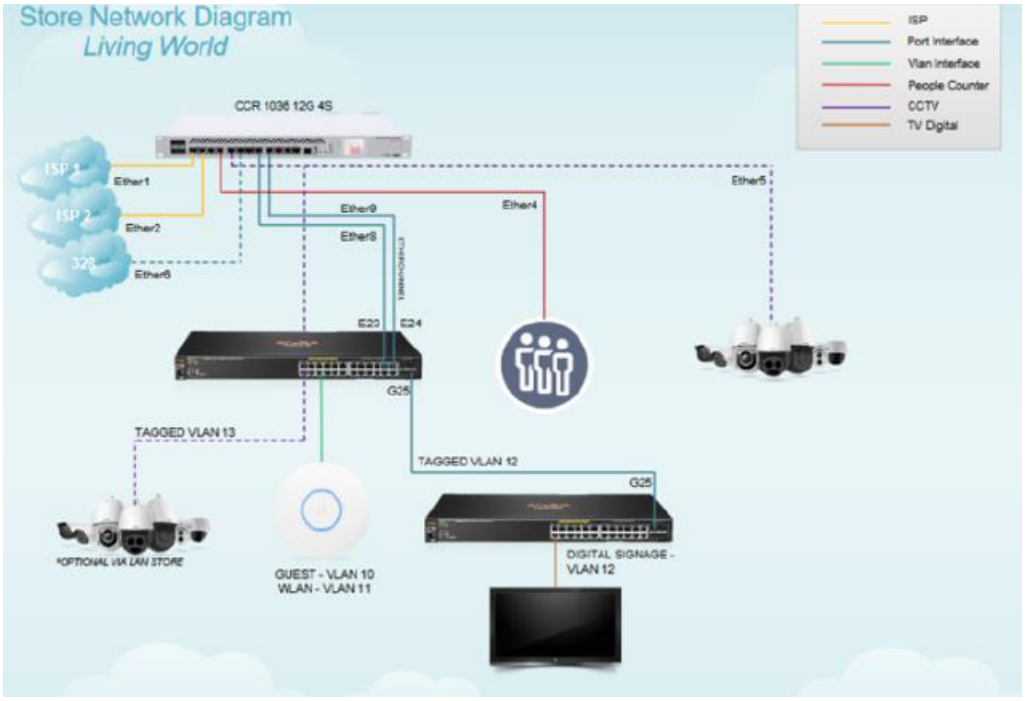


Gambar 5: Tahapan Penelitian



Gambar 6: *Corporate Network Diagram.*

Komunikasi data *store* yang dilewatkan melalui *tunnel* atau VPN cukup beragam terdiri *data replication subserver, e-mail, sap, pos, cctv, peoplecounter, mobile apps, rfid, desktop apps, crm, digital signate* dan lainnya yang membutuhkan reliabilitas dan performansi koneksi yang baik sehingga diperlukan dua koneksi atau lebih untuk proses *redundancy* guna menjaga ketersediaan koneksi sebagai penunjang operasional *store*.



Gambar 7: *Store Network Diagram.*

Gambar 8: *VPN Network Diagram*

Gambar 8 secara umum menjelaskan pertukaran informasi yang berlangsung antara *branch store* dan *main office* berdasarkan infrastruktur VPN yang akan diuji. Tahap Pengujian QoS Pengujian sistem akan dilakukan dengan melakukan analisis QoS pada jaringan VPN yang mencakup *Throughput*, *Packet loss*, Delay, dan *Jitter* sebelumnya terlebih dahulu dilakukan obervasi, pengukuran persiapan hingga desain pengujian sehingga data yang diperoleh valid, tidak terjadi perubahan yang sinifikan dengan sistem yang berjalan. Tahapan pengujian QoS ditunjukan pada Gambar 9.

Hasil dan Pembahasan

Hasil Pengujian

Setelah proses pemindaian packet yang melewati *tunnel* menggunakan Wireshark, diperoleh beberapa data yang dapat diolah dalam perhitungan uji performansi QoS, yaitu sebagai berikut:

1. Pengujian Performansi QoS OpenVPN

   Proses pemindaian packet yang dikirim dan yang diterima akan diverifikasi, pemindaian packet dijalankan pada salah satu *server active directory* di Living World Alam Sutra dengan mengakses salah satu FTP server di *main office*, berikut hasil packet capture yang telah berlangsung melalui *tunnel* OpenVPN secara statistik ditunjukan pada Gambar 10.

   Berdasarkan hasil packet capture yang diperoleh selanjutnya dilakukan perhitungan sesuai dengan parameter yang diperlukan untuk uji performansi QoS, hasil pengujian tersebut dipresentasikan pada Tabel 6.

2. Pengujian Performansi QoS L2TP/IPSec

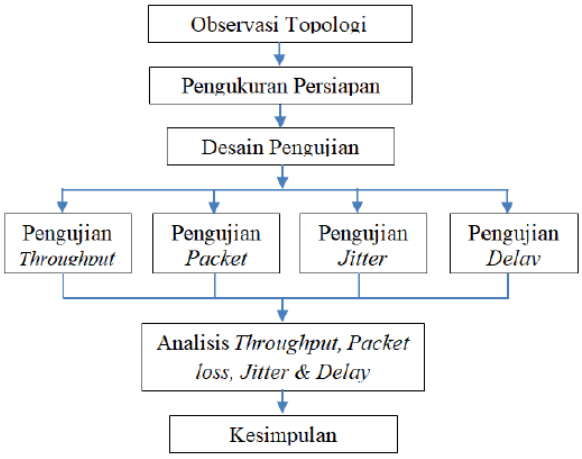
   Pemindaian paket pada *tunnel* VPN L2TP/IPSec secara statistik di tunjukan pada Gambar 11.

   Dengan langkah dan teknik yang sama pengujian dilakukan juga di model VPN L2TP/IPSec, hasil pengujian tersebut dipresentasikan pada Tabel 7.

3. Pengujian Performansi QoS IKEV2/IPSec

   Pemindaian paket pada *tunnel* VPN IKEV2/IPSec secara statistik di tunjukan pada Gambar 12.

   Dengan langkah dan teknik yang sama pengujian dilakukan juga di model VPN IKEV2/IPSec, hasil pengujian tersebut dipresentasikan pada Tabel 8.



Gambar 9: Diagram Analisis QoS

Tabel 6: Hasil Performansi QoS *Tunnel* OpenVPN

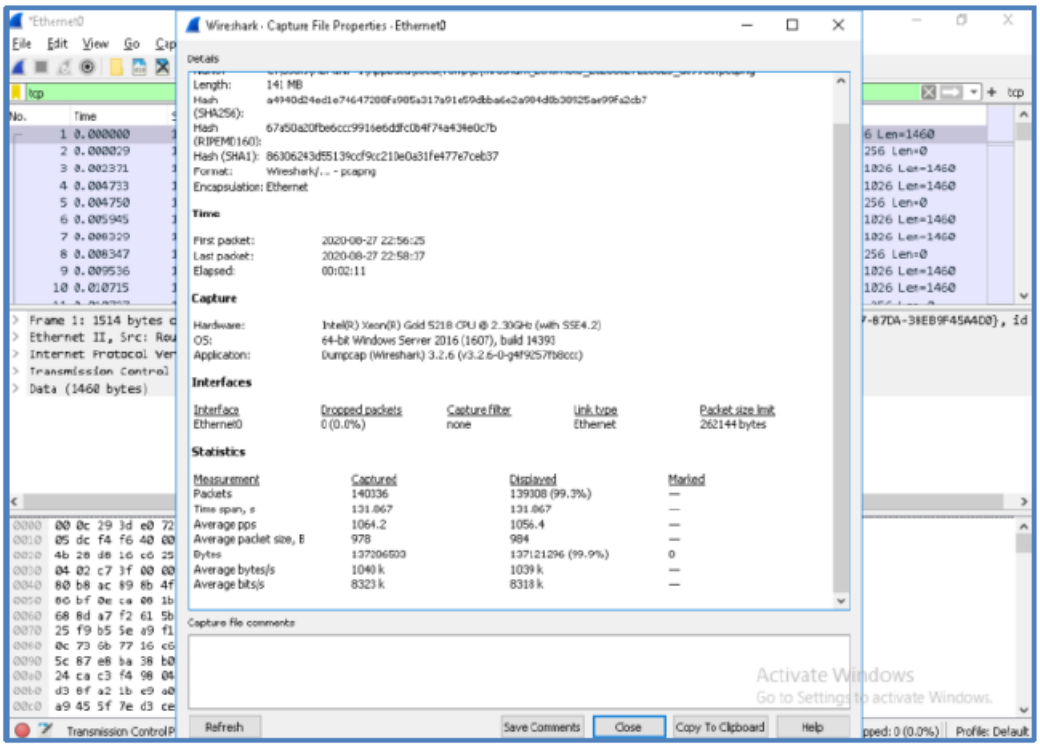
Tunnel OpenVPN	
Parameter	Nilai
Throughput	7.9383 Mb/s
Packet Loss	0,13 %
Delay	0,94 ms
Jitter	0,941 ms

Tabel 7: Hasil Performansi QoS *Tunnel* L2TP/IPSec

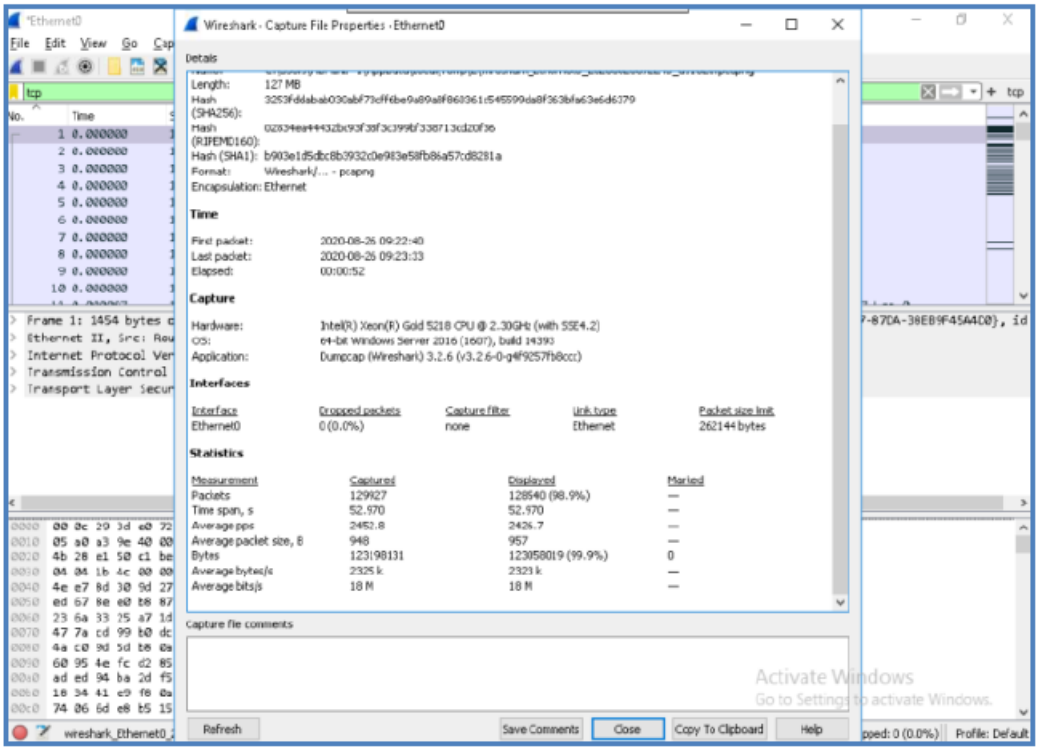
Tunnel L2TP/IPSec	
Parameter	Nilai
Throughput	18.6 Mb/s
Packet Loss	0,12 %
Delay	0,408 ms
Jitter	0,408 ms

Tabel 8: Hasil Performansi QoS *Tunnel* IKEV2/IPSec

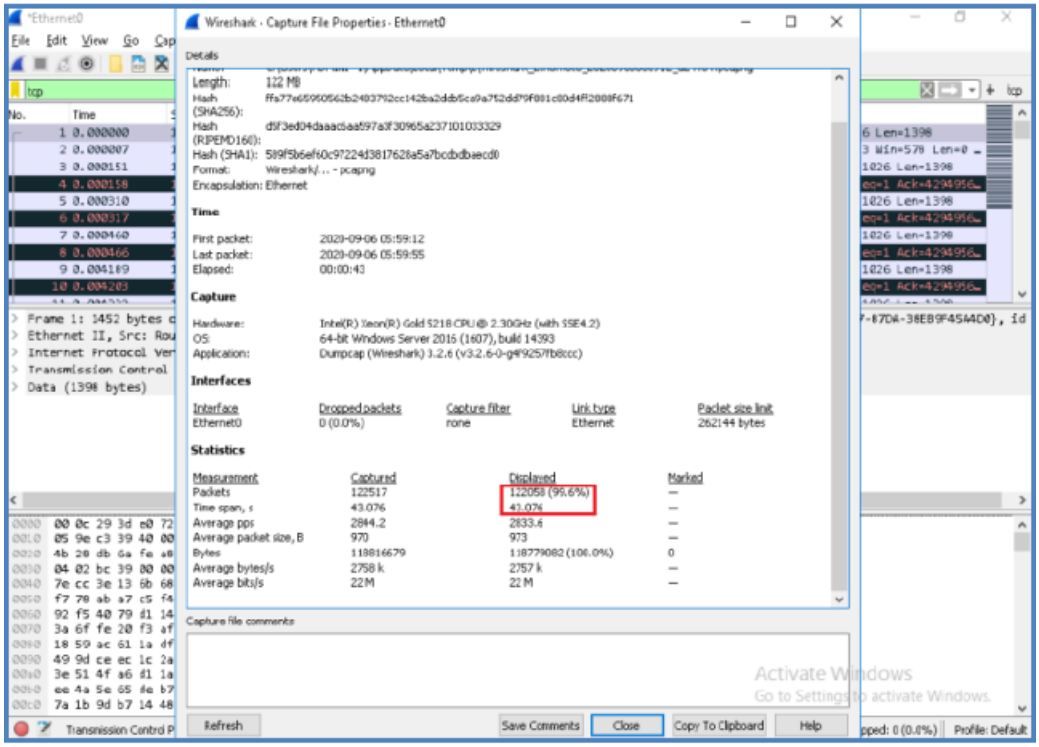
Tunnel IKEV2/IPSec	
Parameter	Nilai
Throughput	22 Mb/s
Packet Loss	0,06 %
Delay	0,351 ms
Jitter	0,352 ms



Gambar 10: Hasil Packet Capture OpenVPN



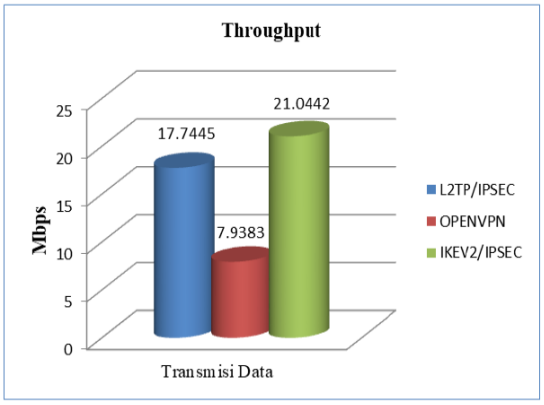
Gambar 11: Hasil Packet Capture L2TP/IPSec



Gambar 12: Hasil Packet Capture IKEV2/IPSec

Analisis Hasil Performansi Jaringan

Berdasarkan hasil uji QoS dengan model VPN L2TP/IPSEC, OpenVPN dan IKEV2/IPSec maka dapat dibuatkan grafik yang membandingkan masing-masing nilai *throughput*, *packet loss*, *delay* dan *jitter* berdasarkan kondisi packet data yang di transmisikan, dimulai dengan grafik perbandingan *throughput* ditunjukkan oleh Gambar 13



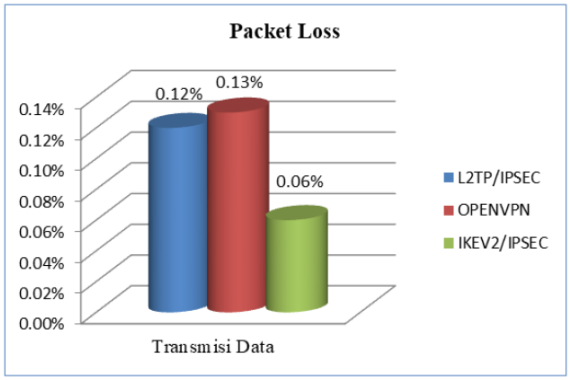
Gambar 13: Nilai *Throughput* Model L2TP/IPSec, OpenVPN dan IKEV2/IPSec.

Berdasarkan hasil pengamatan ketika pembebanan trafik diberikan sebesar 137 MB yang ditransmisikan pada ketiga model VPN menunjukkan protokol IKEV2/IPSec memiliki transfer rate yang lebih besar dibandingkan L2TP/IPSec dan OpenVPN, masing-masing memiliki selisih 15.67% untuk L2TP/IPSec dan 62.27% untuk OpenVPN, secara rinci ditampilkan pada Tabel 9.

Tabel 9: Perbandingan tingkat performansi *Throughput*

Model *VPN*	*Throughput* (Mbps)	Selisih (Mbps)	Presentase Selisih (%)
IKEV2/IPSec	21.0442	0	0
L2TP/IPSec	17.7445	3.299	15.67
OpenVPN	7.9383	9.806	62.27

Masing-masing nilai *throughput* yang diperoleh termasuk kedalam kategori sangat bagus pada standar *throughput* menurut TIPHON yaitu diatas 100 bps, secara kualitas transfer rate per detik IKEV2 memiliki kecepatan yang jauh lebih baik dengan depresiasi hanya 8 Mbps dari 30 Mbps bandwidth *branch store*.



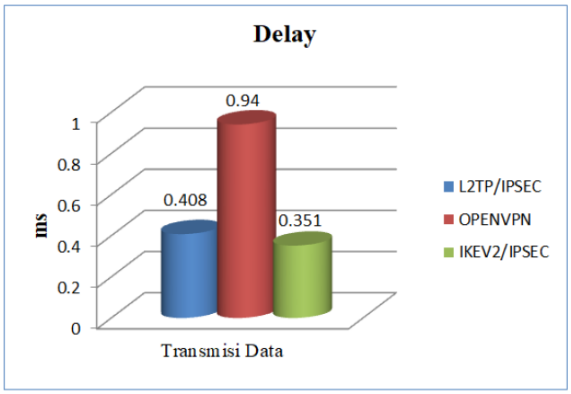
Gambar 14: Nilai *Packet Loss* Model L2TP/IPSec, OpenVPN dan IKEV2/IPSec

Berdasarkan hasil pengamatan perbandingan QoS dari performansi *packet loss* yang di tunjukan pada Gambar 14 untuk tiga kondisi pengujian menunjukkan perbedaan yang cukup signifikan bahwa protokol IKEV2/IPSec memiliki tingkat *packet loss* yang lebih kecil dibandingkan L2TP/IPSec dan OpenVPN saat data ditransmisikan, dengan nilai presentase 0.06%, IKEV2/IPSec dapat meminimalisir jumlah packet yang hilang saat transfer data berlangsung, seperti ditunjukan pada Tabel 10.

Tabel 10: Perbandingan tingkat performansi *Packet Loss*

No.	Model *VPN*	*Packet Loss* (%)
1	IKEV2/IPSec	0.06
2	L2TP/IPSec	0.12
3	OpenVPN	0.13

Masing-masing nilai *packet loss* yang diperoleh termasuk kedalam kategori sangat memuaskan pada standar *packet loss* menurut TIPHON yaitu sekitar 0%.



Gambar 15: Nilai *Delay* Model L2TP/IPSec, OpenVPN dan IKEV2/IPSec

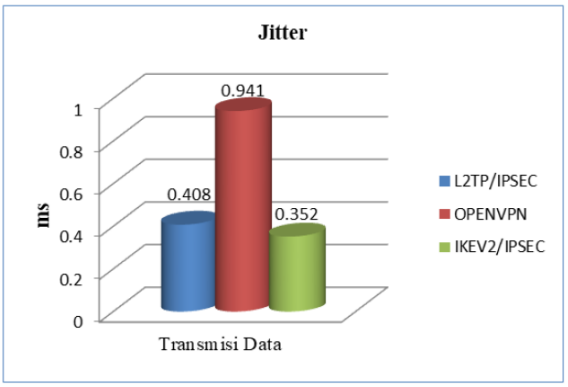
Berdasarkan hasil pengamatan perbandingan QoS dari performansi *delay* pada Gambar 15 untuk tiga kondisi pengujian menunjukkan bahwa protokol IKEV2/IPSec memiliki tingkat *delay* yang lebih kecil dari L2TP/IPSec dengan nilai 0,351 ms, sedangkan protokol OpenVPN memiliki perbedaan *delay* yang cukup signifikan dengan nilai 0,94 ms, hal ini menunjukan bahwa IKEV2/IPSec memiliki tingkat waktu latency terkecil saat dihitung berdasarkan lama waktu yang dibutuhkan paket asal menuju paket tujuan. Berikut hasil perbandingan performansi *delay* ditunjukan pada Tabel 11.

Tabel 11: Perbandingan tingkat performansi Delay

No.	Model *VPN*	*Delay* (ms)
1	IKEV2/IPSec	0,351
2	L2TP/IPSec	0,408
3	OpenVPN	0,94

Masing-masing nilai *delay* yang diperoleh termasuk kedalam kategori sangat memuaskan pada standar *jitter* menurut TIPHON yaitu dibawah 150 ms.

Berdasarkan hasil pengamatan perbandingan QoS dari performansi *jitter* pada Gambar 16 untuk tiga kondisi pengujian menunjukkan bahwa protokol IKEV2/IPSec memiliki tingkat *jitter* yang lebih kecil dari L2TP/IPSec dengan nilai 0,351 ms, sedangkan protokol OpenVPN memiliki perbedaan *jitter* yang cukup signifikan dengan nilai 0,941 ms.



Gambar 16: Nilai *Jitter* Model L2TP/IPSec, OpenVPN dan IKEV2/IPSec

Nilai *jitter* yang diperoleh IKEV2/IPSec menunjukan kecilnya paket yang hilang saat pengiriman data berlangsung dengan kecepatan tinggi. Berikut hasil perbandingan performansi *jitter* ditunjukan pada Tabel 12.

Tabel 12: Perbandingan tingkat performansi *Jitter*

No.	Model *VPN*	*Jitter* (ms)
1	IKEV2/IPSec	0,352
2	L2TP/IPSec	0,408
3	OpenVPN	0,941

Masing-masing nilai *jitter* yang diperoleh termasuk kedalam kategori sangat bagus pada standar *jitter* menurut TIPHON yaitu dibawah 0 ms. Berdasarkan seluruh pengamatan yang dilakukan IKEV2/IPSec mendominasi tingkat performansi QoS yang lebih baik diantara model L2TP/IPSec dan OpenVPN dimulai dari tingkat *throughput*, *packet loss*, *delay* dan *jitter*, secara rinci ditunjukan pada tabel 13.

Tabel 13: Perbandingan tingkat performansi QoS pada masing-masing jaringan VPN

Model *VPN*	*Throughput (Mbps)*	*Packet Loss (%)*	*Delay (ms)*	*Jitter (ms)*
IKEV2/IPSec	22	0.06	0,351	0,352
L2TP/IPSec	18.6	0.13	0,408	0,408
OpenVPN	8.3	0.12	0,94	0,94

Sedangkan akumulasi indeks QoS berdasarkan standar TIHPON seluruhnya memperoleh nilai indeks yang sama dengan kategori sangat memuaskan, ditunjukan pada tabel 14.

Tabel 14: Akumulasi Nilai dan Presentase QoS menurut TIPHON

Model *VPN*	Kategori				*Rata-Rata Nilai*	*%*	Indeks
	Throughput	*Packet Loss*	*Delay*	*Jitter*			
IKEV2	4	4	4	4	4	100	Sangat Bagus
L2TP	4	4	4	4	4	100	Sangat Bagus
Open VPN	4	4	4	4	4	100	Sangat Bagus

Pengujian yang telah dilakukan pada tiga model VPN tersebut memiliki sistem *security* yang mumpuni karena mendukung kombinasi enkripsi IPSec dan SSL, sedangkan secara performansi QoS model IKEV2/IPSec jauh lebih baik dibanding dua model VPN lainnya berdasarkan pada 4 kategori pengujian, sehingga dapat menjadi dasar pertimbangan untuk dilakukannya replacement dari model VPN existing.

Penutup

Analisis perbandingan performansi QoS pada tiga model VPN berhasil dilakukan dengan diperoleh kesimpulan bahwa IKEV2/IPSec secara signifikan memiliki memiliki nilai QoS yang lebih baik dan unggul berdasarkan semua parameter QoS yang diuji mulai dari *throughput*, *packet loss*, *delay* dan *jitter*. IKEV2/IPSec dapat menjadi standar baru untuk implementasi intekoneksi *hybrid cloud* digrup perusahaan tersebut karena dapat mendukung berlangsungnya proses implementasi standar ISO 27001 didasarkan pada kombinasi enkripsi dan performansi QoS yang lebih baik.

Daftar Pustaka

[1] W. O. Zamalia, L. M. F. Aksara, and M. Yamin, "Analisis Perbandingan Performa Qos, Pptp, L2Tp, Sstp Dan Ipsec Pada Jaringan Vpn Menggunakan Mikrotik", semanTIK, vol. 4, no. 2, pp. 29–36, 2018.

[2] F. Basyarahil, H. Astuti, and B. Hidayanto, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya", J. Tek. ITS, vol. 6, no. 1, pp. 116–121, doi: 10.12962/j23373539.v6i1.21211, 2017.

[3] F. Firmansyah, M. Wahyudi, and R. A. Purnama, "Analisis Performa Site to Site IP Security Virtual Private Network (VPN) Menggunakan Algoritma Enkripsi ISAKMP", JUITA J. Inform., vol. 7, no. 2, p. 129, doi: 10.30595/juita.v7i2.4491, 2019.

[4] K. K. Jyothi and B. I. Reddy, "Study on Virtual Private Network (VPN), VPN ' s Protocols And Security", Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 3, no. 5, pp. 919–932, 2018.

[5] S. El Yumin, J. Moh, K. Ii, and J. Selatan, "Komunikasi Softphone Menggunakan Metode Tunneling Softphone Communication Using the Tunneling Method", vol. 29, no. 1, pp. 54–60, 2019.

[6] L. Ibrahim, "Virtual Private Network (VPN) Management and IPSec Tunneling Technology", MECSJ J. Middle East Compr.), vol. 2017, no. 1, pp. 76–87, 2017.

[7] M. Iqbal and I. Riadi, "Analysis of Security Virtual Private Network (VPN) Using OpenVPN", Int. J. Cyber-Security Digit. Forensics, vol. 8, no. 1, pp. 58–65, 2019.

[8] M. Badrul, "Open VPN-Access Server Dengan Enskripsi SSL / TI Open SSL", Informatics Educ. Prof., vol. 1, no. 1, pp. 1–12, 2016.

[9] E. Fernando, D. F. Murad, H. R. Ah, and S. Pandapotan, "Analisa Dan Implementasi Algoritma Enkripsi Simetris Data Encryption Standard (DES) Pada Raspberry Pi", ULTIMATICS, vol. XI, no. 2, pp. 55–59, 2019.

[10] M.S Singh, Mankaran, A. Chassiakos, I.-H. Khoo, and H.-G. Yeh, "Connectivity Between Two Distant Sites with Automatic Failover To IPsec", Disertation, California State University, ISBN: 978-1-369-71591-0, 2017.

[11] A. Darojat and I. Nurhaida, "Analisa Qos Administrative Distance", J. Ilmu Tek. dan Komput., vol. 3, no. 1, pp. 11–21, 2019.

[12] K. K. V. V. Singh and H. Gupta, "A new approach for the securityof VPN", ACM Int. Conf. Proceeding Ser., vol. 04-05, doi: 10.1145/2905055.2905219, March 2016.

[13] D. Hari, P. Dewa, E. S. Pramukantoro, and D. P. Kartikasari, "Analisis Mekanisme Keamanan Antara TLS / SSL Dan Crypto Pada Komunikasi IoT Middleware Dengan Subscriber Berbasis Protokol HTTP", J. Pengemb. Teknol. Inf. dan Ilmu Komput., vol. 2, no. 10, pp. 4027–4033, 2018.

[14] Niko Adianson, Yupianti and Adhadi Kurniawan, "Analisa Perbandingan Performansi Rsa (Rivest Shamir Adleman) Dan Ecc (Elliptic Curve) Pada Protokol Secure Socket Layer (SSL)", Jurnal Media Infotama, vol. 11, no. 1, pp. 71–80, 2015.

[15] S. Ikhwan and A. Amalina, "Analisis Jaringan VPN Menggunakan PPTP dan L2TP", J. Infotel, vol. 9, no. 3, doi: 10.20895/infotel.v9i3.274, 2017.

[16] A. Rachmawan, "Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet di Atas VPN", J. Manaj. Inform., vol. 8, no. 2, pp. 53–57, 2018.

[17] B. Veldhuizen, "Automated state machine learning of IPsec implementations", Bachelor Thesis, Radboud University, 2017.

[18] S. Sudetlin, N. D. Natasha, and U. Darusalam, "Pemanfaatan Private Cloud Storage Berbasis Infrastructure As A Service (IAAS)", JOINTECS (Journal Inf. Technol. Comput. Sci., vol. 3, no. 1, pp. 54–60, doi: 10.31328/jointecs.v3i1.497, 2018.

[19] R. Wulandari, "Analisis QoS (Quality of Service) Pada Jaringan Internet (Studi Kasus: UPT Loka Uji Teknik Penambangan Jampang Kulon - LIPI)", J. Tek. Inform. dan Sist. Inf., vol. 2, no. 2, pp. 162–172, doi: 10.28932/jutisi.v2i2.454, 2016.

[20] S. A. Tirtana and H. T. Hidayat, "Rancang Bangun Prototype Smart Room Berbasis a-14 a-15", Proceeding Semin. Nas. Politek. Negeri Lhokseumawe, vol. 2, no. 1, pp. 14–18, 2018.